

Assignments for Trusted Computing Group

To: T13 Technical Committee
From: Jim Hatfield
 Seagate Technology
 (for the Trusted Computed Group
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 6, 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 TRUSTED_PROTOCOL_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;

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.
- Information processing systems – Open Systems Interconnection – Specification of Abstract Syntax Notation One (ASN.1), International Organization for Standardization. International Standard 8824, (December, 1987)
- T10/1731-D Information technology - SCSI Primary Commands - 3 (SPC-3)

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.

<u>TCG</u>	<u>Trusted Computing Group: An organization that develops and promotes open standards for hardware-enabled trusted computing and security technologies. See https://www.trustedcomputinggroup.org</u>
<u>ASN.1</u>	<u>Abstract Syntax Notation One. (See 2.1.1)</u>
<u>OID</u>	<u>Object Identifier. See ASN.1 and ISO/IEC 9834/ ITU-T X.622.</u>
<u>Background Activities</u>	<u>Optional processes executed by the device when not actively executing a command (e.g. idle). The device shall be capable of interrupting such activity to process new commands. Design and implementation of scheduling algorithms for balancing foreground and background activity shall be vendor-specific. Examples of normal background include (but are not limited to) buffer management (read look-ahead, cache flushing), power management, SMART monitoring, SCT LBA Segment Access, Trusted Computing requests, etc.</u>

2.3 Feature Description

2.4 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.

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). ~~If this feature set is supported, the device shall support at least one of the data-in commands and at least one of the data-out commands.~~ 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, and if it is supported, whether or not it is enabled.

The command block (e.g. taskfile) fields are defined by T13.

The data streams and subsequent actions resulting from these commands are defined by the Trusted protocol 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.

~~These commands are prohibited for use by PACKET devices. PACKET devices needing this functionality are expected to support the optional SCSI commands: TRUSTED IN and TRUSTED OUT via the ATAPI transport. See SPC-4 for details on the TRUSTED IN and TRUSTED OUT commands.~~

2.5 Command Descriptions

2.5.1 IDENTIFY DEVICE – ECh, PIO data-in

This proposal requests that the editor assign ~~two bits~~ one word:

<u>Word</u>	<u>O/M</u>	<u>F/V</u>	<u>Description</u>
TBD1	Q		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.

2.5.2 IDENTIFY PACKET DEVICE – A2h, PIO data-in

This proposal requests that the editor assign two bits:

2.5.2 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.

2.5.3 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 word TBD1 bits A and B to zero of the IDENTIFY DEVICE or IDENTIFY PACKET DEVICE response. This value shall not be changed and command aborted shall be returned if the Security Mode feature set is enabled.

2.5.52.5.4 TRUSTED SEND – 5Eh, PIO data-out

- **Feature Set**

This command is ~~optional~~ 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 TRUSTED_PROTOCOLSECURITY_PROTOCOL specific instructions to be performed by the device. The host uses Trusted receive commands to retrieve any data ~~derived~~ resulting from these instructions. ~~The device shall return Command Complete as soon as it determines the data has been correctly received. This does not indicate that the data has been parsed or that any trusted actions have been processed. These indications are only obtained by sending a TRUSTED RECEIVE command and receiving the results in the associated data transfer.~~

Any association between a TRUSTED SEND command and a subsequent TRUSTED RECEIVE command depends on the protocol specified by the TRUSTED_PROTOCOL field (see Table 2). 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 are 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 depends on the protocol specified by the TRUSTED_PROTOCOLSECURITY_PROTOCOL field (see Table 2)

