memorandum

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

T10/07-361r0

To	From	Subject	Date
INCITS T10 Committee	Curtis Ballard, HP Michael Banther, HP	SSC-3 Out of Band Encryption Key Management	28 August, 2007

Revision History

Revision 0 – Initial document.

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 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 encryption parameters management.

If encryption parameters are controlled by an out of band device the 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.

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

Proposed Changes to SSC-3

4.2.3 Physical Device

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

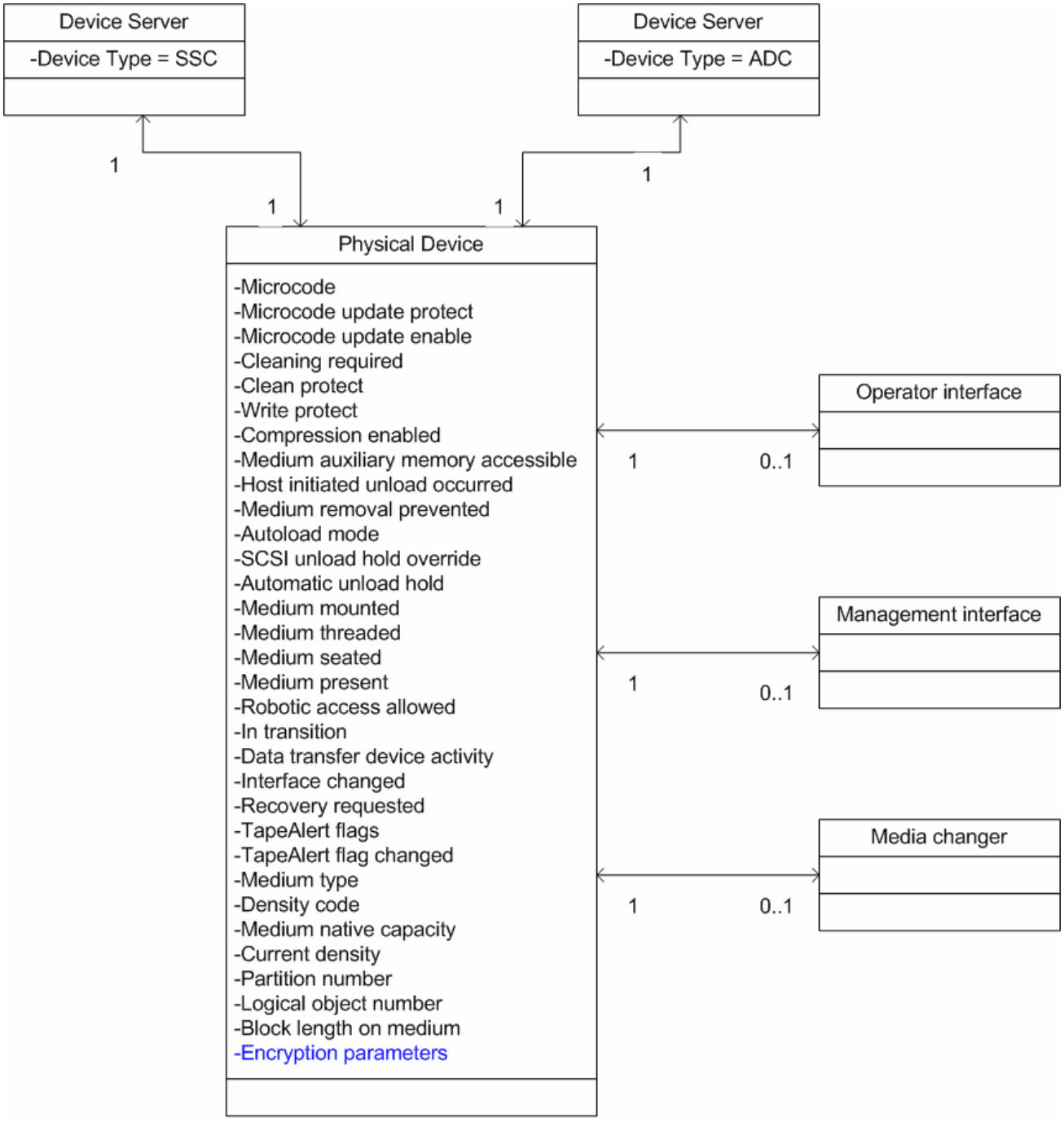

Figure 8 — UML example of SCSI target device and physical device

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

Add 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
Encryption parameters	4.2.20.8

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.

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

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

4.2.22 Encryption control by an entity beyond the scope of this standard

4.2.22.1 Encryption control by an entity beyond the scope of this standard overview

A physical device that supports data encryption may have the ability to configure encryption capabilities or receive encryption parameters from an entity using a mechanism beyond the scope of this standard (e.g. ADC or Management Interface). The encryption control mechanism may be capable of disabling SSC device server support for some or all encryption algorithms and may be capable of providing encryption parameters. Control of encryption capabilities or encryption parameters by an entity beyond the scope of this standard is called external encryption control.

4.2.22.2 External encryption control of encryption capabilities

External encryption control may change the capabilities of the physical device that are reported in a SECURITY PROTOCOL IN command specifying the Tape Data Encryption security protocol and the Data Encryption Capabilities page, Supported Key Formats page, Data Encryption Management Capabilities page, or Device Server Key Wrapping Public Key page.

If external encryption control changes any of the encryption capabilities of the physical device, then the device server should establish a unit attention condition with the additional sense 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.

