TrustedFlash Security System Mapping for SCSI

To: T10 Technical Committee
From: Dave Landsman
SanDisk Corporation
601 McCarthy Blvd
Milpitas, CA
Phone: 206.275.4385
Email: Dave.Landsman@SanDisk.com
Date: **October 30, 2008**

To enable the use of the SPC4 SECURITY PROTOCOL IN and SECURITY PROTOCOL OUT commands as the transport for TrustedFlash commands, for example in applications such as USB card readers, SanDisk has drafted Appendix A (SCSI and ATA Transport Adaptation) to the TrustedFlash spec.

We are providing the TrustedFlash Appendix A in this document, as an informational update for the T10 committee. Please refer to the SCSI-relevant sections.

The TrustedFlash specification, including Annex A, is available to members of the Secure Digital Card Association (SDA - www.sdcard.org), where TrustedFlash is a supported Security System under the Advanced Security SD (ASSD) specification, with a corresponding ASSD protocol ID.

APPENDIX A

SCSI AND ATA TRANSPORT ADAPTATION

1. Overview

This appendix specifies the SCSI and ATA transport layer specific adaptations. These type of transport layers are intended for PC based applications where the flash memory card is interfaced to the host via SCSI or ATA based interface adaptors.

2. References

SBC–3 : SCSI-3 Block Commands (INCITS/T10 Published, Project: 0996-M http://www.t10.org }
SPC-4 : SCSI Primary Commands - 4 (INCITS/T10 Development, Project: 1731-D http://www.t10.org }
ATA8-ACS : AT Attachment 8 - ATA/ATAPI Command Set (INCITS/T13 Development, Project 1600-D http://www.t13.org)

3. SCSI Transport

When a SCSI Transport is employed to communicate with the TrustedFlash enabled flash memory device, using the INCITS/T10 SBC-3 and SPC-4 protocols, then the TrustedFlash commands and the resulting responses shall be carried to and from the device by means of the SECURITY PROTOCOL OUT and SECURITY PROTOCOL IN commands defined in SPC-4 respectively, serving as transparent conduits. The SCSI operation sequence, addressing and error handling shall be identical to the proper (mass)storage related SBC-3 READ and WRITE commands, the difference is that while the READ and WRITE commands transfer storage (sector, LBA) data, the SECURITY PROTOCOL OUT and SECURITY PROTOCOL IN commands transfer the TrustedFlash command blocks and TrustedFlash response buffers.

In order to probe whether a device supports the TrustedFlash Security Protocol, a SECURITY PROTOCOL IN command shall be executed with Security Protocol 00h, as described in paragraph 7.6.1 in SPC-4.

The following tables define the TrustedFlash specific implementation of the SECURITY PROTOCOL OUT and SECURITY PROTOCOL IN CDBs:

Table A-1 — TrustedFlash SECURITY PROTOCOL OUT CDB

Bit / Byte	7	6	5	4	3	2	1	0
0	OPERATION CODE = B5h							
1	SECURITY_PROTOCOL for TrustedFlash = EDh							
2	RESERVED							
3	RESERVED							
4	INC_512=1	RESERVED						
5	RESERVED							
6	(MSB)	TRANSFER_LENGTH (IN 512 BYTE BLOCKS)						
9								(LSB)
10	RESERVED							
11	CONTROL							

INC_512 and the use of optional pad bytes are defined in SCSI Primary Commands-4 [SPC4]. If optional pad bytes are used all such bytes shall have a value of zero (0).
Reserved Bytes and Bits shall be set to zero (0).
The Control Field is defined in The SCSI Architecture Model-4 [SAM4], shall be identical to the values used by the storage READ and WRITE commands..

Table A-2 — TrustedFlash SECURITY PROTOCOL IN CDB

Bit / Byte	7	6	5	4	3	2	1	0
0	OPERATION CODE = A2h							
1	SECURITY_PROTOCOL for TrustedFlash = EDh							
2	RESERVED							
3	RESERVED							
4	INC_512=1	RESERVED						
5	RESERVED							
6	(MSB)	TRANSFER_LENGTH (IN 512 BYTE BLOCKS)						
9								(LSB)
10	RESERVED							
11	CONTROL							

INC_512 and the use of optional pad bytes are defined in SCSI Primary Commands-4 [SPC4]. If optional pad bytes are used all such bytes shall have a value of zero (0).
Reserved Bytes and Bits shall be set to zero (0).
The Control Field is defined in The SCSI Architecture Model-4 [SAM4], shall be identical to the values used by the storage READ and WRITE commands..

4. ATA Transport

When an ATA Transport (either parallel or serial) is employed to communicate with the TrustedFlash enabled flash memory device, using the INCITS/T13 ATA8-ACS protocols, then the TrustedFlash commands and the resulting responses shall be carried to and from the device by means of the TRUSTED SEND and TRUSTED RECEIVE commands defined as part of the ATA8-ACS Trusted Computing feature set, serving as transparent conduits. The

ATA operation sequence, addressing and error handling shall be identical to the proper (mass)storage related ATA8-ACS General Feature set commands (in particular: WRITE BUFFER/WRITE DMA/WRITE MULTIPLE and READ BUFFER/READ DMA/READ MULTIPLE), the main difference is that while the READ and WRITE commands transfer storage (sector, LBA) data, the TRUSTED SEND and TRUSTED RECEIVE commands transfer the TrustedFlash command blocks and TrustedFlash response buffers.

In order to probe whether a device supports the TrustedFlash Security Protocol, a TRUSTED RECEIVE command shall be executed with Security Protocol 00h, as described in paragraph 7.57.6 Security Protocol 00h Description of ATA8-ACS.

The following tables define the TrustedFlash specific implementation of the TRUSTED SEND and TRUSTED RECEIVE commands (using the format of the ATA8-ACS)

Table A-3. TRUSTED SEND COMMAND

Name	**Description**
Feature	Security Protocol, for TrustedFlash EDh[1]
Count	Transfer Length (7:0)
LBA	**Bit Description** 27:24 Reserved 23:8 Reserved 7:0 Transfer Length (15:8) - See 7.59.3.4
Device	**Bit Description** 7 Obsolete 6 N/A 5 Obsolete 4 Transport Dependent, defined in paragraph 6.2.11 of the (ATA8-ACS) 3:0 Reserved
Command	7:0 5Eh for **PIO Data-Out** 5Fh for **DMA**

Reserved and Obsolete fields must be filled with zeroes (00h).

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). Pad bytes are appended to the valid data as needed to meet this requirement.

Pad bytes shall have a value of 00h. A transfer length of zero is invalid.

[1] The Security Protocol value of EDh had been requested, but not yet granted by INCITS/T13. The same value had been assigned by INCITS/T10

Table A-4 TRUSTED RECEIVE

Name	Description
Feature	Security Protocol, for TrustedFlash EDh[2]
Count	Transfer Length (7:0)
LBA	**Bit Description** 27:24 Reserved 23:8 Reserved 7:0 Transfer Length (15:8) - See 7.59.3.4
Device	**Bit Description** 7 Obsolete 6 N/A 5 Obsolete 4 Transport Dependent, defined in paragraph 6.2.11 of the (ATA8-ACS) 3:0 Reserved
Command	7:0 5Ch for **PIO Data-In** 5Dh for **DMA**

Reserved and Obsolete fields must be filled with zeroes (00h).

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). Pad bytes are appended to the valid data as needed to meet this requirement.
Pad bytes shall have a value of 00h. A transfer length of zero is invalid.

[2] The Security Protocol value of EDh had been requested, but not yet granted by INCITS/T13. The same value had been assigned by INCITS/T10