memorandum

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

T10/07-164r0

To	From	Subject	Date
INCITS T10 Committee	Curtis Ballard, HP Michael Banther, HP	Resolve ADC-2 Letter Ballot Comment IBM-49	2 May, 2007

Revision History
Revision 0 – Initial document.

Related Documents

adc2r07c – Automation/Drive Interface Commands

ssc3r03b – SCSI Stream Commands

Background

ADC-2 letter ballot comments IBM-49 and Dell-100 both have commented that the documentation regarding the expected use of the VS bit in the VHF data is not sufficiently clear and HP was asked to bring in a proposal to help clarify their usage of this bit.

The VS bit was intended to provide a location where a drive could report information relating to the encryption capabilities and status in the VHF data. The automation device would be required to read a log page or issue other commands such as a SECURITY PROTOCOL IN command to determine what event had caused a change in encryption parameters.

During the investigation into the use cases for additional VHF data relating to encryption it has become obvious that full library integration will require not only a method for the drive to notify the library of the encryption events but also some method for the library to control some of the encryption capabilities in the drive. Part of that control is already possible with the SECURITY PROTOCOL IN and SECURITY PROTOCOL OUT commands but no method exists to allow a library to configure the encryption support in the drive. Drives may be capable of supporting multiple modes of encryption and the library device may need the ability to control what modes of encryption are supported in a given configuration for purposes of enhanced security or capability licensing.

This proposal will provide a specification for how the VS bit should be used to indicate an event beyond the list of events defined in the VHF data and a specification for the library to configure the encryption capabilities of the drive.

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

Changes to clause 8.5.2.4:

8.5.2.4 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				
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 has no data decryption capability using this algorithm.
1	The device server has the ability to decrypt data using this algorithm in software.
2	The device server has the ability to decrypt data using this algorithm in hardware.
3	The device server 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 has no data encryption capability using this algorithm.
1	The device server has the ability to encrypt data using this algorithm in software.
2	The device server has the ability to encrypt data using this algorithm in hardware.
3	The device server 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.

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 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 not encrypt data that it receives for a WRITE(6) or WRITE(16) command and shall terminate a WRITE(6) or WRITE(16) command (See ADC-2)	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
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

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
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 it 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. (See ADC-2)	invalid	valid
054h-0Fh		Reserved		

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

Proposed Changes to ADC-2

Modifications to 6.1.2:

6.1.2 DT Device Status log page

6.1.2.1 DT Device Status log page overview

The DT Device Status log page (see table 14) defines log information pertaining to the DT device and DT device primary ports.

Table 14 – DT Device Status log page

Bit / Byte	7	6	5	4	3	2	1	0
0	Reserved		PAGE CODE (11h)					
1	Reserved							
2	(MSB)		PAGE LENGTH (n-3)					
3								(LSB)
4	DT Device Status log parameters							
5								

See SPC-3 for a description of the PAGE CODE field and PAGE LENGTH field.

Table 15 defines the DT Device Status log page parameter codes.

Table 15 – DT Device Status log page parameter codes

Parameter code	Description	Reference
0000h	Very high frequency data	6.1.2.2
0001h	Very high frequency polling delay	6.1.2.3
0002h	Extended high frequency data	6.1.2.4
0002~~3~~h-00FFh	Reserved	
100h	Obsolete	
0101h – 0200h	DT device primary port status	6.1.2.~~4~~5
201h	Key management error data	6.1.2.6
020~~1~~2h – 7FFFh	Reserved	
8000h – FFFFh	Vendor specific	

6.1.2.2 Very high frequency data log parameter

The very high frequency data log parameter format is shown in table 16.

Table 16 – Very high frequency data log parameter format

Bit / Byte	7	6	5	4	3	2	1	0
0	(MSB)		PARAMETER CODE (0000h)					
1								(LSB)
2	DU (0)	DS (1)	TSD (0)	ETC (0)	TMC (00)		LBIN (1)	LP (1)
3	PARAMETER LENGTH (04h)							
4	VHF data descriptor							
7								

The PARAMETER CODE field shall be set to 0000h to indicate the very high frequency data log parameter.

