memorandum

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

T10/07-164r4

To	**From**	**Subject**	**Date**
INCITS T10 Committee	Curtis Ballard, HP Michael Banther, HP	Automation Encryption Control	2 October, 2007

Revision History

Revision 0 – Initial document.

Revision 1 – Changes from May 2007 T10 meeting

Added sense data requirements to requirement for terminating command when encrypt/decrypt prohibited
Clarified timeout value in policy is for both read and write key requests
Moved descriptive text for fields from report policy page to configure policy poge
Added a read key request to the policy page
Added WRITE FILEMARKS to list of prohibited write operations when encryption prohibited
Moved key management error data log parameter closer to VHF and EHF parameters
Changed write key request to occur on first write following loss of key instead of on loss

Revision 2 – Moved SSC-3 content into another document, 07-361r0

Revision 3 – Changes from September T10, Vancouver BC

Revision 4 – Changes from September 16th phone conference

Simplified the model clause to only allow exclusive control from ADC, RMC, or Management

Related Documents

adc2r07c – Automation/Drive Interface Commands

ssc3r03e – SCSI Stream Commands

07-361r0 – T10 proposal for SSC-3 out of band encryption control effects

Background

The ADC-3 project proposal lists automation control of encryption parameters as an action item. This proposal introduces a mechanism for automation application client control of the encryption capabilities and parameters of a device that supports tape data encryption.

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 ADC-2

New Definition 3.1.24, existing definitions shift down:

3.1.24 Management Interface: An interface outside the scope of this standard that allows configuration and control of a DT device.

New Definition 3.1.38, existing definitions shift down:

3.1.38 Service request: An indication from the ADC device server that an automation application client action is required.

New Model Clause section 4.10:

4.10 ADC Tape Data Encryption Control

4.10.1 ADC Tape Data Encryption Control introduction

If the DT device is a device that reports itself as an SSC device in the Standard INQUIRY data (see SPC-4), then the DT device may support tape data encryption and may provide support for tape data encryption capabilities management and encryption configuration settings using ADC. If the DT device supports ADC tape data encryption control then the ADC device server shall support the

a) SECURITY PROTOCOL IN command specifying the Tape Data Encryption security protocol;
b) SECURITY PROTOCOL IN command specifying the Data Encryption Configuration security protocol;
c) SECURITY PROTOCOL OUT command specifying the Tape Data Encryption security protocol; and
d) SECURITY PROTOCOL OUT command specifying the Data Encryption Configuration security protocol.

An automation application client may use ADC control of Tape Data Encryption to control the encryption capabilities of the DT device or to control both the encryption capabilities of the DT device and the encryption parameters.

4.10.2 ADC Tape Data Encryption Control of encryption capabilities

4.10.2.1 ADC Tape Data Encryption Control of encryption capabilities introduction

The SECURITY PROTOCOL OUT command specifying the Data Encryption Configuration security protocol (see SPC-4) is used to configure the data encryption capabilities (See SSC-3).

ADC Tape Data Encryption Control of encryption capabilities is used to restrict the ability of the RMC device server or the management interface to configure encryption by changing the supported encryption algorithms reported by the DT device and configuring the DT device to reject configuration of encryption parameters or changes to encryption parameters by the RMC device server or a management interface.

4.10.2.2 ADC Tape Data Encryption Control of encryption algorithms

The SECURITY PROTOCOL OUT command specifying the Data Encryption Configuration security protocol and the Configure Encryption Algorithm Support page (see 6.3.5.2) is used to

a) control the values reported over a primary port in response to a SECURITY PROTOCOL IN command specifying the Tape Data Encryption security protocol and the Data Encryption Capabilities page;
b) take exclusive control of the configuration of encryption parameters for the ADC device server; and
c) disable use of supported encryption algorithms.

4.10.2.2.1 Setting Tape data Encryption control to ADC exclusive

The Tape Data Encryption parameters control type (see 4.10.3.2) should be set to exclusive before data encryption parameters are configured by an automation application client. The Tape Data Encryption parameters control type may be set to exclusive by sending a SECURITY PROTOCOL OUT command specifying the Data Encryption Configuration security protocol with a Configure Encryption Algorithm support page to the ADC device server with:

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

a) the PRVNTCFG field set to 10b (i.e., change the encryption parameters control type to ADC Exclusive, see 6.3.5.2);
b) the PRVNTCFG field set to 11b (i.e., change the encryption parameters control type to ADC Exclusive and mask all supported encryption algorithms from the RMC device server); or
c) preventing control of one or more supported encryption algorithms (see 4.10.3.2.4).

