

## Assignments for Trusted Computing Group

**To:** T13 Technical Committee  
**From:** Jim Hatfield  
Seagate Technology  
(for the Trusted Computed Group  
[www.trustedcomputinggroup.org](http://www.trustedcomputinggroup.org) )  
389 Disc Drive  
Longmont, CO 80503  
**Phone:** 720-684-2120  
**Fax:** 720-684-2722  
**Email:** James.C.Hatfield@seagate.com  
**Date:** February 22, 2006

### Revision History:

- 0: Initial revision
- 1: Corrected names of DMA command versions
- 2: Synchronized with T10/05-157r1 and r2, addressed comments from June 2005 T13 meeting and from the July T10 meeting.
- 3: Address comments from Aug.2005 T13 meeting, Sept. 2005 and Oct.2005 T10 meetings.
- 4: Asked for 1 word in IDENTIFY instead of 2 bits, define 'background activity', describe allowable side-effects, swap TP\_SPECIFIC subcodes of Security\_Protocol 00h for TRUSTED RECEIVE, renamed command fields to match ATA8 nomenclature, changed ALLOCATION\_LENGTH to Transfer\_Length, added DCO support.
- 5: Better definition of IDENTIFY word being requested; Added 4 reserved bytes to Table 11; Synch with what T10 accepted into SPC-4 in January 2006; removed tables showing the content of certificates;
- 6: Changed SP\_Specific and Transfer\_Length fields to security protocol-specific fields to make the interface more extensible for non-TCG protocols; accepted all changes for a clean reading; clarified Transfer\_Length truncation on TRUSTED RECEIVE; general cleanup of leftover change-bar side-effects; removed un-referenced documents and defined terms;
- 7: Restored Transfer\_Length as a named parameter with a fixed location in the command block so that bridges do not have to snoop the security protocol in order to merely transfer data; made minor mods to adhere to the style guides. Approved for inclusion into ATA8-ACS.

## 1 Introduction

The purpose of this proposal is to specify the ATA host interface for "trusted computing" command and resulting data streams.

The intention is for T13 and T10 to define similar command 'containers' to transfer identical data streams. The initial set of data streams are being defined by the Trusted Computing Group (TCG).

See also, T10 proposal 05-157r9 "SPC-4 Security Commands Proposal", which was accepted for inclusion into SPC-4 in January 2006.

ATA opcodes for these commands have already been allocated as 'Reserved for Trusted Computing Group (TCG)' by T13 proposal e04128r3, which was approved in 2004.

## 2 Proposal

I propose that the following text be incorporated into ATA8-ACS to describe the new feature set, the TRUSTED SEND and TRUSTED RECEIVE commands, and for some bit assignments in IDENTIFY DEVICE and DEVICE CONFIGURATION OVERLAY.

### 2.1 References

Add these references to ATA8-ACS:

#### 2.1.1 Approved References

- ITU-T RECOMMENDATION X.509 | ISO/IEC 9594-8, *Information Technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*, ITU, 2000.

#### 2.1.2 IETF References

- RFC 3280, *Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List (CRL) Profile*, IETF, 2002.
- RFC 3281, *An Internet Attribute Certificate: Profile for Authorization*, IETF, 2002.

### 2.2 Definitions

Add these definitions to the Glossary.

TCG	Trusted Computing Group: An organization that develops and promotes open standards for hardware-enabled trusted computing and security technologies. See <a href="https://www.trustedcomputinggroup.org">https://www.trustedcomputinggroup.org</a>
<u>Background Activities</u>	Activities initiated by a command that occur after command completion has been reported.

### 2.3 Feature Description

#### 2.3.1 Trusted Computing feature set

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

These commands are prohibited for use by devices that implement the PACKET command feature set.

This feature set defines two data-in commands (TRUSTED RECEIVE and TRUSTED RECEIVE DMA) and two data-out commands (TRUSTED SEND and TRUSTED SEND DMA). These commands provide for variable length data transfers.

TRUSTED SEND and TRUSTED SEND DMA may be used interchangeably. They only differ by the type of data transport protocol used (PIO vs. DMA). Similarly, TRUSTED RECEIVE and TRUSTED RECEIVE DMA are interchangeable.

The IDENTIFY DEVICE command indicates whether or not this feature set is supported.

The DEVICE CONFIGURATION OVERLAY (SET) command offers a mechanism to remove support for the 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 T10

and T13. The intent is to standardize the data content so it is identical across both ATA and SCSI interfaces.