See SPC-3 for descriptions of the DU bit, DS bit, TSD bit, ETC bit, TMC field, LBIN bit, and LP bit. These bits and fields shall be set to the values shown in table 16.

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

The PARAMETER LENGTH field shall be set to 04h.

The VHF data descriptor is defined in table 17.

Table 17 – VHF data descriptor

Bit / Byte	7	6	5	4	3	2	1	0
0	PAMR	HIU	MACC	CMPR	WRTP	CRQST	CRQRD	DINIT
1	INXTN	Rsvd	RAA	MPRSNT	Rsvd	MSTD	MTHRD	MOUNTED
2	DT DEVICE ACTIVITY							
3	EXTD~~VS~~	Reserved				RRQST	INTFC	TAFC

Comment: Only the VS bit is redefined by this proposal so the text describing the other fields is not repeated here.

~~NOTE 7 When the VS bit is set to one, vendor-specific log parameters may appear in a standard log page (e.g., the vendor-specific parameters in the Error Counter log pages, see SPC-3) or in a vendor-specific log page. If the device includes an ADT port (see ADT-2) the application client may be able to retrieve vendor-specific log parameters using the vendor-specific protocol of ADT-2.~~

When the EXTD bit is set to one, additional high frequency log data may be reported:

a) in the Extended high frequency data log page;

b) in vendor-specific log parameters appearing in a standard log page (e.g. the vendor-specific parameters in the Error Counter log pages, see SPC-3); or

c) in a vendor-specific log page.

When the EXTD bit is set to zero no additional high frequency log data is available.

6.1.2.3 Very high frequency polling delay log parameter

Comment: no changes to this sub-clause are proposed so it is not repeated here

6.1.2.4 Extended high frequency data log parameter

The extended high frequency data log parameter format is shown in table y.

Table y – Extended high frequency data log parameter format

Bit / Byte	7	6	5	4	3	2	1	0
0	(MSB)	PARAMETER CODE (0002h)						
1								(LSB)
2	DU (0)	DS (1)	TSD (0)	ETC (0)	TMC (00)		LBIN (1)	LP (1)
3	PARAMETER LENGTH (04h)							
4	EHF data descriptor							
7								

The PARAMETER CODE field shall be set to 0002h to indicate the extended high frequency data log parameter.

See SPC-3 for descriptions of the DU bit, DS bit, TSD bit, ETC bit, TMC field, LBIN bit, and LP bit. These bits and fields shall be set to the values shown in table 16.

The PARAMETER LENGTH field shall be set to 04h.

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

The EHF data descriptor is defined in table y+1.

Table y+1 – EHF data descriptor

Bit / Byte	7	6	5	4	3	2	1	0
0	Reserved							
1	WKR	RKR	KME	EKP	Reserved			
2	Reserved							
3	Reserved							

A write key request (WKR) bit set to one indicates that the device server requests a write encryption key from the automation application client. The RMC device server shall set the WKR bit to one:

a) upon an event which causes the device server to release the resources used to save the set of data encryption parameters (See SSC-3); or

b) as specified in the write key request policy (See 6.3.3.4).

A WKR bit set to zero indicates that the device server does not request a write encryption key from the automation application client. The device server shall set the WKR bit to zero when:

a) it receives a valid SECURITY PROTOCOL OUT command, with the SECURITY PROTOCOL field set to Tape Data Encryption and with the ENCRYPTION MODE field in a Set Data Encryption page set to DISABLE or ENCRYPT;

b) it receives a valid SECURITY PROTOCOL OUT command, with the SECURITY PROTOCOL field set to Data Encryption Configuration and with the PE bit in a Configure Encryption Policy page set to one; or

c) after a Key Request Period timeout (See 6.3.3.4).

A read key request (RKR) bit set to one indicates that the device server requests a read decryption key from the automation application client. The RMC device server shall set the RKR bit to one:

a) when a medium has been mounted; or

b) when the device server determines that the encryption key is not correct for an encrypted block (See SSC-3).