If the encryption configuration type is ADC Exclusive, then the automation application client may set the encryption configuration state to Open by sending a SECURITY PROTOCOL OUT command specifying the Data Encryption Configuration security protocol with a Configure Encryption Algorithm support page to the ADC device server with the PRVNTCFG field set to 01b (i.e., Change the encryption parameters control type to Open).

NOTE: methods b and c are provided for compatibility with applications that do not understand external encryption control (see SSC-3). Use of method b or c is not recommended for applications that understand external encryption control.

4.10.2.2.2 Detecting DT device algorithm support

A SECURITY PROTOCOL IN command specifying the Tape Data Encryption security protocol and the Data Encryption Capabilities page sent to the ADC device server shall return a list of all encryption algorithms that the DT device is capable of supporting. The list of algorithms reported may be a different list from the list of algorithms reported over a primary port.

Comment: The table in section 6.3.2.1 specifies that the Data Encryption Capabilities page is required on both the ADC device server and the RMC device server so we don't need to cover that.

4.10.2.2.3 Disabling use of a supported encryption algorithm

The automation application client may disable the use of a selected data encryption algorithm (see SSC-3) by sending a security protocol out command specifying the Data Encryption Configuration security protocol with a configure encryption algorithm support page to the ADC device server with the algorithm index field in a encryption algorithm support descriptor set to the algorithm index for the selected encryption algorithm and the DISABLE bit set to one.

The DT device shall not allow a set of encryption parameters for a disabled encryption algorithm to be established.

4.10.2.2.4 Preventing control of a supported encryption algorithm

The automation application client may prevent control of data encryption parameters for a selected encryption algorithm from the RMC device server or a management interface by sending a SECURITY PROTOCOL OUT command specifying the Data Encryption Configuration security protocol with a Configure Encryption Algorithm support page to the ADC device server with the ALGORITHM INDEX field in an Encryption Algorithm Support descriptor set to the selected encryption algorithm with the DECRYPT_P field set to 01b (see 6.3.5.2) and with the ENCRYPT_P field set to 01b.

The automation application client may enable configuration of encryption parameters for a selected encryption algorithm from the RMC device server or a management interface sending a SECURITY PROTOCOL OUT command specifying the Data Encryption Configuration security protocol with a Configure Encryption Algorithm support page to the ADC device server with the ALGORITHM INDEX field in a Encryption Algorithm Support descriptor set to the selected encryption algorithm with the DECRYPT_P field set to 00b and with the ENCRYPT_P field set to 00b.

4.10.3 ADC Tape Data Encryption Control of encryption parameters

4.10.3.1 ADC Tape Data Encryption Control of encryption parameters introduction

The SECURITY PROTOCOL OUT command specifying the Data Encryption Configuration security protocol and the Configure Encryption Policy page may be used to configure a decrypt key request policy, encrypt key request policy, and key request period. (See 6.3.5.3). The encryption parameters control type (see 4.10.3.2) shall be set to ADC exclusive if:

a) the DECRYPT KEY REQUEST POLICY field is set to any value other than 000b; or
b) the ENCRYPT KEY REQUEST POLICY field is set to any value other than 000b.

An encrypt key request policy set to any value other than 000b or a decrypt key request policy set to any value other than 000b shall configure the ADC device server to indicate service requirement notifications.

4.10.3.2 Encryption parameters control type

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

The encryption parameters control type is determined by the settings that affect the ability of the DT device to accept control of encryption parameters.

The values of the encryption parameters control type are shown in table y.

Table y – Encryption parameters control types

Mode	Description
Open	No interface has taken exclusive control of encryption parameters.
ADC Exclusive	Control of encryption parameters is exclusive to the ADC device server. The DT device shall accept configuration of encryption parameters from the ADC device server and shall reject configuration of encryption parameters or changes to encryption parameters from an RMC device server or management interface.
RMC Exclusive	Control of encryption parameters is exclusive to the RMC device server. The DT device shall accept configuration of encryption parameters from the RMC device server and shall reject configuration of encryption parameters or changes to encryption parameters from an ADC device server or management interface.
Management Interface Exclusive	Control of encryption parameters is exclusive to the management interface. The DT device shall accept configuration of encryption parameters from the management interface and shall reject configuration of encryption parameters or changes to encryption parameters from an ADC device server or RMC device server.

4.10.3.3 ADC Data Encryption service requirement notification

4.10.3.4 ADC Data Encryption service requirement notification introduction

When configured to do so, the ADC device server shall notify the automation application client of data encryption service requirements using the DT Device Status log page very high frequency data log parameter ESR bit (see 6.1.2.2), and the ADI encryption control status log parameter. (See 6.1.2.4).

