memorandum

Hewlett-Packard Company
3000 Hanover Street
Palo Alto, CA 94304-1185
USA
www.hp.com

T10/07-361r1

To	**From**	**Subject**	**Date**
INCITS T10 Committee	Curtis Ballard, HP Michael Banther, HP	SSC-3 Out of Band Encryption Key Management	15 September, 2007

Revision History

Revision 0 – Initial document.

Revision 1 – Too many changes to list full details
Changes from feedback before September 07, T10 meetings
Significant editorial changes
Changed several check condition values to DATA PROTECT
Clarified new concept of data encryption capabilities
Modified disabled and split into disabled and prevented as different concepts
Added top level indication of algorithms prevented into data encryption status page
Added indicator of encryption parameters configuration source to data encryption status page

Related Documents

ssc3r03d – SCSI Stream Commands

spc4r11 – SCSI Primary Commands

Background

Discussion in working groups has brought up the issue of methods for encryption key management by devices outside the scope of this standard and a working item on the ADC-3 proposal is "Automation control of encryption performed by data transfer device." Any method for providing data encryption control parameters to a tape device that does not use the existing SECURITY PROTOCOL IN and SECURITY PROTOCOL OUT commands over a primary port will have side effects on the SSC device server including the possibility of key management contention between applications using a primary port and applications using an alternate out of band method for data encryption parameters management.

If data encryption parameters are controlled by an out of band device the data encryption capabilities of the drive may be altered and a method is needed to report that an encryption algorithm is supported but not available. This proposal provides a method for reporting when individual encryption protocols have been disabled. Key management contention may be prevented by disabling support of all encryption protocols over the primary port.

This proposal also provides a model for error condition reporting and recovery when encryption is controlled by an out of band mechanism.

In the proposed changes that follow, new text appears in blue or purple, deleted text appears in ~~red strikeout~~, and editorial comments appear in green.

Proposed Changes to SSC-3

New definition 3.1.14. Existing definitions shift down.

3.1.14 data encryption capabilities: A set of capabilities in the physical device that determine the values reported through a SECURITY PROTOCOL IN command specifying the Tape Data Encryption security protocol and any of the supported pages (see 4.2.21.9).

New definition 3.1.25. Existing definitions shift down.

3.1.25 external data encryption control: A capability of the physical device that allows control of the data encryption parameters and the data encryption capabilities through an external interface (e.g. ADC or a management interface).

4.2.3 Physical Device

Add data encryption parameters and data encryption capabilities to list of items in physical device in figure 8.