## 2.4 Command Descriptions

### 2.4.1 IDENTIFY DEVICE – ECh, PIO data-in

This proposal requests that the editor assign one word:

Word	O/M	F/V	Description
TBD1	O		Trusted Computing Feature Set Options
		F	15 Shall be cleared to zero
		F	14 Shall be set to one
		V	13:1 Reserved for TCG
		F	0 1=Trusted Computing feature set is supported

word TBD1, bit 0            When set to one, indicates that the Trusted Computing feature set is supported.

### 2.4.2 DEVICE CONFIGURATION OVERLAY (IDENTIFY) - B1h/C2h, PIO Data-in

Word TBD3    bit C    1= reporting of support for the Trusted Computing feature set is allowed

Word TBD3, bit C if set to one indicates that the device is allowed to report support for the Trusted Computing feature set.

### 2.4.3 DEVICE CONFIGURATION OVERLAY (SET) - B1h/C3h, PIO Data Out

Word TBD3    bit C    1= reporting of support for the Trusted Computing feature set is allowed

Word TBD3 bit C is cleared to zero to disable support for the Trusted Computing feature set and has the effect of clearing IDENTIFY DEVICE data words TBD1 bits A and B to zero. This value shall not be changed and command aborted shall be returned if the Security Mode feature set is enabled.

#### 2.4.4 TRUSTED SEND – 5Eh, PIO data-out

- **Feature Set**

This command is mandatory for devices implementing the Trusted Computing feature set.

- **Description**

The TRUSTED SEND command is used to send data to the device. The data sent contains one or more Security\_Protocol specific instructions to be performed by the device. The host uses TRUSTED RECEIVE commands to retrieve any data resulting from these instructions.

Any association between a TRUSTED SEND command and a subsequent TRUSTED RECEIVE command depends on the protocol specified by the Security\_Protocol field (see Table 1). Each protocol shall specify whether:

- a) the device shall complete the command with normal status as soon as it determines the data has been correctly received. An indication that the data has been processed is obtained by sending a TRUSTED RECEIVE command and receiving the results in the associated data transfer; or
- b) the device shall complete the command with normal status only after the data has been successfully processed and an associated TRUSTED RECEIVE command is not required.

There may be intentional side effects, depending on the trusted operation requested. Most trusted operations will have no side effects, but there may be some allowable exceptions. For example, a request to lock the device would be expected to cause subsequent reads or writes to fail.

The completion of background activity resulting from a trusted command shall not abort any outstanding queued commands.

The format of the data and some of the command block parameters depends on the protocol specified by the Security\_Protocol field (see Table 1).

- **Inputs**

Word	Name	Description								
00h	Feature	<table border="1"> <thead> <tr> <th>Bit</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>15:8</td> <td>Reserved</td> </tr> <tr> <td>7:0</td> <td>Security_Protocol (See Table 1 )</td> </tr> </tbody> </table>	Bit	Description	15:8	Reserved	7:0	Security_Protocol (See Table 1 )		
Bit	Description									
15:8	Reserved									
7:0	Security_Protocol (See Table 1 )									
01h	Count	<table border="1"> <thead> <tr> <th>Bit</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>15:8</td> <td>Reserved</td> </tr> <tr> <td>7:0</td> <td>Transfer_Length (7:0)</td> </tr> </tbody> </table>	Bit	Description	15:8	Reserved	7:0	Transfer_Length (7:0)		
Bit	Description									
15:8	Reserved									
7:0	Transfer_Length (7:0)									
02h-04h	LBA	<table border="1"> <thead> <tr> <th>Bit</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>47:24</td> <td>Reserved</td> </tr> <tr> <td>23:8</td> <td>Depends on the value of Security_Protocol (See 2.4.4.1)</td> </tr> <tr> <td>7:0</td> <td>Transfer_Length (15:8)</td> </tr> </tbody> </table>	Bit	Description	47:24	Reserved	23:8	Depends on the value of Security_Protocol (See 2.4.4.1)	7:0	Transfer_Length (15:8)
Bit	Description									
47:24	Reserved									
23:8	Depends on the value of Security_Protocol (See 2.4.4.1)									
7:0	Transfer_Length (15:8)									
05h	Command	5Eh								

The Security\_Protocol field identifies which security protocol is being used. This determines the format of the command block parameters and of the data that is transferred. (see Table 1 ). If the Security\_Protocol field is set to a reserved value, the device shall return command aborted.

**Table 1 – TRUSTED SEND - Security\_Protocol field description**

Value	Description
00h	Reserved.
01h – 06h	Defined by TCG.
07h – EFh	Reserved.
F0h – FFh	Vendor Specific.