Comment: The VHF data is not tape specific and the DT Device Status log page is not tape specific so this section needs to be technology independent.

4.10.3.4.1 Encrypt key Request Policies

An encrypt key request policy setting determines when the ADC device server sets an encrypt key request bit to one in the ADI encryption control status log parameter (see 6.1.2.4). If the encrypt key request policy is set to 00b (i.e., No encrypt key request), then the ADC device server shall not set the EKR bit in the ADI encryption control status log parameter to one. If the encrypt key request policy is set to 001b the EKR bit shall be set to one following any command other than a write type command which causes a media position change. This key policy enables multiple keys per tape. If the encrypt key request policy is set to 010b the device server shall only request keys as required to enable a single key per tape.

The DT device shall not accept write data into the buffer, write data to the medium, or process a WRITE FILEMARKS command if the EKR bit is set to one in the ADI encryption control status log parameter.

Comment: This clause should cover the case that used to be in the key exchange process prohibiting a write until a key was available. I have added "WRITE FILEMARKS" to the list of things that require a key because even though a filemark is not encrypted it can be used in error recovery and may destroy encrypted data without intending to if it is allowed to pass through. ERASE is not listed because it may be necessary to recycle a tape that was encrypted without having the key.

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

4.10.3.4.2 Decrypt key Request Policies

A decrypt key request policy determines when the ADC device server will set a decrypt key request bit in the ADI encryption control status log parameter to one. If the decrypt key request policy is set to 00b (i.e., No decrypt key request), then the ADC device server shall not set the DKR bit in the ADI encryption control status log parameter. If the decrypt key request policy is set to 001b (i.e., Request decrypt key as needed), then the ADC device server shall set the DKR bit in the ADI encryption control status log parameter whenever it determines that the current encryption parameters are not correct for the next block.

4.10.3.5 Encryption parameters values

If encryption parameters are controlled by the automation application client, then a SECURITY PROTOCOL OUT command specifying the Tape Data Encryption security protocol and the Set Data Encryption page (see SSC-3) shall contain a

a) SCOPE field set to 2 (i.e., ALL I_T NEXUS); and
b) LOCK bit set to 0.

If the ADC device server receives a SECURITY PROTOCOL OUT command specifying the Tape Data Encryption security protocol and the Set Data Encryption page with the SCOPE field set to a value other than 2, or a LOCK bit set to one, then the device server shall terminate the command with CHECK CONDITION status, with the sense key set to ILLEGAL COMMAND, and the additional sense code set to INVALID FIELD IN PARAMETER LIST.

4.10.3.6 Key exchange process

If a WRITE(6), WRITE(16), WRITE FILEMARKS(6) or WRITE FILEMARKS(16) command is received by the RMC device server, and the encrypt key request policy specifies that a key should be requested for this command, before processing the command, the ADC device server shall

1) set the EKR bit in the ADI encryption control status log parameter; and
2) set the ESR bit in the VHF data.

If a READ(6), READ(16), READ REVERSE(6), READ REVERSE(16), VERIFY(6) or VERIFY(16) command is received by the RMC device server, and the decrypt key request policy specifies that a key should be requested for this command, before processing the command, the ADC device server shall

1) set the DKR bit in the ADI encryption control status log parameter; and
2) set the ESR bit in the VHF data.

If a SECURITY PROTOCOL OUT command specifying the Data Encryption security protocol and the Encryption Parameters Complete page with the CEKR or CDKR bit set to 1 has not been processed the time specified in the KEY REQUEST PERIOD field of the configure encryption policy page (see 6.3.5.3), then the ADC device server shall set the KME bit to one in the ADI encryption control status log parameter and the RMC device server shall terminate the 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 (see SSC-3).

4.10.3.7 Key management errors

If the automation application client receives an encrypt key request and is unable to retrieve an encrypt key, then the automation application client shall send a SECURITY PROTOCOL OUT command specifying the Tape Data Encryption security protocol and an Encryption Parameters Complete page with the EKE bit set to one and the RMC device server shall terminate the command with CHECK CONDITION status, with the sense key set to DATA PROTECT, and the additional sense code set to EXTERNAL DATA ENCRYPTION CONTROL ENCRYPTION ERROR.

If the automation application client receives a decrypt key request and is unable to retrieve an decrypt key, then the automation application client shall send a SECURITY PROTOCOL OUT command specifying the Tape Data Encryption security protocol and an Encryption Parameters Complete page with the DKE bit set to one and the RMC device server shall terminate the command with CHECK CONDITION status, with the sense key set to DATA PROTECT, and the additional sense code set to EXTERNAL DATA ENCRYPTION CONTROL DECRYPTION ERROR.