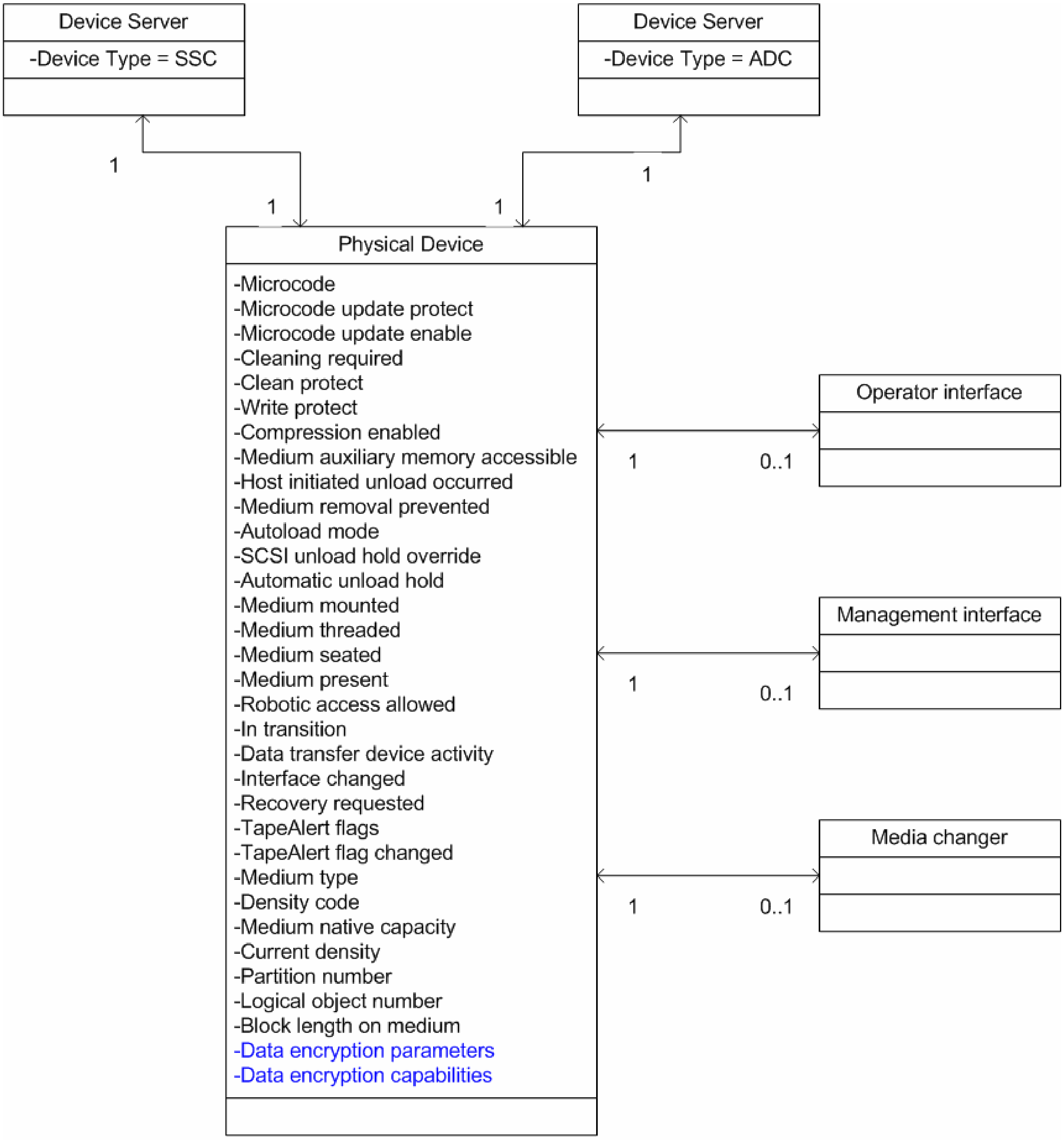

Figure 8 — UML example of SCSI target device and physical device

Add data encryption parameters to table 2.

Table 2 specifies the standard that defines each attribute shown in figure 8.

Table 2 – Physical device attributes

Attribute	Reference
Microcode	SPC-4
Microcode update protect	ADC-2
Microcode update enable	ADC-2
Cleaning required	ADC-2
Clean protect	ADC-2
Write protect	ADC-2
Compression enabled	ADC-2
Medium auxiliary memory accessible	ADC-2
Host initiated unload occurred	ADC-2
Medium removal prevented	ADC-2
Autoload mode	SPC-4
SCSI unload hold override	ADC-2
Automatic unload hold	ADC-2
Medium mounted	ADC-2
Medium threaded	ADC-2
Medium seated	ADC-2
Medium present	ADC-2
Robotic access allowed	ADC-2
In transition	ADC-2
Data transfer device activity	ADC-2
Interface changed	ADC-2
Recovery requested	ADC-2
TapeAlert flags	table 10
TapeAlert flag changed	ADC-2
Medium type	7.8.4
Density code	8.2.4.3
Medium native capacity[a]	7.8.3
Current density	ADC-2
Partition number	7.6.3
Logical object number	7.6.3
Block length on medium	SPC-4
Data encryption parameters	4.2.21.8
Data encryption capabilities	4.2.22.2

a) Medium native capacity is the value reported in the CAPACITY field of the density support data block descriptor when the MEDIA bit is one, and a SET CAPACITY command has not been used to affect the capacity of the medium.

New model clause section 4.2.21.9. Existing clauses shift down.

4.2.21.9 Data encryption capabilities

A physical device that supports data encryption shall have a set of data encryption capabilities. The data encryption capabilities determine the values reported through a SECURITY PROTOCOL IN command specifying the Tape Data Encryption security protocol and any of the supported pages.