The meaning of is the security protocol-specific fields are defined by each security protocol. For Security\_Protocol values 01h-06h, see 2.4.4.1.

- **Normal outputs**

See [Editor’s note: ATA8-ACS clause 7.1.5 Normal Outputs]

- **Error outputs**

The device shall return command aborted if the command is not supported or if an unrecoverable error occurred during the execution of the command. The amount of data transferred is indeterminate. See [ Editor’s note: ATA8-ACS clause 7.1.6 Error Outputs]

**2.4.4.1 TRUSTED SEND – Command Block Parameters for Security\_Protocol 01h – 06h**

For TRUSTED SEND, when Security\_Protocol is 01h – 06h, the security protocol-specific command block fields are mapped as in Table 2.

**Table 2 - TRUSTED SEND – Command Block Parameters for Security\_Protocol 01h-06h**

LBA(23:16)	LBA(15:8)
SP_Specific(15:0)	

The TRANSFER\_LENGTH field contains the number of 512-byte blocks of data to be transferred. (One means 512 bytes, two means 1024 bytes, etc.). Pad bytes are appended to the valid data as needed to meet this requirement. Pad bytes shall have a value of 00h. A value of zero specifies that no data transfer shall take place, and shall not be considered to be an error.

The SP\_Specific field provides Security\_Protocol field specific information. The meaning of this field is defined by each security protocol.

### 2.4.5 TRUSTED SEND DMA – 5Fh, DMA data-out

- **Feature Set**

This command is mandatory for devices implementing the Trusted Computing feature set.

- **Description**

See the TRUSTED SEND (5Eh) command for the description of this command and parameters.

- **Inputs**

Word	Name	Description								
00h	Feature	<table border="1"> <thead> <tr> <th>Bit</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>15:8</td> <td>Reserved</td> </tr> <tr> <td>7:0</td> <td>Security_Protocol (See Table 1 )</td> </tr> </tbody> </table>	Bit	Description	15:8	Reserved	7:0	Security_Protocol (See Table 1 )		
Bit	Description									
15:8	Reserved									
7:0	Security_Protocol (See Table 1 )									
01h	Count	<table border="1"> <thead> <tr> <th>Bit</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>15:8</td> <td>Reserved</td> </tr> <tr> <td>7:0</td> <td>Transfer_Length (7:0)</td> </tr> </tbody> </table>	Bit	Description	15:8	Reserved	7:0	Transfer_Length (7:0)		
Bit	Description									
15:8	Reserved									
7:0	Transfer_Length (7:0)									
02h-04h	LBA	<table border="1"> <thead> <tr> <th>Bit</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>47:24</td> <td>Reserved</td> </tr> <tr> <td>23:8</td> <td>Depends on the value of Security_Protocol (See 2.4.4.1)</td> </tr> <tr> <td>7:0</td> <td>Transfer_Length (15:8)</td> </tr> </tbody> </table>	Bit	Description	47:24	Reserved	23:8	Depends on the value of Security_Protocol (See 2.4.4.1)	7:0	Transfer_Length (15:8)
Bit	Description									
47:24	Reserved									
23:8	Depends on the value of Security_Protocol (See 2.4.4.1)									
7:0	Transfer_Length (15:8)									
05h	Command	5Fh								

- **Normal outputs**

See [Editor's note: ATA8-ACS clause 7.1.5 Normal Outputs]

- **Error outputs**

The device shall return command aborted if the command is not supported or if an unrecoverable error occurred during the execution of the command. The amount of data transferred is indeterminate. See [Editor's note: ATA8-ACS clause 7.1.6 Error Outputs]

**2.4.6 TRUSTED RECEIVE – 5Ch, PIO data-in**

- **Feature Set**

This command is mandatory for devices implementing the Trusted Computing feature set.

- **Description**

The TRUSTED RECEIVE command is used to retrieve security protocol information (see 2.4.6.2) or the results from one or more TRUSTED SEND commands.

Any association between a previous TRUSTED SEND command and the data transferred by a TRUSTED RECEIVE command depends on the protocol specified by the Security\_Protocol field (see Table 3). If the device has no data to transfer (e.g., the results for any previous TRUSTED SEND commands are not yet available), the device may transfer data indicating it has no other data to transfer.

Indications of data overrun or underrun and the mechanism, if any, for processing retries depend on the protocol specified by the Security\_Protocol field (see Table 3).

For Security\_Protocol field set to 00h, the format of the data is described in 2.4.6.2. The format of the data for other Security\_Protocol values is documented by the group that owns the associated Security\_Protocol value.