Comment: EXTERNAL DATA ENCRYPTION CONTROL ENCRYPTION ERROR and EXTERNAL DATA ENCRYPTION CONTROL ENCRYPTION ERROR are not defined yet.

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

If the DKR bit is set to one in the ADI encryption control status log parameter, the automation application client sends a SECURITY PROTOCOL OUT command specifying the Tape Data Encryption security protocol and an Encryption Parameters Complete page with the CDKR bit set to one, and the read command fails for an invalid decryption key, then the ADC device server shall set the KME bit in the ADI encryption control status log parameter. The automation application client may retry the decryption key request until the exhaustive key search limit has been reached (see SSC-3).

If the KME bit is set to one in the ADI encryption control status log parameter, then the automation application client should read the DT Device Status log page and the key management error data log parameter. If the KTO bit in the ADI encryption status log parameter is set to one, then the command has failed for a timeout and the automation application client should abort the key lookup process for the key request with the matching KEY REQUEST SEQUENCE IDENTIFIER. If the KTO bit is set to zero, then the automation application client should compare the key request sequence identifier specified in the KEY REQUEST SEQUENCE IDENTIFIER field with the key request sequence identifier for the key lookup process in progress. If the key request sequence identifier matches, then the command has failed for the reason specified in the SENSE KEY field, ADDITIONAL SENSE CODE field, and the ADDITIONAL SENSE CODE QUALIFIER field. If the key request sequence identifier does not match, then the key management error was for a previous key and should be ignored.

Comment: it is possible that the ADC device server sets decrypt key request only after attempting to read the next block and detecting that it does not have the correct key. The error reading the next block will trigger a KME, but the issues is cleared when the decrypt key is sent.

If the ABT bit is set to one in the ADI encryption control status log parameters, then the automation application client should abort all key lookup processes.

If an EKR bit is set to one or a DKR bit is set to one in the ADI encryption control status log parameters and a key lookup process is in progress, then the automation application client should abort all key lookup processes.

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.

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

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	ADI encryption control status	6.1.2.4
0003h	Key management error data	6.1.2.5
0002~~2~~4h-00FFh	Reserved	
100h	Obsolete	
0101h – 0200h	DT device primary port status	6.1.2.~~4~~6
0201h – 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.

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	EPP	MSTD	MTHRD	MOUNTED
2	DT DEVICE ACTIVITY							
3	VS	Reserved			ESR	RRQST	INTFC	TAFC

Comment: Only the EXP and ESR bits ar defined by this proposal so the text describing the other fields is not repeated here.

An encryption parameters present (EPP) bit set to one indicates that the DT device 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 EPP bit set to zero indicates that the DT 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.

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

An encryption service request (ESR) bit set to one indicates that at least one bit in the SERVICE REQUEST INDICATORS field in the ADI encryption control status log parameters has been set to one since the last retrieval of the ADI encryption control status log parameter (See 6.1.2.4) by this I_T nexus. The ADC device server shall set the ESR bit to zero after successful completion of a command requesting the ADI encryption control status log parameter by this I_T nexus. An ESR bit set to zero indicates that no service request bits have changed.

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 ADI encryption control status log parameter

The ADI encryption control status log parameter format is shown in table y+1.

Table y+1 – ADI encryption control status 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 (08h)							
4	SERVICE REQUEST INDICATORS							
5								
6	KEY REQUEST SEQUENCE IDENTIFIER							
7	Reserved							
8	Reserved				SENSE KEY			
9	ADDITIONAL SENSE CODE							
10	ADDITIONAL SENSE CODE QUALIFIER							
11	Reserved							

The PARAMETER CODE field shall be set to 0002h to indicate the ADI encryption control status 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 y+1.

The PARAMETER LENGTH field shall be set to 08h.

The SERVICE REQUEST INDICATORS field is shown in table y+2.

Table y + 2: SERVICE REQUEST INDICATORS field

Bit / Byte	7	6	5	4	3	2	1	0
0	Reserved							
1	EKR	DKR	KME	ABT	Reserved			

An encrypt key request (EKR) bit set to one indicates that the device server requests an encryption key from the automation application client. The device server shall set the EKR bit to one as specified in the encrypt key request policy (see 6.3.5.3). If the EKR bit is set to one, then the automation application client may abort any key request in progress which has a key request identifier that is different from the value specified in the KEY REQUEST IDENTIFIER field.