If a supported encryption algorithm has been disabled for decryption by external encryption control, then the device server shall respond to a SECURITY PROTOCOL IN command specifying the tape data encryption protocol and the data encryption capabilities page with:

a) data algorithm descriptors for the disabled encryption algorithm with the DECRYPT_C field set to 3 (i.e. the device server has the ability to decrypt data using this algorithm but the data decryption capabilities are disabled) (see 8.5.3.2); or
b) no descriptors for the disabled encryption algorithms.

If a supported encryption algorithm has been disabled for encryption by external encryption control, then the device server should respond to a SECURITY PROTOCOL IN command specifying the tape data encryption protocol and the data encryption capabilities page with:

a) a data algorithm descriptor for the disabled encryption algorithm with the ENCRYPT_C field set to 3 (i.e. the device server has the ability to encrypt data using this algorithm but the data encryption capabilities are disabled) (see 8.5.3.2); or
b) no descriptors for the disabled encryption algorithms.

Comment: In most environments it would be useful to be able to report that a particular capability is under control of an external device however it is possible the some environments may wish to completely hide disabled algorithms so the above statements allow both behaviors.

If an encryption algorithm has been disabled, and a data algorithm descriptor for the disabled algorithm is returned in response to a SECURITY PROTOCOL IN command specifying the tape data encryption protocol and the data encryption capabilities page, then the device server shall disable support for receiving encryption parameters for the disabled algorithm and shall terminate the a SECURITY PROTOCOL OUT command specifying the Tape Data Encryption protocol and the Set Data Encryption page with CHECK CONDITION STATUS with the sense key set to ILLEGAL REQUEST, and the additional sense code set to INVALID FIELD IN CDB.

4.2.22.3 External encryption control of encryption parameters

If the encryption parameters are defined by external encryption control then the physical device should disable SSC device server support for receiving encryption parameters by disabling all supported encryption algorithms.

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

If SSC device server support for receiving encryption parameters is disabled, then the device server shall report all encryption algorithms as disabled by responding to a SECURITY PROTOCOL IN command specifying the tape data encryption protocol and the data encryption capabilities page with a data algorithm descriptor for all encryption algorithm indicies with the DECRYPT_C field set to 3 (i.e. the device server has the ability to decrypt data using this algorithm but the data decryption capabilities are disabled) and the ENCRYPT_C field set to 3 (i.e. the device server has the ability to encrypt data using this algorithm but the data encryption capabilities are disabled).

4.2.22.4 Error Conditions

4.2.22.4.1 Encryption control errors

If external encryption control is being used and an error condition occurs, the physical device shall enter an encryption error state. The physical device shall enter an encryption error state if:

a) the physical device is not able to retrieve a write key as part of the processing of a WRITE(6), WRITE(16), or ERASE command;

b) the physical device is not able to retrieve a read key as part of the processing of a READ(6), READ(16), READ REVERSE(6), READ REVERSE(16), RECOVER BUFFERED DATA, VERIFY(6) or VERIFY(16) command;

c) a volume is mounted that does not support data encryption using the algorithm specified by the algorithm index in the data encryption parameters; or

d) other vendor-specific events

If the physical device is in an encryption error state, the device server shall 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).

If the physical device is in an encryption error state the device server shall terminate a WRITE(6) or WRITE(16) command with CHECK CONDITION status, with the sense key set to ILLEGAL REQUEST, and the additional sense code set to CRYPTOGRAPHIC KEY UNAVAILABLE and 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 ILLEGAL REQUEST, and the additional sense code set to CRYPTOGRAPHIC KEY UNAVAILABLE.

Comment: 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.

An encryption error state shall be cleared on a command that causes a reposition of the media or an unload.

Note: If the physical device is not able to retrieve a write key or read key for the next block following a reposition the physical device may transition right back into the error state.

4.2.22.4.2 Task Management interaction

If the a command requiring a key is being processed and the external encryption control has not provided a key when the command is aborted, the physical device may discard encryption parameters received following the abort.

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.

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

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				
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.

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	Reserved		NONCE_C		Reserved			
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	(MSB)			Reserved				
19								(LSB)
20	(MSB)			SECURITY ALGORITHM CODE				
23								(LSB)

Comment: there are no changes proposed to any fields except for the DECRYPT_C field and the ENCRYPT_C field so none of the other fields are repeated here.

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

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 the data decryption capabilities are disabled.

The ENCRYPT_C field (see table 101) specifies the 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 the data encryption capabilities are disabled.

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.

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

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.

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

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	PROHIBIT ENCRYPT	The device server shall terminate a WRITE(6), WRITE(16), or WRITE FILEMARKS command with CHECK CONDITION status, with the sense key set to ILLEGAL REQUEST, and the additional sense code set to CRYPTOGRAPHIC KEY UNAVAILABLE.	invalid	valid
04~~3~~h-0Fh		Reserved		

If the ENCRYPTION MODE field in the parameter data of a SECURITY PROTOCOL OUT command is set to PROHIBIT ENCRYPT, 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.

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

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

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	PROHIBIT DECRYPT	The device server shall not decrypt data that is read from the medium when processing a READ(6), READ(16), READ REVERSE(6), READ REVERSE(16), RECOVER BUFFERED DATA command or verified when processing a VERIFY(6) or VERIFY(16) command. 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 ILLEGAL REQUEST, and the additional sense code set to CRYPTOGRAPHIC KEY UNAVAILABLE.	invalid	valid
054h-0Fh		Reserved		

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

If the DECRYPTION MODE field in the parameter data of a SECURITY PROTOCOL OUT command is set to PROHIBIT DECRYPT, 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 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.

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

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 3, the device server shall terminate the command with CHECK CONDITION STATUS, 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 3, the device server shall terminate the command with CHECK CONDITION STATUS, 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.