memorandum

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

T10/07-164r3

To	From	Subject	Date
INCITS T10 Committee	Curtis Ballard, HP Michael Banther, HP	Automation Encryption Control	26 September, 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

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.

Proposed Changes to ADC-2

New Definition 3.1.17, existing definitions shift down:

3.1.17 Interface connection: A connection that exists between a physical device and an application client. This connection may be an I_T nexus or a management interface link.

New Definitions 3.1.25 through 3.1.27, existing definitions shift down:

3.1.25 Management Server: A system outside the scope of this standard that provides configuration and control commands to a physical device through a management interface.

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

3.1.27 Management Interface link: An relationship between a management interface, a management server, and the objects with them.

New Definition 3.1.40, existing definitions shift down:

3.1.40 Service requirement: An indication from the physical device that a remote SMC device server action is required.

New Model Clause section 4.10:

4.10 ADI Tape Data Encryption control

4.10.1 ADI Tape Data Encryption control introduction

If the DT device is a 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 tape data encryption control then the DT device shall support the SECURITY PROTOCOL IN command specifying the Tape Data Encryption and the Data Encryption Configuration security protocols and the SECURITY PROTOCOL OUT command specifying the Tape Data Encryption and the Data Encryption Configuration security protocols.

4.10.2 ADI Tape Data Encryption control of encryption capabilities

4.10.2.1 ADI Tape Data Encryption control of encryption capabilities introduction

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

The automation application client may use the SECURITY PROTOCOL OUT command specifying the Data Encryption Configuration security protocol and the Configure Encryption Algorithm Support page to

a) remove reporting of supported encryption algorithms;
b) disable use of supported encryption algorithms; or
c) prevent configuration of encryption parameters from other logical units.

Comment: It has been suggested that these three methods of control could all be restated as "disable" with different capabilities disabled. I believe that would be too confusing with different levels of disable and instead rewrote these slightly.

4.10.2.2 ADI 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 is used to 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.

4.10.2.3 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 logical unit via an ADT I_T nexus 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.

A SECURITY PROTOCOL IN command specifying the Tape Data Encryption security protocol and the Data Encryption Capabilities page sent to the RMC logical unit shall return the same list of data encryption algorithm descriptors as is reported over a primary port.

4.10.2.3.1 Removing reporting of a supported encryption algorithm

The automation application client may remove reporting of a selected encryption algorithm 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 RMV bit set to one.

4.10.2.3.2 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 physical device shall not allow a set of encryption parameters for a disabled encryption algorithm to be established using any interface connection.

4.10.2.3.3 Exclusive control of encryption parameters for a supported encryption algorithm

The automation application client may take exclusive control of data encryption parameters for a supported encryption algorithm by preventing control of encryption parameters for that algorithm from any other interface connection.

The automation application client may prevent control of data encryption parameters for a selected encryption algorithm from any other interface connection 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_D field set to 01b (i.e. the physical device shall disable decryption capabilities using this algorithm, See 6.3.5.2) and with the ENCRYPT_D field set to 01b (i.e. the physical device shall disable encryption capabilities using this algorithm).

The automation application client may enable configuration of encryption parameters for a selected encryption algorithm from any other interface connection 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 selected encryption algorithm with the DECRYPT_D field set to 00b (i.e. the RMC device server shall enable decryption capabilities using this algorithm, See 6.3.5.2) and with the ENCRYPT_D field set to 00b (i.e. the RMC device server shall enable encryption capabilities using this algorithm).

4.10.2.3.4 Encryption control mode

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

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

Table y – Encryption control modes

Mode	Description
Allow	Control of encryption parameters is allowed from all interface connections. The physical device shall accept configuration of encryption parameters from any supported interface connection.

Exclusive	Control of encryption parameters is exclusive to this interface connection. The physical device shall accept configuration of encryption parameters from this interface connection and shall reject configuration of encryption parameters or changes to encryption parameters from all other interface connections.

4.10.2.3.5 Exclusive control of encryption parameters for all supported encryption algorithms

The automation application client may set the encryption configuration mode 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 the with the PRVNTCFG field set to 10b (i.e. change the encryption control mode to Exclusive, See 6.3.5.2).