The device shall retain data resulting from a TRUSTED SEND command awaiting retrieval by a TRUSTED RECEIVE command until one of the following events is processed:

- a) the data is delivered according to the Security\_Protocol field (see Table 3) specific rules for the TRUSTED RECEIVE command;
- b) any reset; or
- c) loss of communication with the host that sent the TRUSTED SEND command.

- **Inputs**

Word	Name	Description						
00h	Feature	<table border="0"> <tr> <td><b>Bit</b></td> <td><b>Description</b></td> </tr> <tr> <td>15:8</td> <td>Reserved</td> </tr> <tr> <td>7:0</td> <td>Security_Protocol (See Table 3 )</td> </tr> </table>	<b>Bit</b>	<b>Description</b>	15:8	Reserved	7:0	Security_Protocol (See Table 3 )
<b>Bit</b>	<b>Description</b>							
15:8	Reserved							
7:0	Security_Protocol (See Table 3 )							
01h	Count	<table border="0"> <tr> <td><b>Bit</b></td> <td><b>Description</b></td> </tr> <tr> <td>15:8</td> <td>Reserved</td> </tr> <tr> <td>7:0</td> <td>Transfer_Length (7:0)</td> </tr> </table>	<b>Bit</b>	<b>Description</b>	15:8	Reserved	7:0	Transfer_Length (7:0)
<b>Bit</b>	<b>Description</b>							
15:8	Reserved							
7:0	Transfer_Length (7:0)							
02h-04h	LBA	<table border="0"> <tr> <td><b>Bit</b></td> <td><b>Description</b></td> </tr> <tr> <td>47:24</td> <td>Reserved</td> </tr> <tr> <td>23:0</td> <td>Transfer_Length (15:8)</td> </tr> </table>	<b>Bit</b>	<b>Description</b>	47:24	Reserved	23:0	Transfer_Length (15:8)
<b>Bit</b>	<b>Description</b>							
47:24	Reserved							
23:0	Transfer_Length (15:8)							
05h	Command	5Ch						

The Security\_Protocol field identifies which security protocol is being used. This determines the format of the command block parameters and of the data that is transferred (see Table 3). If the Security\_Protocol field is set to a reserved value, the device shall return command aborted.

**Table 3 – TRUSTED RECEIVE - Security\_Protocol field description**

Value	Description
00h	Return security protocol information (see 2.4.6.2)
01h – 06h	Reserved for TCG.
07h – EFh	Reserved.
F0h – FFh	Vendor Specific

- **Normal outputs**

See[Editor's note: ATA8-ACS clause 7.1.5 Normal Outputs]

- **Error outputs**

The device shall return command aborted if the command is not supported. An unrecoverable error encountered during execution of this command results in the termination of the command. The amount of data transferred is indeterminate. See [ Editor's note: ATA8-ACS clause 7.1.6 Error Outputs]

**2.4.6.1 TRUSTED RECEIVE - Command Block Parameters for Security\_Protocol 00h – 06h**

For TRUSTED RECEIVE, when Security\_Protocol is 00h – 06h, the security protocol-specific command block fields are mapped as in Table 4.

Table 4 - TRUSTED RECEIVE – Command Block Parameters for Security\_Protocol 00h – 06h

LBA(23:16)	LBA(15:8)
SP_Specific(15:0)	

The SP\_Specific field provides Security\_Protocol field specific information. The meaning of these fields are defined by each security protocol. For Security\_Protocol field set to 00h, see 2.4.6.2.

The Transfer\_Length field contains the number of 512-byte blocks of data to be transferred. (One means 512 bytes, two means 1024 bytes, etc.) A Transfer\_Length value of zero specifies that no data shall be transferred. This condition shall not be considered an error.

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.

**2.4.6.2 Security\_Protocol 00h Description**

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 the Security\_Protocol field is set to 00h, the SP\_Specific fields are shown in Table 5.

**Table 5 – Security\_Protocol 00h - SP\_Specific field descriptions**

SP_Specific	Description	Reference	Support
0000h	Return supported security protocol list	2.4.6.3	Mandatory
0001h	Return a certificate	2.4.6.4	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.

**2.4.6.3 Supported security protocols list description**

When the Security\_Protocol field is set to 00h, and SP\_Specific is set to 0000h in a TRUSTED RECEIVE command, the parameter data shall have the format shown in Table 6.