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

A EKR bit set to zero indicates that the device server does not request an encryption key from the automation application client. The device server shall set the EKR bit to zero if:

a) it successfully processes a SECURITY PROTOCOL OUT command, with the SECURITY PROTOCOL field set to Tape Data Encryption and with the CEKR bit in an Encryption Parameters Complete page set to one;
b) it successfully processes a SECURITY PROTOCOL OUT command, with the SECURITY PROTOCOL field set to Data Encryption Configuration and with the EKE bit in an Encryption Parameters Complete page set to one; or
c) after a Key Request Period timeout (see 6.3.5.3).

A decrypt key request (DKR) bit set to one indicates that the device server requests a decryption key from the automation application client. The ADC device server shall set the DKR bit to as specified in the decrypt key request policy. If the DKR bit is set to one, then the automation application client may abort any key request in progress.

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

a) it successfully processes a SECURITY PROTOCOL OUT command, with the SECURITY PROTOCOL field set to Tape Data Encryption and with the CDKR bit in an Encryption Parameters Complete page set to one;
b) it successfully processes a SECURITY PROTOCOL OUT command, with the SECURITY PROTOCOL field set to Data Encryption Configuration and with the DKE bit in a Encryption Parameters Complete page set to one; or
c) after a Key Request Period timeout.

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

a) the device server has set the EKR bit to one in the ADI encryption control status log parameter 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 with the CEKR bit in an Encryption Parameters Complete page set to one within the Key Request Period;
b) the device server has set the DKR bit to one in the ADI encryption control status log parameter 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 with the CDKR bit in an Encryption Parameters Complete page set to one within the Key Request Period; or
c) the DT device has detected that the decryption key is not valid for the next block.
d) other vendor specific events.

If the KME bit is set to one, then the key management error data log parameter shall contain information about the key management error.

The device server shall set the KME bit to zero and the ERROR TYPE field to 0:

a) upon completion of a LOG SENSE command that reports the ADI encryption control status log parameter; or

b) as part of the processing of a Logical Unit Reset condition.

An abort (ABT) bit set to one indicates that the key request specified by the KEY REQUEST SEQUENCE IDENTIFIER field has been aborted and the key request has been cleared. If the EKR bit or the DKR bit is set to one, then the ABT bit shall be set to zero.

If the WRK bit or the DKR bit is set to one, then the KEY REQUEST SEQUENCE IDENTIFIER field shall contain a value assigned by the ADC device server to identify the key request. If the KME bit or the ABT bit is set to one, the KEY REQUEST SEQUENCE IDENTIFIER field shall contain the value assigned to the key request which has completed with a key management error or abort status.

The EKR bit, DKR bit, KME bit, and ABT bit shall not be set to zero or changed with the use of a LOG SELECT command.

6.1.2.5 Key management error data log parameter

If the device server sets the KME bit in the ADI encryption control status log parameter to one, then it shall record information pertaining to the error in the key management error data log parameter. The automation application client may retrieve this

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

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+3.

Table y+3 – Key management error data log parameter

Bit / Byte	7	6	5	4	3	2	1	0
0	(MSB)			PARAMETER CODE (3h)				
1								(LSB)
2	DU (0)	DS (1)	TSD (0)	ETC (0)	TMC (00)		LBIN (1)	LP (1)
3	PARAMETER LENGTH (08h)							
4	Reserved				KTO	ERROR TYPE		
5	Reserved							
6								
7	KEY REQUEST SEQUENCE IDENTIFIER							
8	Reserved				SENSE KEY			
9	ADDITIONAL SENSE CODE							
10	ADDITIONAL SENSE CODE QUALIFIER							
11	Reserved							

The PARAMETER CODE field shall be set to 3h 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 y+2.

The PARAMETER LENGTH field shall be set to 08h.

A key timeout error (KTO) bit set to one indicates that the device server

a) set the DKR bit to one (see 6.1.2.4) and the automation application client failed to send a SECURITY PROTOCOL OUT command with the SECURITY PROTOCOL field set to Tape Data Encryption and containing an Encryption Parameters Complete page with the CDKR bit set to one within the Key Request Period (See 6.3.3.4); or
b) set the EKR bit to one and the automation application client failed to send a SECURITY PROTOCOL OUT command with the SECURITY PROTOCOL field set to Tape Data Encryption and containing an Encryption Parameters Complete page with the CEKR bit set to one within the Key Request Period.

A KTO bit set to zero indicates that:

a) the device server set the EKR bit or the DKR bit in the ADI encryption control status log parameter to one and the automation application client sent a SECURITY PROTOCOL OUT command with the SECURITY PROTOCOL field set to Tape Data Encryption and an Encryption Parameters Complete page with the CDKR bit set to one within the Key Request Period; or

b) the device server has not set the EKR bit to one or the DKR bit to one since the last event that caused the KTO bit to be set to zero.