A RKR bit set to zero indicates that the device server does not request a read decryption key from the automation application client. The device server shall set the RKR bit to zero when:

a) it receives a valid SECURITY PROTOCOL OUT command, with the SECURITY PROTOCOL field set to Tape Data Encryption and with the DECRYPTION MODE field in a Set Data Encryption page set to DISABLE, DECRYPT or MIXED;

b) it receives a valid SECURITY PROTOCOL OUT command, with the SECURITY PROTOCOL field set to Data Encryption Configuration and with the PD bit in a Configure Encryption Policy page set to one; or

c) after a Key Request Period timeout (See 6.3.3.4).

A key management error (KME) bit set to one indicates that:

a) the device server has set the WKR bit to one and the automation application client has failed to send a SECURITY PROTOCOL OUT command with the SECURITY PROTOCOL field set to Tape Data Encryption and containing a Set Data Encryption page in the parameter data with the ENCRYPTION MODE field set to ENCRYPT within the Key Request Period (See 6.3.3.4);

b) the device server has set either the WKR bit to one or the RKR bit to one and the automation application client has failed to send a SECURITY PROTOCOL OUT command with the SECURITY PROTOCOL field set to Tape Data Encryption and containing a Set Data Encryption page in the parameter data with the DECRYPTION MODE field set to DECRYPT or MIXED within the Key Request Period; or

c) the DT device has detected a cryptographic error.

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

The device server shall set the KME bit to zero as part of the processing of a LOG SENSE command that reports the key management error data log parameter (see 6.1.2.6). A KME bit set to zero indicates that, since the most recently processed LOG SENSE command that reported the key management error log parameter or the most recent event resulting in a Logical Unit Reset condition:

a) the device server has set either the WKR bit to one or the RKR bit to one and the automation application client has sent a SECURITY PROTOCOL OUT command with the SECURITY PROTOCOL field set to Tape Data Encryption and containing a Set Data Encryption page in the parameter data within the Key Request Period (See 6.3.3.4);

b) the device server has not set the WKR bit or the RKR bit to one; and

c) the DT device has not detected a cryptographic error.

An encryption key present (EKP) bit set to one indicates that the RMC device server has a set of saved data encryption parameters associated with one or more I_T nexus with either the ENCRYPTION MODE field or the DECRYPTION MODE field set to a value other than DISABLE. An EKP bit set to zero indicates that the RMC device server does not have a set of saved data encryption parameters associated with any I_T nexus with either the ENCRYPTION MODE field or the DECRYPTION MODE field set to a value other than DISABLE.

6.1.2.5 ~~6.1.2.4~~ DT device primary port status log parameter(s)

Comment: no changes to this sub-clause are proposed so it is not repeated here

6.1.2.6 Key management error data log parameter

When the device server sets the KME bit in the extended high frequency parameter data to one, it shall record information pertaining to the error in the key management error data log parameter data. The automation application client may retrieve this parameter data to determine the nature of the last cryptographic error that caused the device server to set the KME bit to one. The key management error log parameter format is shown in table y+2.

Table y+2 – Key management error data log parameter

Bit / Byte	7	6	5	4	3	2	1	0
0	(MSB)			PARAMETER CODE (0201h)				
1								(LSB)
2	DU (0)	DS (1)	TSD (0)	ETC (0)	TMC (00)		LBIN (1)	LP (1)
3	PARAMETER LENGTH (08h)							
4	Cryptographic error descriptor							
11								

The PARAMETER CODE field shall be set to 0201h to indicate the key management error data log parameter.

See SPC-3 for descriptions of the DU bit, DS bit, TSD bit, ETC bit, TMC field, LBIN bit, and LP bit. These bits and fields shall be set to the values shown in table 16.

The PARAMETER LENGTH field shall be set to 08h.

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

The Cryptographic error descriptor is defined in table y+3.