**Table 6 – TRUSTED RECEIVE parameter data for SP\_Specific=0000h**

Bit	7	6	5	4	3	2	1	0	
<b>Byte</b>									
<b>0</b>	RESERVED								
<b>1</b>	RESERVED								
<b>2</b>	RESERVED								
<b>3</b>	RESERVED								
<b>4</b>	RESERVED								
<b>5</b>	RESERVED								
<b>6</b>	(MSB)	LIST length (M – 7)							
<b>7</b>								(LSB)	
<b>8</b>	SUPPORTED Security_Protocol LIST								
<b>M</b>									
<b>M+1</b>									
<b>511</b>	PAD BYTES (if any)								

The LIST LENGTH field indicates the total length, in bytes, of the supported security protocol list.

The SUPPORTED Security\_Protocol LIST field shall contain a list of all supported Security\_Protocol field values. Each byte indicates a supported Security\_Protocol field value. The values shall be in ascending order starting with 00h.

The total data length shall be 512 bytes. Pad bytes are appended as needed to meet this requirement. Pad bytes shall have a value of 00h.

**2.4.6.4 Certificate data description**

**2.4.6.4.1 Certificate overview**

A certificate is either an X.509 Attribute Certificate or an X.509 Public Key Certificate depending on the capabilities of the device.

When the Security\_Protocol field of the TRUSTED RECEIVE command is set to 00h, and SP\_Specific is 0001h, the parameter data shall have the format shown in Table 7.

**Table 7 – TRUSTED RECEIVE parameter data for SP\_Specific=0001h**

Bit	7	6	5	4	3	2	1	0	
<b>Byte</b>									
<b>0</b>	RESERVED								
<b>1</b>	RESERVED								
<b>2</b>	(MSB)	CERTIFICATE LENGTH (M – 3)							
<b>3</b>								(LSB)	
<b>4</b>	X.509 certificate bytes								
<b>M</b>									
<b>M+1</b>									
<b>N</b>	PAD BYTES (if any)								

The CERTIFICATE LENGTH indicates the total length, in bytes, of the certificate(s). This length includes one or more certificates. If the device doesn't have a certificate to return, the certificate length is set to 0000h and only the 4 byte header and 508 pad bytes are returned.

The contents of the certificate fields are defined in 2.4.6.4.2 and 0.

The total data length shall conform to the Transfer\_Length field requirements.

**2.4.6.4.2 Public Key certificate description**

RFC 3280 defines the certificate syntax for certificates consistent with X.509v3 Public Key Certificate Specification. Any further restrictions beyond the requirements of RFC 3280 are TBD.

**2.4.6.4.3 Attribute certificate description**

RFC 3281 defines the certificate syntax for certificates consistent with X.509v2 Attribute Certificate Specification. Any further restrictions beyond the requirements of RFC 3281 are TBD.

### 2.4.7 TRUSTED RECEIVE DMA – 5Dh, DMA data-in

- **Feature Set**

This command is mandatory for devices implementing the Trusted Computing feature set.

- **Description**

See the TRUSTED RECEIVE (5Ch) command for the description of this command and its parameters.

- **Inputs**

Word	Name	Description						
00h	Feature	<table border="1"> <thead> <tr> <th>Bit</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>15:8</td> <td>Reserved</td> </tr> <tr> <td>7:0</td> <td>Security_Protocol (See Table 3)</td> </tr> </tbody> </table>	Bit	Description	15:8	Reserved	7:0	Security_Protocol (See Table 3)
Bit	Description							
15:8	Reserved							
7:0	Security_Protocol (See Table 3)							
01h	Count	<table border="1"> <thead> <tr> <th>Bit</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>15:8</td> <td>Reserved</td> </tr> <tr> <td>7:0</td> <td>Transfer_Length (7:0)</td> </tr> </tbody> </table>	Bit	Description	15:8	Reserved	7:0	Transfer_Length (7:0)
Bit	Description							
15:8	Reserved							
7:0	Transfer_Length (7:0)							
02h-04h	LBA	<table border="1"> <thead> <tr> <th>Bit</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>47:24</td> <td>Reserved</td> </tr> <tr> <td>23:0</td> <td>Transfer_Length (15:8)</td> </tr> </tbody> </table>	Bit	Description	47:24	Reserved	23:0	Transfer_Length (15:8)
Bit	Description							
47:24	Reserved							
23:0	Transfer_Length (15:8)							
05h	Command	5Dh						

- **Normal outputs**

See [Editor's note: ATA8-ACS clause 7.1.5 Normal Outputs]

- **Error outputs**

The device shall return command aborted if the command is not supported. An unrecoverable error encountered during execution of this command results in the termination of the command. The amount of data transferred is indeterminate. See [Editor's note: ATA8-ACS clause 7.1.6 Error Outputs]