- **Inputs**

Table 1 - TRUSTED SEND command parameters

<u>Word</u>	<u>Name</u>	<u>Description</u>								
<u>00h</u>	<u>Feature</u>	<table border="1"> <thead> <tr> <th><u>Bit</u></th> <th><u>Description</u></th> </tr> </thead> <tbody> <tr> <td><u>15:8</u></td> <td><u>Reserved</u></td> </tr> <tr> <td><u>7:0</u></td> <td><u>SECURITY_PROTOCOL (See Table 2)</u></td> </tr> </tbody> </table>	<u>Bit</u>	<u>Description</u>	<u>15:8</u>	<u>Reserved</u>	<u>7:0</u>	<u>SECURITY_PROTOCOL (See Table 2)</u>		
<u>Bit</u>	<u>Description</u>									
<u>15:8</u>	<u>Reserved</u>									
<u>7:0</u>	<u>SECURITY_PROTOCOL (See Table 2)</u>									
<u>01h</u>	<u>Count</u>	<table border="1"> <thead> <tr> <th><u>Bit</u></th> <th><u>Description</u></th> </tr> </thead> <tbody> <tr> <td><u>15:8</u></td> <td><u>Reserved</u></td> </tr> <tr> <td><u>7:0</u></td> <td><u>TRANSFER_LENGTH [7:0]</u></td> </tr> </tbody> </table>	<u>Bit</u>	<u>Description</u>	<u>15:8</u>	<u>Reserved</u>	<u>7:0</u>	<u>TRANSFER_LENGTH [7:0]</u>		
<u>Bit</u>	<u>Description</u>									
<u>15:8</u>	<u>Reserved</u>									
<u>7:0</u>	<u>TRANSFER_LENGTH [7:0]</u>									
<u>02h-04h</u>	<u>LBA</u>	<table border="1"> <thead> <tr> <th><u>Bit</u></th> <th><u>Description</u></th> </tr> </thead> <tbody> <tr> <td><u>47:24</u></td> <td><u>Reserved</u></td> </tr> <tr> <td><u>23:8</u></td> <td><u>SP_SPECIFIC</u></td> </tr> <tr> <td><u>7:0</u></td> <td><u>TRANSFER_LENGTH [15:8]</u></td> </tr> </tbody> </table>	<u>Bit</u>	<u>Description</u>	<u>47:24</u>	<u>Reserved</u>	<u>23:8</u>	<u>SP_SPECIFIC</u>	<u>7:0</u>	<u>TRANSFER_LENGTH [15:8]</u>
<u>Bit</u>	<u>Description</u>									
<u>47:24</u>	<u>Reserved</u>									
<u>23:8</u>	<u>SP_SPECIFIC</u>									
<u>7:0</u>	<u>TRANSFER_LENGTH [15:8]</u>									
<u>05h</u>	<u>Command</u>	<u>5Eh</u>								

The TRUSTED_PROTOCOLSECURITY_PROTOCOL field identifies which ~~trusted protocol~~security protocol is being used. This determines the format of the data that is transferred. (see Table 2)

Table 2 – TRUSTED SEND - TRUSTED_PROTOCOLSECURITY_PROTOCOL field description

<u>Value</u>	<u>Description</u>
<u>00h</u>	<u>Reserved</u>
<u>01h – 06h</u>	Reserved for <u>Defined by TCG.</u>
<u>07h – Efh</u>	<u>Reserved.</u>
<u>F0h – FFh</u>	<u>Vendor Specific</u>

The TRANSFER_LENGTH field contains the number of 512-byte increments 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 for the TRANSFER_LENGTH field is specifies that no data transfer shall take place, and shall not be considered to be an error.

The SP_SPECIFIC TP_SPECIFIC1 and TP_SPECIFIC2 parameters field provides TRUSTED_PROTOCOL SECURITY_PROTOCOL field specific information. The meaning of this field is defined by each ~~trusted protocol~~security protocol.

- **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]

2.5.62.5.5 TRUSTED SEND DMA – 5Fh, DMA data-out

- **Feature Set**

This command is ~~optional~~ 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**