Table y+3 – Cryptographic error descriptor

Bit / Byte	7	6	5	4	3	2	1	0
0	Reserved				KTO	ERROR TYPE		
1	Reserved							
3								
4	Reserved				SENSE KEY			
5	ADDITIONAL SENSE CODE							
6	ADDITIONAL SENSE CODE QUALIFIER							
7	Reserved							

A key timeout error (KTO) bit set to one indicates that the automation application client failed to send a SECURITY PROTOCOL OUT command with the SECURITY PROTOCOL field set to Tape Data Encryption and containing a Set Data Encryption page in the parameter data within the Key Request Period (See 6.3.3.4). A KTO bit set to zero indicates that the automation application client sent a SECURITY PROTOCOL OUT command with the SECURITY PROTOCOL field set to Tape Data Encryption and containing a Set Data Encryption page in the parameter data within the Key Request Period.

The ERROR TYPE field indicates the type of the last cryptographic error reported by the DT device. The error types defined for the cryptographic error descriptor are shown in table y+4.

Table y+4 – ERROR TYPE field value

CODE	Description
000b	No error
001b	Data encryption error
010b	Data decryption error
011b – 111b	Reserved

See SPC-3 for descriptions of the SENSE KEY field, ADDITIONAL SENSE CODE field, and ADDITIONAL SENSE CODE QUALIFIER field. The SENSE KEY field, ADDITIONAL SENSE CODE field, and ADDITIONAL SENSE CODE QUALIFIER field shall contain the sense key and additional sense code values that the RMC device server reported or shall report in the sense data to the application client for the most recent read operation or write operation that failed because of a cryptographic error.

The device server shall set the KTO bit and ERROR TYPE field to zero;

a) as part of the processing of a LOG SENSE command that reports the key management error data log parameter; or

b) due to an event resulting in a Logical Unit Reset condition.

If the ERROR TYPE field is set to zero, the KTO bit, SENSE KEY field, ADDITIONAL SENSE CODE field, and ADDITIONAL SENSE CODE QUALIFIER field shall be ignored.

New sub-clause 6.3:
(Note: existing sub-clause 6.3 shifts to become 6.4 with the addition of this new sub-clause)

6.3 Security protocol parameters

6.3.1 Security protocol overview

This subclause describes the protocols, pages, and descriptors used by automation/drive interface devices with the SECURITY PROTOCOL IN and SECURITY PROTOCOL OUT commands.

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

6.3.2 SECURITY PROTOCOL IN command specifying Tape Data Encryption security protocol

6.3.2.1 SECURITY PROTOCOL IN command specifying Tape Data Encryption security protocol overview

The SECURITY PROTOCOL IN command (see SPC-4) specifying Tape Data Encryption security protocol (i.e., 20h) requests the device server to return information about the data security methods in the device server and on the medium. The command supports a series of pages that are requested individually. An application client requests a page by using a SECURITY PROTOCOL IN command with the SECURITY PROTOCOL field set to Tape Data Encryption security protocol and the SECURITY PROTOCOL SPECIFIC field set to the page code requested.

A device server that supports the Tape Data Encryption protocol in the SECURITY PROTOCOL OUT command shall also support a SECURITY PROTOCOL IN command specifying the Tape Data Encryption protocol.

The SECURITY PROTOCOL SPECIFIC field (see table y+5) specifies the type of report that the application client is requesting.

Table y+5 – SECURITY PROTOCOL SPECIFIC field value

CODE	Description	Support	Reference
0000h	Tape Data Encryption In Support page	M	SSC-3
0001h	Tape Data Encryption Out Support page	M	SSC-3
0002 – 000Fh	Reserved		
0010h	Data Encryption Capabilities page		SSC-3
0011h	Supported Key Formats page		SSC-3
0012h	Data Encryption Management Capabilities page		SSC-3
0013h – 001Fh	Reserved		
0020h	Data Encryption Status page		SSC-3
0021h	Next Block Encryption Status page		SSC-3
0022h – FEFFh	Reserved		
FF00h – FFFFh	Vendor specific		
Support key: M – mandatory for device servers that support the Tape Data Encryption security protocol			