The data encryption capabilities include supported:

a) key scopes;
b) encryption modes;
c) supplemental decryption keys;
d) algorithms;
e) CKOD values;
f) CKORL values;
g) CKORP values;
h) U-KAD length;
i) A-KAD length;
j) M-KAD length;
k) raw decryption mode disable settings;
l) check external encryption mode settings;
m) other vendor specific data encryption capabilities.

New model clause section 4.2.22. Existing clause 4.2.22 shifts down to become 4.2.23:

4.2.22 External data encryption control

4.2.22.1 External data encryption control overview

A physical device that supports data encryption may support external data encryption control and provide the ability for an external entity to configure data encryption capabilities or data encryption parameters using an external interface not specified by this standard (e.g. ADC or a management interface). The external entity may be capable of changing the device server's data encryption capabilities and may be capable of providing data encryption parameters.

4.2.22.2 External data encryption control of data encryption capabilities

External data encryption control may change the data encryption capabilities of the physical device that are reported in response to a SECURITY PROTOCOL IN command (see SPC-4) specifying the Tape Data Encryption security protocol and any of the supported pages.

If external data encryption control changes any of the data encryption capabilities of the physical device, then the device server shall establish a unit attention condition with the additional sense data of DATA ENCRYPTION CAPABILITIES CHANGED for all I_T nexus that have their registered for encryption unit attentions state set to one (see 4.2.20.7).

Comment: DATA ENCRYPTION CAPABILITIES CHANGED is a new ASC/ASCQ.

4.2.22.2.1 External data encryption control of encryption algorithm support

External data encryption control may change the device server encryption algorithm support by:

a) disabling a supported encryption algorithm;
b) preventing SSC device server control of data encryption parameters for a supported algorithm; or
c) preventing SSC device server control of data encryption parameters for all supported algorithms.

If external data encryption control has disabled a supported encryption algorithm or has prevented SSC device server control of data encryption parameters for a supported encryption algorithm, then the device server shall:

a) remove the encryption algorithm from the list of supported encryption algorithms returned in the Data Encryption Capabilities page; or
b) report the encryption algorithm in the list of supported encryption algorithms returned in the Data Encryption Capabilities page.

If external data encryption control has disabled a supported encryption algorithm, then the physical device shall not accept data encryption parameters for that algorithm, and the device server shall return a Data Encryption Algorithm descriptor for the disabled encryption algorithm with the DISABLED bit set to one in response to a SECURITY PROTOCOL IN command specifying the Tape Data Encryption security protocol and the Data Encryption Capabilities page.

If external data encryption control has prevented SSC device server control of data encryption parameters for a supported encryption algorithm and a Data Encryption Algorithm descriptor is returned in response to a SECURITY PROTOCOL IN command specifying the Tape Data Encryption security protocol and the Data Encryption Capabilities page for the encryption algorithm, then the device server shall set:

a) the DECRYPT_C field in the Data Encryption Algorithm descriptor to 3 (i.e., the physical device has the ability to decrypt data using this algorithm but control of the data encryption parameters by the addressed logical unit is prevented) (see 8.5.3.2); and

b) the ENCRYPT_C field in the Data Encryption Algorithm descriptor for the restricted encryption algorithm to 3 (i.e., the physical device has the ability to encrypt data using this algorithm but control of the data encryption parameters by the addressed logical unit is prevented).

If external data encryption control has prevented SSC device server control of data encryption parameters for a supported encryption algorithm, then the device server shall terminate a SECURITY PROTOCOL OUT command specifying the Tape Data Encryption security protocol and a Set Data Encryption page that has the algorithm specified in the ALGORITHM INDEX field with CHECK CONDITION STATUS, with the sense key set to ILLEGAL REQUEST, and the additional sense code set to DATA ENCRYPTION CONFIGURATION PREVENTED.

Comment: DATA ENCRYPTION CONFIGURATION PREVENTED is a new ASC/ASCQ.

Note: If external data encryption control has prevented SSC device server control of any of the data encryption parameters, the data encryption parameters may be controlled by a device outside the scope of this standard. The encryption status may be read using the SECURITY PROTOCOL OUT command specifying the Tape Data Encryption security protocol and the Data Encryption Status page.