The automation application client may set the encryption configuration state to Allow 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 control state to Allow, See 6.3.5.2).

4.10.3 ADI Tape Data Encryption control of encryption parameters

4.10.3.1 ADI 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 can be used to configure a decrypt key request policy, encrypt key request policy, and key request period. (See 6.3.5.3). The encryption control mode shall be set to 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 ADI Data Encryption service requirement notification

The ADT device server may notify the automation application client of data encryption service requirements using the DT Device Status log page and the ADI encryption control status log parameter. An ESR bit set to one in the VHF data indicates that the automation application client should retrieve the DT Device Status log page and the ADI encryption control status log parameter. (See 6.2.1.4).

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.

4.10.3.3 Encrypt key Request Policies

An encrypt key request policy setting determines when the DT device sets an encrypt key request bit in the EHF log parameter data. (See 6.3.5.3) If the encrypt key request policy is set to 00b (i.e. No encrypt key request), then the ADC device server shall set the EKR bit in the EHF data bit to zero. If the encrypt key request policy is set to 001b the EKR bit shall be set 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.

4.10.3.4 Decrypt key Request Policies

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

4.10.3.5 Key exchange process

If a command to modify the media is received by the DT device, and a key request policy has been configured, before processing any data, the DT device shall

a) set the key request bit in the ADI encryption control status log parameter; and

b) set the ESR bit in the VHF data.

If the physical device has set a key request bit in the ADI encryption control status log parameter, then the RMC device server shall not process any data until a SECURITY PROTOCOL OUT command specifying the Data Encryption Configuration security protocol and the Encryption Parameters Complete page has been received by the ADC device server. If a SECURITY PROTOCOL OUT command specifying the Data Encryption security protocol and the Encryption Parameters Complete page has not been received before the time specified in the KEY REQUEST PERIOD field of the configure encryption policy page, then the physical device shall set the KME bit 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)

4.10.3.6 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 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 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 ENCRYPTION ERROR.

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

If the physical device has set the DKR bit in the ADI encryption control status log parameter, and 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 physical device 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 in the ADI encryption control status log parameters has been set, then the automation application shall read the DT Device Status log page and the key management error data log parameter. If the KTO bit in the cryptographic error descriptor 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 SEQUENCE IDENTIFIER ADI encryption control status log parameter. If the KTO bit is not set to one, then the automation application client should compare the KEY REQUEST SEQUENCE IDENTIFIER ADI encryption control status log parameter 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 DT device 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.

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	ADI encryption control status	6.1.2.4
0003h	Key management error data	6.1.2.5
000~~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	EKP	MSTD	MTHRD	MOUNTED
2	DT DEVICE ACTIVITY							
3	VS	Reserved			ESR	RRQST	INTFC	TAFC

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

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.

An encryption service request (ESR) bit set to one indicates that at least one service request bit in the DT Device Status Log page and the ADI encryption control status log parameters has changed from its previous value since the last retrieval of the DT Device Status Log page and the ADI encryption control status log parameter (See 6.x.x.x) by this I_T nexus. The ADC device server sets the ESR bit to zero after retrieval of the DT Device Status Log Page and 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	Reserved							
5	EKR	DKR	KME	ABT	Reserved			
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 16.

The PARAMETER LENGTH field shall be set to 08h.

An encrypt key request (EKR) bit set to one indicates that the device server requests a write 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.x.x.x). If the EKR bit is set to one, then the automation application client may abort any key request in progress.

The device server shall set the EKR bit to zero if:

a) it successfully process 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 process 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.x.x.x).

A decrypt key request (DKR) bit set to one indicates that the device server requests a decryption key from the automation application client. The device server shall set the DKR bit to one when the physical device determines that the current encryption parameters are not correct for an encrypted block (See SSC-3). 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 when:

a) it receives a valid 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 receives a valid 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 (See 6.x.x.x).

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

a) the device server has set the EKR 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 with the CDKR bit in an Encryption Parameters Complete page set to one within the Key Request Period (See 6.x.x.x);

b) the device server has set the EKR 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 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 a cryptographic error.