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

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

The KEY REQUEST SEQUENCE IDENTIFIER field shall contain the value assigned by the ADC device server in the ADI encryption control status log parameter to identify the key request that has resulted in the described error. If the described error does not describe an error on a key request in process, then the KEY REQUEST SEQUENCE IDENTIFIER field shall contain the next available identifier.

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 data reported by the RMC device server 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 following successful completion of;

a) a LOG SENSE command that reports the key management error data log parameter;
b) an unload operation;
c) a SECURITY PROTOCOL OUT command specifying the Data Encryption Configuration security protocol and the Configure Encryption Policy page; or
d) a Hard Logical Reset Event (see SAM-3).

Comment: It would seem obvious to clear a KTO bit on a SPOUT with a Completion Page but that would open a race condition where the drive may set a timeout right at the time the library sent the completion page then the library would never see the TO.

The KTO bit and ERROR TYPE field shall not be set to zero or changed with the use of a LOG SELECT command.

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.

6.1.2.6 ~~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

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

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.

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

Table y+5 – SECURITY PROTOCOL SPECIFIC field value

CODE	Description	Support		Reference
		ADC Device Server	RMC Device Server	
0000h	Tape Data Encryption In Support page	M	M	SSC-3
0001h	Tape Data Encryption Out Support page	M	M	SSC-3
0002 – 000Fh	Reserved			
0010h	Data Encryption Capabilities page	M	M	SSC-3
0011h	Supported Key Formats page	O	O	SSC-3
0012h	Data Encryption Management Capabilities page	O	O	SSC-3
0013h – 001Fh	Reserved			
0020h	Data Encryption Status page	M	M	SSC-3
0021h	Next Block Encryption Status page	M	M	SSC-3
0022h – 002Fh	Reserved			
30h	Random Number page	O	O	SSC-3
31h	Device Server Key Wrapping Public Key page	O	O	SSC-3
0032h – FEFFh	Reserved			
FF00h – FFFFh	Vendor specific			
Support key: M – mandatory for device servers that support the Tape Data Encryption security protocol O – optional 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 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.

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	6.3.3.2
0001h	Data Encryption Configuration Out Support page	M	6.3.3.3
0002 – 000Fh	Reserved		
0010h	Report Data Encryption Policy page	O	6.3.3.4
0011h – FEFFh	Reserved		
FF00h – FFFFh	Vendor specific		
Support key: M – mandatory for device servers that support the Data Encryption Configuration security protocol			

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

O – optional 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.

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.

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.

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

6.3.3.4 Report Data Encryption Policy page.

The Report Data Encryption Policy page indicates the current encryption policy configuration for the DT device. 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	ENCRYPTION PARAMETERS CONTROL TYPE							
5	Reserved							
6								
7	Reserved			DECRYPT KEY REQUEST POLICY			ENCRYPT KEY REQUEST POLICY	
8	(MSB)			KEY REQUEST PERIOD				
9								(LSB)
10	Reserved							
11								

The PAGE CODE field shall be set to 0010h to indicate the Report Data Encryption policy page.

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

The ENCRYPTION PARAMETERS CONTROL TYPE field contains information on the data encryption parameters control type. Table y+10 shows the values of the ENCRYPTION PARAMETERS CONTROL TYPE field.

Table y+10 – ENCRYPTION PARAMETERS CONTROL TYPE field values

CODE	Description
000b	Data encryption parameters control type is set to Open.
001b	Data encryption parameters control type is set to ADC exclusive.
010b	Data encryption parameters control type is set to RMC exclusive.
011b	Data encryption parameters control type is set to Management Interface exclusive.
100b-111b	Reserved

See 6.3.5.3 for the definitions of the DECRYPT KEY REQUEST POLICY, ENCRYPT KEY REQUEST POLICY field and the KEY REQUEST PERIOD field.

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	Support	Reference
0000h – 000Fh	Reserved		
0010h	Set Data Encryption page	M	SSC-3
0011h	SA Encapsulation page	O	SSC-3
0012h – 002Fh	Reserved		
0030h	Data Encryption Parameters Complete	M	ADC-3
0031h – FEFFh	Reserved		
FF00h – FFFFh	Vendor specific		
Support key: M – mandatory for device servers that support the Tape Data Encryption security protocol O – optional 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.

6.3.4.2 Data Encryption Parameters Complete page.

Table y+12 specifies the format of the Encryption Parameters Complete page.