4.2.22.2.2 External data encryption control of other data encryption capabilities

If external data encryption control configures data encryption capabilities other than the supported encryption algorithms, the new capabilities shall be reported in response to a SECURITY PROTOCOL IN command specifying the Tape Data Encryption security protocol and the page containing the modified capability.

4.2.22.3 External data encryption control of data encryption parameters

External data encryption control of data encryption parameters may result in changes to the encryption status which may be detected using the SECURITY PROTOCOL IN COMMAND and the Data Encryption Status page.

If external data encryption control is used to configure the data encryption parameters for a supported encryption algorithm, then the device server shall:

a) set the CFG_P field (see 8.2.5.4) in the Data Encryption Capabilities page to 010b (i.e., The device server shall not allow data encryption parameters to be established for any supported encryption algorithm via the I_T nexus associated with the SECURITY PROTOCOL IN command that requested this page); and
b) terminate a SECURITY PROTOCOL OUT command specifying the Tape Data Encryption security protocol and a Set Data Encryption page with CHECK CONDITION STATUS, with the sense key set to ILLEGAL REQUEST, and the additional sense code set to DATA ENCRYPTION CONFIGURATION PREVENTED.

If external data encryption control is used to configure the data encryption parameters for a supported encryption algorithm, then the device server shall not process any data when processing of a READ(6), READ(16), READ REVERSE(6), READ

REVERSE(16), RECOVER BUFFERED DATA, VERIFY(6), VERIFY(16), WRITE(6), WRITE(16), or ERASE command until the external data encryption control data encryption parameters lookup process has completed. The external data encryption control data encryption parameters lookup process is beyond the scope of this standard.

4.2.22.4 External data encryption control error conditions

If external data encryption control is being used to control the data encryption parameters and the external data encryption control system returns an error, then the device server shall:

a) terminate a WRITE(6), WRITE(16), READ(6), READ(16), READ REVERSE(6), READ REVERSE(16), RECOVER BUFFERED DATA, VERIFY(6) or VERIFY(16) command with CHECK CONDITION status, with the sense key set to DATA PROTECT, and the additional sense code set to EXTERNAL DATA ENCRYPTION CONTROL ERROR; and
b) respond to a SECURITY PROTOCOL IN command specifying the Tape Data Encryption security protocol and the Data Encryption Status page with the ENCRYPTION MODE field set to 03h (i.e. PROHIBIT ENCRYPT) and with the DECRYPTION MODE field set to 04h (i.e. PROHIBIT DECRYPT).

Comment: EXTERNAL DATA ENCRYPTION CONTROL ERROR is a new additional sense code. It may be useful to define multiple ASC/ASCQ combinations that can be returned so different error conditions such as failure to access the key manager, key manager reported an error, or media does not support encryption may be returned.

If external data encryption control is being used to control the data encryption parameters and the external data encryption control process does not complete before a vendor specified timeout period, then the device server shall terminate a WRITE(6), WRITE(16), READ(6), READ(16), READ REVERSE(6), READ REVERSE(16), RECOVER BUFFERED DATA, VERIFY(6) or VERIFY(16) command with CHECK CONDITION status, with the sense key set to DATA PROTECT, and the additional sense code set to EXTERNAL DATA ENCRYPTION CONTROL TIMEOUT.

Comment: EXTERNAL DATA ENCRYPTION CONTROL TIMEOUT is a new additional sense code.

Comment: No text specific to abort is provided as it appears that abort handling to be normal from the SSC device server perspective.

Changes to clause 8.5.2.4:

8.2.5.4 Data Encryption Capabilities page

Table 98 specifies the format of the Data Encryption Capabilities page.

Table 98 – Data Encryption Capabilities page

Bit Byte	7	6	5	4	3	2	1	0
0	(MSB)	PAGE CODE (0010h)						
1								(LSB)
2	(MSB)	PAGE LENGTH (n-3)						
3								(LSB)
4	Reserved					CFG_P		
5	Reserved							
19								
Data Encryption Algorithm descriptor list								
20	Data Encryption Algorithm descriptor (first)							
	Data Encryption Algorithm descriptor (last)							
n								

See SPC-4 for a description of the PAGE LENGTH field.