The device server shall set the KME bit to zero:

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.

A KME bit set to zero indicates that, since the most recently processed LOG SENSE command that reported the key management error data log parameter or the most recent event resulting in a Logical Unit Reset condition:

a) the device server has set the EKR 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 an Encryption Parameters Complete page with the CEKR bit set to one within the Key Request Period (See 6.3.3.4);

b) the device server has set the DKR 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 an Encryption Parameters Complete page with the CDKR bit set to one within the Key Request Period;

c) the device server has not set the EKR bit to one or the DKR bit to one; or

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

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, and KME 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 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							
4	Cryptographic error descriptor							
11								
n +1	KEY-ASSOCIATED DATA DESCRIPTORS LIST							
M								

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 the length of the data to follow.

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 3	Reserved							
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 device server set the RKR bit to one or the WKR 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 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:

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

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 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) following successful completion of 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 Encryption Parameters Complete page; or

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

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.

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.

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.

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	POLICY CONTROL							
5	Reserved							
6								
7	Reserved		DECRYPT KEY REQUEST POLICY			ENCRYPT KEY REQUEST POLICY		
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 POLICY CONTROL field contains information on how the data encryption parameters were set. Table y+10 shows the values of the POLICY CONTROL field.

Table y+10 – PARAMETERS CONTROL field values

CODE	Description
000b	Data encryption policy has not been configured
001b	Data encryption policy was configured using a primary port.
010b	Data encryption policy was configured using an ADI port.
011b	Data encryption policy was configured using a management interface.
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.

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 – 002Fh	Reserved	
0030h	Encryption Parameters Complete	ADC-3
0031h – 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.

6.3.4.2 Encryption Parameters Complete page.

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

Table y+12 –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 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

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.

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	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.

6.3.5.2 Configure Encryption Algorithm Support page

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

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)							
	Encryption Algorithm Support descriptor (last)							
N								

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 state of the DT Device.

Table y+16 – PRVNTCFG field values

CODE	Description
00b	Do not change the encryption configuration mode
01b	Change the encryption control state to Allow
10b	Change the encryption control state to Exclusive
11b	Reserved

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_D		ENCRYPT_D	
6	Reserved				RMV	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 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_D field (see table y+18) specifies the decryption configuration that the RMC device server shall apply for the specified algorithm index.

Table y+18 – DECRYPT_D field values

CODE	Description
00b	The physical device shall enable decryption capabilities using this algorithm
01b	The physical device shall disable decryption capabilities using this algorithm
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 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+19) specifies the encryption configuration that the RMC device server shall apply for the specified algorithm index.

Table y+19 – ENCRYPT_D field values

CODE	Description
00b	The RMC device server shall enable encryption capabilities using this algorithm
01b	The RMC device server shall disable encryption capabilities using this algorithm
10b-11b	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.

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 be set to default after:

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

If the remove (RMV) bit is set to zero, then the algorithm shall be included in the list of supported algorithms. If the RMV bit is set to one, the algorithm shall not be included in the list of supported algorithms.

If the DISABLE bit is set to zero, then the Data Encryption Algorithm descriptor for the specified algorithm shall have the DISABLED bit set to zero. If the DISABLE bit is set to one, then the Data Encryption Algorithm descriptor for the specified algorithm shall have the DISABLED bit set to one.

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.

Table y+21 – DECRYPT KEY REQUEST POLICY field values

Value	Policy Name	Description
000b	No decrypt key request	The DT device shall never set the DKR bit in the extended high frequency data log parameter.
001b	Request decrypt key as needed	Request decrypt key when the DT device processes a command that will perform a read operation and the decryption key for the next block is not in the current set of data encryption parameters.
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	Do not request encrypt keys
001b	Request encrypt key every reposition	Request encrypt 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 encrypt key after a space/locate/read or rewind operation. The ADC device server shall request a new encrypt key after an event which causes the loss of the data encryption parameters.
010b	Request encrypt key when not set	If data encryption is enabled and the mounted device supports the selected encryption algorithm at the current logical position then the DT Device shall request an encrypt key before altering the media while processing the first write type 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.
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.