Table 3 - TRUSTED SEND DMA command parameters

<u>Word</u>	<u>Name</u>	<u>Description</u>								
<u>00h</u>	<u>Feature</u>	<table border="0"> <thead> <tr> <th><u>Bit</u></th> <th><u>Description</u></th> </tr> </thead> <tbody> <tr> <td><u>15:8</u></td> <td><u>Reserved</u></td> </tr> <tr> <td><u>7:0</u></td> <td><u>SECURITY_PROTOCOL (See Table 2)</u></td> </tr> </tbody> </table>	<u>Bit</u>	<u>Description</u>	<u>15:8</u>	<u>Reserved</u>	<u>7:0</u>	<u>SECURITY_PROTOCOL (See Table 2)</u>		
<u>Bit</u>	<u>Description</u>									
<u>15:8</u>	<u>Reserved</u>									
<u>7:0</u>	<u>SECURITY_PROTOCOL (See Table 2)</u>									
<u>01h</u>	<u>Count</u>	<table border="0"> <thead> <tr> <th><u>Bit</u></th> <th><u>Description</u></th> </tr> </thead> <tbody> <tr> <td><u>15:8</u></td> <td><u>Reserved</u></td> </tr> <tr> <td><u>7:0</u></td> <td><u>TRANSFER_LENGTH [7:0]</u></td> </tr> </tbody> </table>	<u>Bit</u>	<u>Description</u>	<u>15:8</u>	<u>Reserved</u>	<u>7:0</u>	<u>TRANSFER_LENGTH [7:0]</u>		
<u>Bit</u>	<u>Description</u>									
<u>15:8</u>	<u>Reserved</u>									
<u>7:0</u>	<u>TRANSFER_LENGTH [7:0]</u>									
<u>02h-04h</u>	<u>LBA</u>	<table border="0"> <thead> <tr> <th><u>Bit</u></th> <th><u>Description</u></th> </tr> </thead> <tbody> <tr> <td><u>47:24</u></td> <td><u>Reserved</u></td> </tr> <tr> <td><u>23:8</u></td> <td><u>SP_SPECIFIC</u></td> </tr> <tr> <td><u>7:0</u></td> <td><u>TRANSFER_LENGTH [15:8]</u></td> </tr> </tbody> </table>	<u>Bit</u>	<u>Description</u>	<u>47:24</u>	<u>Reserved</u>	<u>23:8</u>	<u>SP_SPECIFIC</u>	<u>7:0</u>	<u>TRANSFER_LENGTH [15:8]</u>
<u>Bit</u>	<u>Description</u>									
<u>47:24</u>	<u>Reserved</u>									
<u>23:8</u>	<u>SP_SPECIFIC</u>									
<u>7:0</u>	<u>TRANSFER_LENGTH [15:8]</u>									
<u>05h</u>	<u>Command</u>	<u>5Fh</u>								

- **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]

2.5.72.5.6 TRUSTED RECEIVE – 5Ch, PIO data-in

- **Feature Set**

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

- **Description**

The TRUSTED RECEIVE command is used to retrieve ~~trusted protocol~~ security protocol information (see 2.5.6.12-5.7.4) or the results from one or more TRUSTED SEND commands.

~~Any linkage between a previous TRUSTED SEND command and the data returned by a TRUSTED RECEIVE command is TRUSTED_PROTOCOL field specific. If the device has no data to transfer (e.g. the results for any previous TRUSTED SEND command commands are not yet available), the device may return TRUSTED_PROTOCOL field specific data indicating it has no other data to return. The command shall be completed with normal status, unless a transport protocol failure (e.g. CRC error) occurs.~~

~~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 5). 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 5).~~

~~For TRUSTED_PROTOCOL SECURITY_PROTOCOL field set to 00h, the format of the data is described in 2.5.6.12-5.7.4. The format of the data for other TRUSTED_PROTOCOL SECURITY_PROTOCOL values is documented by the group that owns the associated TRUSTED_PROTOCOL 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 TRUSTED_PROTOCOL SECURITY_PROTOCOL field (see Table 5) specific rules for the TRUSTED RECEIVE command;~~
- ~~b) any hard reset; or~~
- ~~c) power-on reset; or~~
- ~~d) loss of communication with the host that sent the TRUSTED SEND command.~~

~~If the data is lost due to one of these events and the host still wants to perform the TRUSTED_PROTOCOL SECURITY_PROTOCOL specific instruction, the host may have to send a new TRUSTED SEND command.~~