The configuration prevented (CFG_P) field (see table y) specifies the data encryption parameters configuration capabilities for the I_T nexus associated with the SECRUITY PROTOCOL IN command that requested this page.

Table y – CFG_P field values

CODE	Description
000b	The data encryption parameters configuration capabilities are not reported
001b	The device server shall not allow data encryption parameters to be established for at least one supported encryption algorithm via the I_T nexus associated with the SECURITY PROTOCOL IN command that requested this page.
010b	The device server shall not allow data encryption parameters to be established for any supported encryption algorithm via the I_T nexus associated with the SECURITY PROTOCOL IN command that requested this page.
011b	The device server may allow data encryption parameters to be established via the I_T nexus associated with the SECURITY PROTOCOL IN command that requested this page.
111b	Reserved

Note: If the configuration of data encryption parameters is prevented, the data encryption parameters may be controlled by external data encryption control. The external data encryption control status may be read using the SECURITY PROTOCOL IN command specifying the Tape Data Encryption security protocol and the Data Encryption Status page.

Each Data Encryption Algorithm descriptor (see table 99) contains information about a data encryption algorithm supported by the device server. If more than one descriptor is included, they shall be sorted in ascending order of the value in the ALGORITHM INDEX field.

Table 99 -- Data Encryption Algorithm descriptor

Bit Byte	7	6	5	4	3	2	1	0
0	ALGORITHM INDEX							
1	Reserved							
2	(MSB)	DESCRIPTOR LENGTH (20)						
3								(LSB)
4	AVFMV	SDK_C	MAC_C	DED_C	DECRYPT_C		ENCRYPT_C	
5	AVFCLP		NONCE_C		Reserved	DISABLED	UKADF	AKADF
6	(MSB)	MAXIMUM UNAUTHENTICATED KEY-ASSOCIATED DATA BYTES						
7								(LSB)
8	(MSB)	MAXIMUM AUTHENTICATED KEY-ASSOCIATED DATA BYTES						
9								(LSB)
10	(MSB)	KEY SIZE						
11								(LSB)
12	Reserved				RDMC_C			EAREM
13	(MSB)	Reserved						
19								(LSB)
20	(MSB)	SECURITY ALGORITHM CODE						
23								(LSB)

Comment: fields that are not changed are not repeated here.

The DECRYPT_C field (see table 100) specifies the decryption capabilities of the device server.

Table 100 – DECRYPT_C field values

CODE	Description
0	The ~~device server~~ physical device has no data decryption capability using this algorithm.
1	The ~~device server~~ physical device has the ability to decrypt data using this algorithm in software.
2	The ~~device server~~ physical device has the ability to decrypt data using this algorithm in hardware.
3	The physical device has the ability to decrypt data using this algorithm but control of the data encryption parameters by the addressed logical unit is prevented.

The ENCRYPT_C field (see table 101) specifies the data encryption capabilities of the device server.

Table 101 – ENCRYPT_C field value

CODE	Description
0	The ~~device server~~ physical device has no data encryption capability using this algorithm.
1	The ~~device server~~ physical device has the ability to encrypt data using this algorithm in software.
2	The ~~device server~~ physical device has the ability to encrypt data using this algorithm in hardware.
3	The physical device has the ability to encrypt data using this algorithm but control of the data encryption parameters by the addressed logical unit is prevented.

The DISABLED bit shall be set to one if the specified encryption algorithm has been disabled (See 4.2.22.3). The DISABLED bit shall be set to zero if the specified encryption algorithm has not been disabled.

Changes to clause 8.5.2.7:

8.5.2.7 Data Encryption Status page

Table 107 specifies the format of the Data Encryption Status page.

