To: T10 Technical Committee
From: Jim Hatfield, Seagate (James.C.Hatfield@seagate.com),
Date: August 17, 2007
Subject: CAP- Update to SECURITY PROTOCOL IN

Revision History
Revision 0a (August 30, 2007)   First revision

Related Documents
SCSI Primary Commands-4 (SPC-4), revision 11

Overview
The SECURITY PROTOCOL IN command uses Protocol ID= 00h for the host to request certain information from the device about its security capabilities. This proposal adds the capability for the device server to return protocol specific information for an individual Protocol ID. This is very useful when a device server supports multiple security protocols.

Suggested Changes

6.29.2.2 CDB description
When the SECURITY PROTOCOL field is set to 00h in a SECURITY PROTOCOL IN command, the SECURITY PROTOCOL SPECIFIC field (see table 195) contains a single numeric value as defined in 3.5.

Table 195 — SECURITY PROTOCOL SPECIFIC field for SECURITY PROTOCOL IN protocol 00h

SP_Specific	Description	Support	Reference
0000h	Supported security protocol list	Mandatory	6.29.2.3
0001h	Certificate data	Mandatory	6.29.2.4
0002h- 8000h	Reserved		
8001h-80FFh	Security properties for a specific security protocol	Security protocol specific	6.29.2.5
8100h-FFFFh	Reserved		
0002h-FFFFh	Reserved		

All other CDB fields for SECURITY PROTOCOL IN command shall meet the requirements stated in 6.29.1.

Each time a SECURITY PROTOCOL IN command with the SECURITY PROTOCOL field set to 00h is received, the device server shall transfer the data defined 6.29.2 starting with byte 0.

6.29.2.5 Security Properties for a specific Security Protocol

When SECURITY PROTOCOl is set to 00h, and SECURITY PROTOCOL SPECIFIC is set to a value in the range of 8001h – 80FFh, and the device server supports protocol xx

> where: xx = SP_Specific – 8000h

the returned parameter data shall have the format shown in Table 1; otherwise, the device server shall return CHECK CONDITION status, ABORTED COMMAND sense key, and INVALID FIELD IN CDB sense code.

Table 1 – SECURITY PROTOCOL IN parameter data for SECURITY PROTOCOL=00, SECURITY PROTOCOL SPECIFIC = 80xxh

Bit Byte	7	6	5	4	3	2	1	0
0	Length (N)							
1								
2								
3								
4	Device security properties for SecurityProtocol xx							
…								
N-1								

The Length field contains the total length of the data returned, including the Length field.

After the Length field, the data returned shall describe the security protocol-specific device server security properties for security protocol xx.