If the SECURITY PROTOCOL SPECIFIC field is set to a reserved or unsupported value, the ADC 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 CDB

6.3.3 SECURITY PROTOCOL IN command specifying Data Encryption Configuration security protocol

6.3.3.1 SECURITY PROTOCOL IN command specifying Data Encryption Configuration security protocol overview

The SECURITY PROTOCOL IN command (see SPC-4) specifying the Data Encryption Configuration security protocol (i.e. 21h) requests the device server to return information about the data security configuration methods in the device server. The command supports a series of pages that are requested individually. An application client requests a page by using a SECURITY PROTOCOL IN command with the SECURITY PROTOCOL field set to Data Encryption Configuration security protocol and the SECURITY PROTOCOL SPECIFIC field set to the page code requested.

A device server that supports the Data Encryption Configuration security protocol in the SECURITY PROTOCOL OUT command shall also support a SECURITY PROTOCOL IN command specifying the Data Encryption Configuration security protocol.

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

The security protocol specific field (see table y+6) specifies the type of report that the application client is requesting.

Table y+6 – SECURITY PROTOCOL SPECIFIC field value

CODE	Description	Support	Reference
0000h	Data Encryption Configuration In Support page	M	TBD
0001h	Data Encryption Configuration Out Support page	M	TBD
0002 – 000Fh	Reserved		
0010h	Report Data Encryption Policy page		TBD
0011h – FEFFh	Reserved		
FF00h – FFFFh	Vendor specific		
Support key: M – mandatory for device servers that support the Data Encryption Configuration security protocol			

If the SECURITY PROTOCOL SPECIFIC field is set to a reserved or unsupported value, the ADC 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 CDB.

The ALLOCATION LENGTH field specifies the maximum number of bytes that the device server may return (see SPC-3).

6.3.3.2 Data Encryption Configuration In Support page.

Table y+7 specifies the format of the Data Encryption Configuration In Support page.

Table y+7 – Data Encryption Configuration In Support page

Bit / Byte	7	6	5	4	3	2	1	0
0	(MSB)			PAGE CODE (0000h)				
1								(LSB)
2	(MSB)			PAGE LENGTH (n-3)				
3								(LSB)
Data Encryption Configuration In Support page code list								
4	Data Encryption Configuration In Support page code (first)							
5								
n-1	Data Encryption Configuration In Support page code (last)							
n								

The PAGE CODE field shall be set to 0000h to indicate the data encryption configuration in support page.

See SPC-3 for a description of the PAGE LENGTH field.

The Data Encryption Configuration In Support page code list shall contain a list of all of the pages that the device server supports for the SECURITY PROTOCOL IN command specifying the Data Encryption Configuration security protocol in ascending order beginning with page code 0000h.

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

6.3.3.3 Data Encryption Configuration Out Support page.

Table y+8 specifies the format of the Data Encryption Configuration Out Support page.

Table y+8 – Data Encryption Configuration Out Support page

Bit / Byte	7	6	5	4	3	2	1	0
0	(MSB)			PAGE CODE (0001h)				
1								(LSB)
2	(MSB)			PAGE LENGTH (n-3)				
3								(LSB)
Data Encryption Configuration Out Support page code list								
4	Data Encryption Configuration Out Support page code (first)							
5								
n-1	Data Encryption Configuration Out Support page code (last)							
n								

The PAGE CODE field shall be set to 0001h to indicate the data encryption configuration out support page.

See SPC-3 for a description of the PAGE LENGTH field.

The Data Encryption Configuration Out Support page code list shall contain a list of all of the pages that the device server supports for the SECURITY PROTOCOL OUT command specifying the Data Encryption Configuration security protocol in ascending order.

6.3.3.4 Report Data Encryption Policy page.

Table y+9 specifies the format of the Report Data Encryption Policy page.