- Inputs

Table 4 - TRUSTED RECEIVE command parameters

<u>Word</u>	<u>Name</u>	<u>Description</u>								
00h	Feature	<table border="1"> <thead> <tr> <th><u>Bit</u></th> <th><u>Description</u></th> </tr> </thead> <tbody> <tr> <td>15:8</td> <td>Reserved</td> </tr> <tr> <td>7:0</td> <td>SECURITY_PROTOCOL (See Table 5.)</td> </tr> </tbody> </table>	<u>Bit</u>	<u>Description</u>	15:8	Reserved	7:0	SECURITY_PROTOCOL (See Table 5.)		
<u>Bit</u>	<u>Description</u>									
15:8	Reserved									
7:0	SECURITY_PROTOCOL (See Table 5.)									
01h	Count	<table border="1"> <thead> <tr> <th><u>Bit</u></th> <th><u>Description</u></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>	<u>Bit</u>	<u>Description</u>	15:8	Reserved	7:0	TRANSFER_LENGTH [7:0]		
<u>Bit</u>	<u>Description</u>									
15:8	Reserved									
7:0	TRANSFER_LENGTH [7:0]									
02h-04h	LBA	<table border="1"> <thead> <tr> <th><u>Bit</u></th> <th><u>Description</u></th> </tr> </thead> <tbody> <tr> <td>47:24</td> <td>Reserved</td> </tr> <tr> <td>23:8</td> <td>SP_SPECIFIC</td> </tr> <tr> <td>7:0</td> <td>TRANSFER_LENGTH [15:8]</td> </tr> </tbody> </table>	<u>Bit</u>	<u>Description</u>	47:24	Reserved	23:8	SP_SPECIFIC	7:0	TRANSFER_LENGTH [15:8]
<u>Bit</u>	<u>Description</u>									
47:24	Reserved									
23:8	SP_SPECIFIC									
7:0	TRANSFER_LENGTH [15:8]									
05h	Command	5Ch								

The TRUSTED_PROTOCOLSECURITY_PROTOCOL field identifies which ~~trusted protocol~~ security protocol is being used. This determines the format of the data that is transferred (see Table 5).

Table 5 – TRUSTED RECEIVE - TRUSTED_PROTOCOLSECURITY_PROTOCOL field description

<u>Value</u>	<u>Description</u>
00h	Return trusted protocol security protocol information (see <u>2.5.6.12.5.7.4</u>)
01h – 06h	Reserved for TCG.
07h – Efh	Reserved.
F0h – FFh	Vendor Specific

The SP_SPECIFICTP_SPECIFIC1 and TP_SPECIFIC2 parameters field provides TRUSTED_PROTOCOLSECURITY_PROTOCOL field specific information. The meaning of these fields are defined by each ~~trusted protocol~~ security protocol.

The ALLOCATION_LENGTHTRANSFER_LENGTH field contains the ~~maximum~~ number of 512-byte increments of data to be transferred. (One means 512 bytes, two means 1024 bytes, etc.) Pad bytes are appended by the device as needed to meet this requirement. Pad bytes shall have a value of 00h.

If the allocation length is not sufficient to return all of the data bytes the device has available to transfer, the device shall transfer as many bytes as possible consistent with the requirements of the specified TRUSTED_PROTOCOLSECURITY_PROTOCOL field without exceeding the allocation length, and shall be completed with normal status. Indications of data overrun or underrun or the mechanism, if any, for processing retries are TRUSTED_PROTOCOLSECURITY_PROTOCOL-specific.

An ~~allocation length~~ TRANSFER_LENGTH value of zero specifies that no data shall be transferred. This condition shall not be considered an error.

- 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]

2.5.7.12.5.6.1 TRUSTED_PROTOCOL_SECURITY_PROTOCOL 00h Description

The purpose of TRUSTED_PROTOCOL_SECURITY_PROTOCOL 00h is to return the security identification credential for the device. A TRUSTED RECEIVE using TRUSTED_PROTOCOL_SECURITY_PROTOCOL field set to 00h is not linked to an earlier TRUSTED SEND command. When the TRUSTED_PROTOCOL_SECURITY_PROTOCOL field is set to 00h, the TP_SPECIFIC_SP_SPECIFIC fields are shown in Table 6.

Table 6 – SECURITY_PROTOCOL 00h - SP_SPECIFIC field descriptions

SP_SPECIFIC	Description	Reference	Support
0000h	Return supported security protocol list	2.5.6.22-5.7.2	Mandatory
0001h	Return a certificate	2.5.6.32-5.7.3	Mandatory
0002h – FFFFh	Reserved.		

If the SP_SPECIFIC_TP_SPECIFIC1 or TP_SPECIFIC2 fields are is set to a reserved value, the command shall be aborted.

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

2.5.6.2 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 7.

Table 7 – TRUSTED RECEIVE parameter data for SP_SPECIFIC=0000h

Bit	7	6	5	4	3	2	1	0	
Byte 0	RESERVED								
1	RESERVED								
2	RESERVED								
3	RESERVED								
4	RESERVED								
5	RESERVED								
6	(MSB)	LIST length (M – 7)							
7								(LSB)	
8	SUPPORTED SECURITY_PROTOCOL LIST								
M									
M+1									
N	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 conform to the TRANSFER_LENGTH field requirements (i.e. the total data length shall be a multiple of 512 bytes). Pad bytes are appended as needed to meet this requirement. Pad bytes shall have a value of 00h.