Table 107 –– Data Encryption Status page

Bit Byte	7	6	5	4	3	2	1	0
0	(MSB)	PAGE CODE (0020h)						
1								(LSB)
2	(MSB)	PAGE LENGTH (n-3)						
3								(LSB)
4	I_T NEXUS SCOPE			Reserved		KEY SCOPE		
5	ENCRYPTION MODE							
6	DECRYPTION MODE							
7	ALGORITHM INDEX							
8	(MSB)	KEY INSTANCE COUNTER						
11								(LSB)
12	Reserved		PARAMETERS CONTROL			CEEMS		RDMD
13	Reserved							
23								
24	KEY-ASSOCIATED DATA DESCRIPTORS LIST							
n								

Comment: Fields that are not changed are not repeated here.

The PARAMETERS CONTROL field contains information on how the data encryption parameters were set. Table y+2 shows the values of the PARAMETERS CONTROL field.

Table y+2 – PARAMETERS CONTROL field values

CODE	Description
000b	Data encryption parameters source is not reported
001b	Data encryption parameters were configured using a primary port.
010b	Data encryption parameters were configured using an ADI port.
011b	Data encryption parameters were configured using a management interface.
100b-111b	Reserved

Comment: Fields could be added to describe the current state if in an error state and those could report the same values as a command on the primary interface. That would consume quite a bit of space so I haven't added those fields since the CHECK CONDITION on the primary interface would have already reported the condition and defining multiple additional sense codes could remove the need for detailed additional information.

Changes to clause 8.5.3.1:

8.5.3.1 SECURITY PROTOCOL OUT command specifying Tape Data Encryption security protocol overview

Comment: Only table 114 is changed so the rest of the text is not repeated here

The SECURITY PROTOCOL SPECIFIC field (see table 114) specified the type of page that the application client is sending.

Table 114 – SECURITY PROTOCOL SPECIFIC field values

CODE	Description	Reference
0000h—000Fh	Reserved	
0010h	Set Data Encryption page	8.5.3.2
0011h	SA Encapsulation page	8.5.3.3~~2~~
0012h—~~FEFFh~~001Fh	Reserved	
0030h—003Fh	Restricted	
0040h—FEFFh	Reserved	
FF00h—FFFFh	Vendor Specific	

Changes to clause 8.5.3.2:

8.5.3.2 Set Data Encryption page

Table 110 specifies the format of the Set Data Encryption page.

Table 110 -- Set Data Encryption page

Bit Byte	7	6	5	4	3	2	1	0
0	(MSB)	PAGE CODE (0010h)						
1								(LSB)
2	(MSB)	PAGE LENGTH (m-3)						
3								(LSB)
4	SCOPE			Reserved				LOCK
5	Reserved				SDK	CKOD	CKORP	CKORL
6	ENCRYPTION MODE							
7	DECRYPTION MODE							
8	ALGORITHM INDEX							
9	KEY FORMAT							
10	Reserved							
17								
18	(MSB)	KEY LENGTH (n-19)						
19								(LSB)
20	KEY							
N								
n +1	KEY-ASSOCIATED DATA DESCRIPTOR LIST							
M								

Comment: Only the ENCRYPTION MODE and DECRYPTION MODE fields and one paragraph following those fields are modified by this proposal so the text describing the other fields is not repeated here.

Table 112 specifies the values for the ENCRYPTION MODE field.

Table 112 – ENCRYPTION MODE field values

Code	Name	Description	In SECURITY PROTOCOL OUT parameter data	In SECURITY PROTOCOL IN parameter data
00h	DISABLE	Data encryption is disabled.	valid	valid
01h	EXTERNAL	The data associated with the WRITE(6) and WRITE(16) commands has been encrypted by a system that is compatible with the algorithm specified by the ALGORITHM INDEX field.	valid	valid
02h	ENCRYPT	The device server shall encrypt all data that it receives for a WRITE(6) or WRITE(16) command using the algorithm specified in the ALGORITHM INDEX field and the key specified in the KEY field.	valid	valid
03h	LOCKED	The device server shall terminate the a WRITE(6), WRITE(16), or ERASE command with CHECK CONDITION status, with the sense key set to DATA PROTECT and the additional sense code set to EXTERNAL DATA ENCRYPTION CONTROL ERROR.	invalid	valid
04~~3~~h-0Fh		Reserved		

Table 113 specifies the values for the DECRYPTION MODE field. See 4.2.20.3 for configuration and exception condition requirements.