Table y+9 – Report Data Encryption Policy page

Bit / Byte	7	6	5	4	3	2	1	0
0	(MSB)			PAGE CODE (0010h)				
1								(LSB)
2	(MSB)			PAGE LENGTH (8)				
3								(LSB)
4	(MSB)			DATA ENCRYPTION POLICY CONFIGURATION LOGICAL UNIT				
5								(LSB)
6	PE	PD	Reserved			WRITE KEY REQUEST POLICY		
7	Reserved							
8	(MSB)			KEY REQUEST PERIOD				
9								(LSB)
10	Reserved							
11								

The Report Data Encryption Policy page indicates the current encryption policy configuration for the RMC logical unit.

The PAGE CODE field shall be set to 0010h to indicate the data encryption policy page.

See SPC-3 for a description of the PAGE LENGTH field.

The DATA ENCRYPTION POLICY CONFIGURATION LOGICAL UNIT field shall contain the logical unit number for the logical unit that last sent a SECURITY PROTOCOL OUT command specifying the Data Encryption Configuration security protocol and the Configure

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

Encryption Policy page with the CFG bit set to one (See 6.3.5.3). The DATA ENCRYPTION POLICY CONFIGURATION LOGICAL UNIT field shall be set to the RMC logical unit upon:

a) an event that causes a hard reset condition; or

b) successful completion of a SECURITY PROTOCOL OUT command specifying the Data Encryption Configuration security protocol and the Configure Encryption Policy page with the CFG bit set to zero.

A prohibit encrypt (PE) bit set to one shall indicate that data encryption is prohibited. A PE bit set to zero shall indicate that data encryption is not prohibited. When the PE bit is set to one, the RMC device server shall terminate a write type command with CHECK CONDITION status, the sense key set to DATA PROTECT, the additional sense code set to CRYPTOGRAPHIC KEY UNAVAILABLE.

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

A prohibit decrypt (PD) bit set to one shall indicate that data decryption is prohibited. A PD bit set to zero shall indicate that data decryption is not prohibited. When the PD bit is set to one, the RMC device server shall terminate a read type command with CHECK CONDITION status, the sense key set to DATA PROTECT, the additional sense code set to CRYPTOGRAPHIC KEY UNAVAILABLE.

The WRITE KEY REQUEST POLICY field indicates the policy the device server shall use for acquiring write encryption keys from the automation application client. The WRITE KEY REQUEST POLICY field shall be ignored when the data encryption policy configuration logical unit is set to the RMC logical unit. The write key request policy values are defined in table y+10.

Table y+10 – WRITE KEY REQUEST POLICY field values

Value	Policy
000b	Do not request write keys
001b	Request write key when the DT device processes a command that will perform a write operation following a command to reposition the media. The DT Device shall request a new write key after a space/locate/read or rewind operation.
010b	Request key once per mounted media. The DT Device shall request a write key before altering the media while processing the first write type command after the medium in mounted in the DT device and shall continue to use the key until the current media is un-mounted.
011b – 111b	Reserved

The KEY REQUEST PERIOD field indicates the maximum time, in 100 millisecond increments, the ADC device server shall wait after requesting a key (See 6.1.2.4) from the automation application client. A KEY REQUEST PERIOD field value of 0000h indicates the key request period shall be infinite. The KEY REQUEST PERIOD field shall be set to 0000h when the data encryption policy configuration logical unit is set to the RMC logical unit.

6.3.4 SECURITY PROTOCOL OUT command specifying Tape Data Encryption security protocol

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

The SECURITY PROTOCOL OUT command specifying the Tape Data Encryption security protocol (i.e. 20h) is used to configure the data security methods in the device server and on the medium. The command supports a series of pages that are sent individually. An application client requests to send a page by using a SECURITY PROTOCOL OUT command with the SECURITY PROTOCOL field set to Tape Data Encryption security protocol and the SECURITY PROTOCOL SPECIFIC field set to the page code requested.

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

The SECURITY PROTOCOL SPECIFIC field (see table y+11) specifies the type of page that the application client is sending.

