To: **T10 Committee**
From: **Gerry Houlder, Seagate Technology,** gerry_houlder@seagate.com
Developed for **Trusted Computing Group**, www.trustedcomputinggroup.org
Represented by **Steven Sletten, SUN Microsystems**, steven.sletten@sun.com
and **Mike Fitzpatrick, Fujitsu**, mfitzpatrick@fcpa.fujitsu.com
Subj: **SPC-3 Security Commands proposal**
Date: **June 21, 2004**

This document presents a strategy for defining an industry standard set of interface commands for a trusted device, which is a component of an overall trusted system.

A trusted device provides a horizontal security product embedded in devices whose behavior may be authorized via interaction with a trusted host system.

This proposal creates two commands: TRUSTED COMPUTING OUT and TRUSTED COMPUTING IN. These commands provide for variable length data transfers. We request two 12 byte CDBs to provide commonality between SCSI and ATAPI implementations. The SCSI commands proposed provide a data transfer length field of 4 bytes and expresses the data length as a number of bytes to be transferred.

The CDB parameters and data payload shall be defined by the Trusted Computing Group (TCG) in its Storage Systems Working Group. The subsequent actions resulting from these commands will also be defined by TCG. The intent is to standardize this data content so it is identical across both ATA and SCSI. This proposal refers to the data payload format as “restricted” to indicate that the format shall conform to their definition.

0.1 Definitions

0.1.a Security Action: A group of bytes that describe a security procedure that a device server is requested to perform.

0.1.b Security Information Group: A group of bytes that contain the results of a requested security action or the status from processing a requested security action.

1.1.1 Trusted Computing Out command

The TRUSTED COMPUTING OUT command (see table 1) is used to send trusted security information to the device server. The data sent contains one or more security actions to be performed by the device server. The application client shall use TRUSTED COMPUTING IN command to retrieve any results and status information resulting from the security actions.

Table 1 – Trusted Computing Out command

Bit / Byte	7	6	5	4	3	2	1	0
0	OPERATION CODE (B5h)							
1	RESERVED			RESTRICTED				
2	RESTRICTED							
3	RESTRICTED							
4	RESTRICTED							
5	RESTRICTED							
6	(MSB)							
7	PARAMETER LIST LENGTH							
8								
9								(LSB)
10	RESERVED							
11	CONTROL							

The PARAMETER LIST LENGTH field specifies the length in bytes of the trusted security parameters that shall be transferred from the application client to the device server. A parameter list length of zero indicates that no data shall be transferred, and that no security functions shall be performed. If the parameter list length violates the length requirements, then the device server shall return CHECK CONDITION status with the sense key set to ILLEGAL REQUEST and an additional sense code of INVALID FIELD IN CDB.

The device server shall return GOOD status as soon as it determines the data has been correctly received. This does not indicate that the data has been parsed or that any security actions have been processed. These indications are only obtained by sending a TRUSTED COMPUTING IN command and receiving the results in the associated data transfer.

Once a TRUSTED COMPUTING OUT command has been sent by an application client, at least one TRUSTED COMPUTING IN command shall be sent before it can send another TRUSTED COMPUTING OUT command.

The data is organized as one or more security actions. The format of the security action data is restricted.

1.1.2 Trusted Computing In command

The TRUSTED COMPUTING IN command (see table 2) is used to retrieve results and status of security actions that were sent in a previous TRUSTED COMPUTING OUT command.

Table 2 – Trusted Computing In command

Bit / Byte	7	6	5	4	3	2	1	0
0	OPERATION CODE (A2h)							
1	RESERVED			RESTRICTED				
2	RESTRICTED							
3	RESTRICTED							
4	RESTRICTED							
5	RESTRICTED							
6	(MSB)							
7	ALLOCATION LENGTH							
8								
9								(LSB)
10	RESERVED							
11	CONTROL							

The ALLOCATION LENGTH field is described in xxx. [Editor's note: reference to standard paragraph defining Allocation Length] If the length is not sufficient to return all of the bytes the device server has available to send, the device server shall send as many complete security information groups as possible without exceeding the allocation length. A partial security information group shall not be sent.

If the device server has no security information groups to send, the device server shall return a security information group indicating it has no data to return and the command shall end with GOOD status.

The returned data is organized as one or more security information groups. The format of the security information groups is restricted.

It is the application client's responsibility to have an outstanding TRUSTED COMPUTING IN command whenever it believes there are security information groups pending in the device server.