Table y+12 – Data Encryption Parameters Complete page

Bit / Byte	7	6	5	4	3	2	1	0
0	(MSB)			PAGE CODE (0030h)				
1								(LSB)
2	(MSB)			PAGE LENGTH (12)				
3								(LSB)
4	AUTOMATION COMPLETE RESULTS							
5	KEY REQUEST SEQUENCE IDENTIFIER							
6	Reserved				EKE	DKE	CEKR	CDKR
7	Reserved							
15								

The PAGE CODE field shall be set to 0030h to indicate the Data Encryption Parameters complete page.

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

The AUTOMATION REQUEST RESULTS field indicates the results of the key request specified in the KEY REQUEST SEQUENCE IDENTIFIER field and is described in table y+13.

Table y+13 – AUTOMATION COMPLETE RESULTS field value

CODE	Description
00h	No results
01h	The automation device has completed servicing a request
02h	The automation device experienced an unrecoverable error in attempting to access the key manager.
03h	The key manager returned an error status when the automation device attempted to access the key.
04h	The requested key was not found.
05h-FFh	Reserved

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

The KEY REQUEST SEQUENCE IDENTIFIER field shall contain the sequence value for the key request corresponding to these results.

An encryption key error (EKE) bit set to one indicates that the automation application client encountered an error while processing an encryption key request.

A decryption key error (DKE) bit set to one indicates that the automation application client encountered an error while processing a decryption key request.

Comment: It would be useful to put a sense data field in the completion results so specific sense data could be provided to the application client on the primary interface when an encryption key or decryption key error occurs. An alternative would be to rely on the results field and specify what sense data should be returned for each result in the SSC-3 proposal.

If the clear encrypt key request (CEKR) bit is set to one the encrypt key request for the indicated key request sequence shall be cleared. If the CEKR bit is set to zero the encrypt key request for the indicated key request sequence shall not be cleared.

If the clear decrypt key request (CDKR) bit is set to one the decrypt key request for the indicated key request sequence shall be cleared. If the CDKR bit is set to zero the encrypt key request for the indicated key request sequence shall not be cleared.

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+14) specifies the type of page that the application client is sending.

Table y+14 – SECURITY PROTOCOL SPECIFIC field value

CODE	Description	Support	Reference
0000h – 000Fh	Reserved		
0010h	Configure Encryption Algorithm Support page	M	6.3.5.2
0011h	Configure Encryption Policy page	M	6.3.5.3
0011h – FEFFh	Reserved		
FF00h – FFFFh	Vendor specific		
Support key: M – mandatory for device servers that support the Data Encryption Configuration security protocol O – optional 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.

6.3.5.2 Configure Encryption Algorithm Support page

Table y+15 specifies the format of the Configure Encryption Algorithm Support page.

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

Table y+15 – 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				PRVNTCFG		Reserved	
5				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.

The prevent configuration (PRVNTCFG) field (see table y+16) specifies the encryption control type of the DT Device.

Table y+16 – PRVNTCFG field values

CODE	Description
00b	Do not change the encryption parameters control type.
01b	Change the encryption parameters control type to Open (see 4.10.3.2).
10b	Change the encryption parameters control type to ADC Exclusive.
11b	Change the encryption parameters control type to ADC Exclusive and mask all supported encryption algorithms from the RMC device server.

Each Encryption Algorithm Support descriptor (see table y+17) 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 in ascending order of the value in the ALGORITHM INDEX field. It shall not be considered an error if all Encryption Algorithm Support descriptors are not included for all algorithms supported by the DT device.

If the DT device currently has a saved set of data encryption parameters associated with any I_T nexus the ADC device server shall terminate a SECURITY PROTOCOL OUT command specifying the Configure Encryption Algorithm Support page 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+17 – 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_P		ENCRYPT_P	
6	Reserved					DISABLE	Reserved	
7	Reserved							

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. If the value

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

specified in the ALGORITHM INDEX field is not an algorithm index for a supported encryption algorithm, then the device server shall terminate the command with CHECK CONDITION STATUS with the sense key set to ILLEGAL COMMAND and the additional sense code set to INVALID FIELD IN PARAMETER LIST.

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

The DECRYPT_P field (see table y+18) specifies the decryption configuration that the DT device shall apply to commands processed by the RMC device server for the specified algorithm index.