Table y+11 – SECURITY PROTOCOL SPECIFIC field value

CODE	Description	Reference
0000h – 000Fh	Reserved	
0010h	Set Data Encryption page	SSC-3
0011h – FEFFh	Reserved	
FF00h – FFFFh	Vendor specific	

If the SECURITY PROTOCOL SPECIFIC field is set to a reserved or unsupported value, the ADC 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 CDB

6.3.5 SECURITY PROTOCOL OUT command specifying Data Encryption Configuration security protocol

6.3.5.1 SECURITY PROTOCOL OUT command specifying Data Encryption Configuration security protocol overview

The SECURITY PROTOCOL OUT command (see SPC-4) specifying the Data Encryption Configuration security protocol (i.e. 21h) is used to configure the data security methods in the RMC device server. The command supports a series of pages that are sent individually. An application client requests to send a page by using a SECURITY PROTOCOL OUT command with the SECURITY PROTOCOL field set to Data Encryption Configuration security protocol and the SECURITY PROTOCOL SPECIFIC field set to the page code requested.

The security protocol specific field (see table y+12) specifies the type of page that the application client is sending.

Table y+12 – SECURITY PROTOCOL SPECIFIC field value

CODE	Description	Reference
0000h – 000Fh	Reserved	
0010h	Configure Encryption Algorithm Support page	6.3.5.2
0011h	Configure Encryption Policy page	6.3.5.3
0011h – FEFFh	Reserved	
FF00h – FFFFh	Vendor specific	

If the SECURITY PROTOCOL SPECIFIC field is set to a reserved or unsupported value, the ADC 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 CDB.

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

6.3.5.2 Configure Encryption Algorithm Support page

Table y+13 specifies the format of the Configure Encryption Algorithm Support page.

Table y+13 – Configure Encryption Algorithm Support 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								
Encryption Algorithm Support descriptor list								
20	Encryption Algorithm Support descriptor (first)							
N	Encryption Algorithm Support descriptor (last)							

The PAGE CODE field shall be set to 0010h to indicate the configure encryption algorithm support page.

See SPC-3 for a description of the PAGE LENGTH field.

Each Encryption Algorithm Support descriptor (see table y+14) shall contain configuration settings for a data encryption algorithm supported by the RMC logical unit. If more than one descriptor is included, they shall be sorted in ascending order of the value in the ALGORITHM INDEX field. The Encryption Algorithm Support descriptor list may not contain all algorithms supported by the RMC logical unit and this shall not be considered an error.

If the RMC device server currently has a saved set of data encryption parameters associated with any I_T nexus the ADC device server shall terminate the command with CHECK CONDITION status and set the sense key to ILLEGAL REQUEST, the additional sense code to INVALID FIELD IN PARAMETER LIST, and the sense key specific FIELD POINTER field set to the PAGE CODE field.

Table y+14 – Encryption Algorithm Support descriptor

Bit / Byte	7	6	5	4	3	2	1	0
0	ALGORITHM INDEX							
1	Reserved							
2	(MSB)			DESCRIPTOR LENGTH (4)				
3								(LSB)
4	Reserved						DECRYPT_D	ENCRYPT_D
5	Reserved							
7								

The ALGORITHM INDEX field indicates which of the encryption algorithms reported by the SECURITY PROTOCOL IN command specifying the Tape Data Encryption protocol and the Data Encryption Capabilities pages shall be configured.

See SPC-3 for a description of the DESCRIPTORS LENGTH field.

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

The DECRYPT_D field (see table y+15) specifies the decryption configuration that the RMC device server shall apply for the specified algorithm index.

Table y+15 – DECRYPT_D field values

CODE	Description
0	The RMC device server shall enable decryption capabilities using this algorithm
1	The RMC device server shall disable decryption capabilities using this algorithm
2-3	Reserved

If the DECRYPT_D field is set to one, the ADC device server shall report a 0, 1, or 2 in the DECRYPT_C field in the Data Encryption Algorithm descriptor for the specified algorithm index in response to a SECURITY PROTOCOL IN command and the RMC device server shall:

a) report a 0 or 3 in the DECRYPT_C field in the Data Encryption Algorithm descriptor for the specified algorithm index in response to a SECURITY PROTOCOL IN command; and
b) terminate a SECURITY PROTOCOL OUT command specifying the Tape Data Encryption security protocol and the Set Data Encryption page that attempts to set a decryption mode other than DISABLE for the specified algorithm 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.