2.5.7.3.2.5.6.3 Certificate data description

2.5.7.3.2.5.6.3.1 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 TRUSTED_PROTOCOL_SECURITY_PROTOCOL field of the TRUSTED RECEIVE command is set to 00h, and SP_SPECIFIC_TP_SPECIFIC1 is 00h and TP_SPECIFIC2 is 0001h, the parameter data shall have the format shown in Table 8.

Table 8 – TRUSTED RECEIVE parameter data for TP_SPECIFIC SP_SPECIFIC=0001h

Bit	7	6	5	4	3	2	1	0	
0	RESERVED								
1	RESERVED								
2	(MSB)	CERTIFICATE LENGTH (M – 3)							
3								(LSB)	
4	X.509 certificate bytes								
M									
M+1									
N	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 2.5.6.3.2.2.5.7.3.2 and 2.5.6.3.2.5.7.3.3.

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

2.5.7.3.2.5.6.3.2 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. ~~describes the trusted command usage of the X.509 public key certificate fields and the relationship of that usage to the definitions of RFC 3280.~~

Table -- Usage of X.509 certificate values in RFC 3280 context

Certificate Field [1]	Details
SignatureAlgorithm	As described in RFC 3280.
SignatureValue	As described in RFC 3280.
Version	Shall be set to 2 (i.e. version 3).
SerialNumber	As described in RFC 3280.
Signature	As described in RFC 3280.
Issuer	As described in RFC 3280 with the added constraint that UTF8String encoding of DirectoryString shall be used.
Validity	As described in RFC 3280. It is recommended to set Begin Date to the time of credential issuance and the Expiration Date to the Begin Date plus one hundred years if the intent is not to indicate an expiration date.
Subject	As described in RFC 3280. Information contained in this field shall either be populated with a non-empty distinguished name identifying the device or a null value.
SubjectPublicKeyInfo	As described in RFC 3280.
subject Alternate Name Extension	As described in RFC 3280, but may be ignored. This specification restricts the use to the following options only: -otherName; -directoryName. One and only one of the following values is allowed for subjectAltName: -The device serial number using directoryName; -The device serial number using otherName. If this field is used then subject field shall contain a null value.
basicConstraints Extension	As described in RFC 3280.
cRLDistributionPoints Extension	As described in RFC 3280.
subjectDirectoryAttributes Extension: _____ protocols	Sequence of OIDs
[1] Certificate field names are as described in RFC 3280.	

2.5.7.3.32.5.6.3.3 Attribute certificate description

RFC 3281 defines the certificate syntax for certificates consistent with X.509v2 Attribute Certificate Specification. -describes the trusted command usage of the X.509 attribute certificate fields and the relationship of that usage to the definitions of RFC 3281. Any further restrictions beyond the requirements of RFC 3281 are TBD.

Table — Usage of X.509 certificate values in RFC 3281 context

Certificate Field [1]	Details
SignatureAlgorithm	As described in RFC 3281.
SignatureValue	As described in RFC 3281.
Version	Shall be set to 1 (i.e. version 2).
Holder	As described in RFC 3281 with the added constraint that entityName option be used in the Holder field containing one and only one of the of the following values: —an URI using uniformResourceIdentifier; —the device serial number using directoryName or otherName; —a null value.
Issuer	As described in RFC 3281.
Signature	As described in RFC 3281.
SerialNumber	As described in RFC 3281.
AttrCertValidityPeriod	As described in RFC 3281. It is recommended to set Begin Date to the time of credential issuance and the Expiration Date to the Begin Date plus one hundred years if the intent is not to indicate an expiration date.
attributes: ——— protocols	SEQUENCE OF OID Defines supported Security and Integrity Protocols.
basicAttConstraints Extension	As described in RFC 3281.
eRLDistributionPoints Extension	As described in RFC 3281.
[1] Certificate field names are as described in RFC 3281.	

2.5.82.5.7 TRUSTED RECEIVE DMA – 5Dh, DMA data-in

- **Feature Set**

This command is ~~optional~~ 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**

Table 11 - TRUSTED RECEIVE DMA command parameters

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

- **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]