Table 113 –DECRYPTION MODE field values

Code	Name	Description	In SECURITY PROTOCOL OUT parameter data	In SECURITY PROTOCOL IN parameter data
00h	DISABLE	Data encryption is disabled. If the device server encounters an encrypted logical block while reading, it shall not allow access to the data.	valid	valid
01h	RAW	Data decryption is disabled. If the device server encounters an encrypted logical block while reading, it shall pass the encrypted block to the host without decrypting it. The enctypted block may contain data that is not user data.	valid	valid

Table 113 –DECRYPTION MODE field values (Continued)

Code	Name	Description	In SECURITY PROTOCOL OUT parameter data	In SECURITY PROTOCOL IN parameter data
02h	DECRYPT	The device server shall decrypt all data that is read from the medium when processing a READ(6), READ(16), READ REVERSE(6), READ REVERSE(16), or RECOVER BUFFERED DATA command or verified when processing a VERIFY(6) or VERIFY(16) command. The data shall be decrypted using the algorithm specified in the ALGORITHM INDEX field and the key specified in the KEY field.	valid	valid
03h	MIXED	The device server shall decrypt all data that is read from the medium when processing a READ(6), READ(16), READ REVERSE(6), READ REVERSE(16), or RECOVER BUFFERED DATA command or verified when processing a VERIFY(6) or VERIFY(16) command. The data shall be decrypted using the algorithm specified in the ALGORITHM INDEX field and the key specified in the KEY field. If the device server encounters unencrypted data when processing a READ(6), READ(16), READ REVERSE(6), READ REVERSE(16), RECOVER BUFFERED DATA, VERIFY(6) or VERIFY(16) command, the data shall be processed without decrypting.	valid	valid
04h	LOCKED	The device server shall terminate a READ(6), READ(16), READ REVERSE(6), READ REVERSE(16), RECOVER BUFFERED DATA, VERIFY(6) or VERIFY(16) command with CHECK CONDITION status, with the sense key set to DATA PROTECT, and the additional sense code set to EXTERNAL DATA ENCRYPTION CONTROL ERROR.	invalid	valid
05~~4~~h- 0Fh		Reserved		

Comment: An additional sense code value for CRYTOGRAPHIC KEY UNAVAILABLE does not yet exist.

If the device server is not capable of distinguishing encrypted blocks from unencrypted blocks using the algorithm specified in the ALGORITHM INDEX field and the DECRYPTION MODE field is set to MIXED, the device server shall terminate the command with CHECK CONDITION status, with the sense key set to ILLEGAL REQUEST, and the additional sense code set to INVALID FIELD IN PARAMETER DATA.

If the ENCRYPTION MODE field is set to ENCRYPT and the KEY LENGTH field is set to zero, the device server shall terminate the command with CHECK CONDITION status, with the sense key set to ILLEGAL REQUEST, and the additional sense code set to INVALID FIELD IN PARAMETER DATA.

If the ENCRYPTION MODE field is set to ENCRYPT or EXTERNAL and the ENCRYPT_C field in the data algorithm descriptor for the specified encryption algorithm index in the data encryption capabilities page is set to 03h, then the device server shall terminate the command with CHECK CONDITION STATUS, with the sense key set to ILLEGAL REQUEST, the additional sense code set to INVALID FIELD IN PARAMETER LIST, and the sense key specific FIELD POINTER field set to the ENCRYPTION MODE field.

If the DECRYPTION MODE field is set to DECRYPT or MIXED and the KEY LENGTHfield is set to zero, the device server shall terminate the command with CHECK CONDITION status, with the sense key set to ILLEGAL REQUEST, and the additional sense code set to INVALID FIELD IN PARAMETER DATA.

If the DECRYPTION MODE field is set to DECRYPT, RAW or MIXED and the DECRYPT_C field in the data algorithm descriptor for the specified encryption algorithm index in the data encryption capabilities page is set to 03h, then the device server shall terminate the command with CHECK CONDITION STATUS, with the sense key set to ILLEGAL REQUEST, the additional sense code set to INVALID FIELD IN PARAMETER LIST, and the sense key specific FIELD POINTER field set to the DECRYPTION MODE field.