If the DECRYPT_D field is set to zero, the RMC device server shall report a 0, 1, or 2 in the DECRYPT_C field in the Data Encryption Algorithm descriptor for the specified algorithm index in response to a SECURITY PROTOCOL IN command and the ADC device server shall:

a) report a 0 or 3 in the DECRYPT_C field in the Data Encryption Algorithm descriptor for the specified algorithm index in response to a SECURITY PROTOCOL IN command; and
b) terminate a SECURITY PROTOCOL OUT command specifying the Tape Data Encryption security protocol and the Set Data Encryption page that attempts to set a decryption mode other than DISABLE for the specified algorithm 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.

The ENCRYPT_D field (see table y+16) specifies the encryption configuration that the RMC device server shall apply for the specified algorithm index.

Table y+16 – ENCRYPT_D field values

CODE	Description
0	The device server shall enable encryption capabilities using this algorithm
1	The device server shall disable encryption capabilities using this algorithm
2-3	Reserved

If the ENCRYPT_D field is set to one, the ADC device server shall report a 0, 1, or 2 in the ENCRYPT_C field in the Data Encryption Algorithm descriptor for the specified algorithm index in response to a SECURITY PROTOCOL IN command and the RMC device server shall:

a) report a 0 or 3 in the ENCRYPT_C field in the Data Encryption Algorithm descriptor for the specified algorithm index in response to a SECURITY PROTOCOL IN command; and
b) terminate a SECURITY PROTOCOL OUT command specifying the Tape Data Encryption security protocol and the Set Data Encryption page that attempts to set a encryption mode other than DISABLE for the specified algorithm 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.

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

If the ENCRYPT_D field is set to zero, the RMC device server shall report a 0, 1, or 2 in the ENCRYPT_C field in the Data Encryption Algorithm descriptor for the specified algorithm index in response to a SECURITY PROTOCOL IN command and the ADC device server shall:

a) report a 0 or 3 in the ENCRYPT_C field in the Data Encryption Algorithm descriptor for the specified algorithm index in response to a SECURITY PROTOCOL IN command; and
b) terminate a SECURITY PROTOCOL OUT command specifying the Tape Data Encryption security protocol and the Set Data Encryption page that attempts to set a encryption mode other than DISABLE for the specified algorithm 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.

The encryption algorithm configuration values shall terminate after:

a) any event that results in a hard reset condition; or
b) other vendor-specific events.

6.3.5.3 Configure Encryption Policy page

Table y+17 specifies the format of the Configure Encryption Policy page.

Table y+17 – Configure Encryption Policy page

Bit / Byte	7	6	5	4	3	2	1	0
0	(MSB)			PAGE CODE (0011h)				
1								(LSB)
2	(MSB)			PAGE LENGTH (8)				
3								(LSB)
4	Reserved							
5								
6	PE	PD	Reserved		CFG	WRITE KEY REQUEST POLICY		
7	Reserved							
8	(MSB)			KEY REQUEST PERIOD				
9								(LSB)
10	Reserved							
11								

The PAGE CODE field shall be set to 0011h to indicate the configure encryption policy page.

See SPC-3 for a description of the PAGE LENGTH field.

A configure (CFG) bit set to one indicates that the RMC logical unit shall use the data encryption policies specified by the PE bit, PD bit, WRITE KEY REQUEST POLICY field, and KEY REQUEST PERIOD field. A CFG bit set to zero indicates that the RMC logical unit shall revert to using default data encryption policies. When the CFG bit is set to zero, the PE bit, PD bit, WRITE KEY REQUEST POLICY field and KEY REQUEST PERIOD field shall be ignored.

See 6.3.2.4 for the definitions of the PE bit, PD bit, WRITE KEY REQUEST POLICY field and the KEY REQUEST PERIOD field.