Table y+18 – DECRYPT_P field values

CODE	Description
00b	The DT device shall report this algorithm as available for decryption (i.e, the algorithm shall be included in the list of supported algorithms reported in a Data Encryption Capabilities page with the DECRYPT_C field set to 0, 1, or 2) for all device servers except the ADC device server.
01b	The DT device shall report this algorithm as disabled for decryption (i.e, the algorithm, if included in the list of supported algorithms reported in a Data Encryption Capabilities page, shall have the DECRYPT_C field set to 3) for all device servers except the ADC device server.
10b-11b	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 DT device shall:

a) report a 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 processed by the RMC device server; and
b) cause the RMC device server to terminate a SECURITY PROTOCOL OUT command specifying the Tape Data Encryption security protocol and the Set Data Encryption page 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.

If the DECRYPT_D field is set to zero, the DT device shall cause the RMC device server to 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 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 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.

The ENCRYPT_D field (see table y+19) specifies the encryption configuration that the DT device shall apply to commands processed by the RMC device server for the specified algorithm index.

Table y+19 – ENCRYPT_D field values

CODE	Description
00b	The DT device shall report this algorithm as available for encryption (i.e, the algorithm shall be included in the list of supported algorithms reported in a Data Encryption Capabilities page with the ENCRYPT_C field set to 0, 1, or 2) for all device servers except the ADC device server.
01b	The DT device shall report this algorithm as disabled for encryption (i.e, the algorithm, if included in the list of supported algorithms reported in a Data Encryption Capabilities page, shall have the ENCRYPT_C field set to 3) for all device servers except the ADC device server.
10b-11b	Reserved

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

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 DT device shall cause the RMC device server to:

a) report a 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 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 ENCRYPT_D field is set to zero, the DT device shall cause the RMC device server to 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 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 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.

The ENCRYPT_D setting, DECRYPT_D setting, and DISABLE setting shall be set to default after:

a) a hard reset event (see SAM-3); or
b) other vendor-specific events.

If the DISABLE bit is set to one, then the DT device shall disable the specified data encryption algorithm (i.e., return an Encryption Algorithm descriptor for the specified algorithm in response to a SECURITY PROTOCOL IN command specifying the Tape Data Encryption security protocol and the Data Encryption Capabilities page with the DISABLED bit set to one, see SSC-3). If the DISABLE bit is set to zero, then the DT device shall not disable the specified encryption algorithm. If the DISABLE bit is set to zero and the specified encryption algorithm is disabled, the DT device shall enable the specified encryption algorithms.

6.3.5.3 Configure Encryption Policy page

Table y+20 specifies the format of the Configure Encryption Policy page.

Table y+20 – 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							
6								
7	Reserved		DECRYPT KEY REQUEST POLICY			ENCRYPT KEY REQUEST POLICY		
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.

The DECRYPT KEY REQUEST POLICY field indicates the policy the device server shall use for acquiring read decryption keys from the automation application client. The decrypt key request policy values are defined in table y+21.

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

Table y+21 – DECRYPT KEY REQUEST POLICY field values

Value	Policy Name	Description
000b	No decrypt key request	The ADC device server shall never request a decrypt key.
001b	Request decrypt key as needed	Request decrypt key when the RMC device server processes a READ(6), READ(16), READ REVERSE(6), READ REVERSE(16), VERIFY(6) or VERIFY(16) command and the decryption mode or key in the current set of data encryption parameters is not correct for the next block.
010b – 111b		Reserved

The ENCRYPT KEY REQUEST POLICY field indicates the policy the device server shall use for acquiring write encryption keys from the automation application client. The encrypt key request policy values are defined in table y+22.

Table y+22 – ENCRYPT KEY REQUEST POLICY field values

Value	Policy Name	Description
000b	No encrypt key request	The ADC device server shall never request an encrypt key.
001b	Request encrypt key every reposition	Request encrypt key when the RMC device server processes a WRITE(6), WRITE(16), WRITE FILEMARKS(6), or WRITE FILEMARKS(16) command following an a) ERASE(6), ERASE(16), LOAD UNLOAD, LOCATE(10), LOCATE(16), REWIND, SPACE(6), or SPACE(16) command; or b) after an event which causes the loss of the data encryption parameters (see SSC-3).
010b	Request encrypt key when not set	The ADC device server shall request an encrypt key before altering the media while processing the first WRITE(6), WRITE(16), WRITE FILEMARKS(6) or WRITE FILEMARKS(16) command after a) the medium in mounted in the DT device b) an event that causes the DKR bit in the extended high frequency data log parameter to be set to one. c) an event that causes the loss of the data encryption parameters.
011b – 111b		Reserved

The KEY REQUEST PERIOD field indicates the maximum time, in 100 millisecond increments, the ADC device server shall wait after requesting an encrypt key or requesting a decrypt 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.