memorandum

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

T10/07-164r2 – Draft B –

To	From	Subject	Date
INCITS T10 Committee	Curtis Ballard, HP Michael Banther, HP	Automation Encryption Control	16 August, 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

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 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 tape device, 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

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

Comment: the reference to SSC-3 assumes 07-361 is incorporated into SSC-3.

4.10.2.1 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.

4.10.2.2 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 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.

4.10.2.2.1 Removing a supported encryption algorithm

The automation application client may remove the 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.

4.10.2.2.2 Disabling a supported encryption algorithm

The automation application client may disable the 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 DISABLE bit set to one.

4.10.2.2.3 Preventing and enabling configuration of encryption parameters using another port for a selected algorithm

The automation application client may prevent configuration of encryption parameters for a selected encryption algorithm using any other port 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

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

RMC device server shall disable decryption capabilities using this algorithm, See 6.3.5.2) and with the ENCRYPT_D field set to 01b (i.e. the RMC device server shall disable encryption capabilities using this algorithm).

The automation application client may enable configuration of encryption parameters for a selected encryption algorithm using any other port (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 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).

4.10.2.2.4 Preventing and enabling configuration of encryption parameters using another port for all algorithms

The ability to accept encryption parameters over any other port is called the encryption configuration state. If the encryption configuration state is set to enable configuration, then the DT device server shall allow configuration of encryption parameters over any port. If the encryption configuration state is set to prevent configuration, then the DT device server shall prevent configuration of encryption parameters over any port.

Comment: If we like the concept of an encryption configuration state then this probably needs some model text and may even provide a way for a primary port to say "I'm in control" so we could use this state for the primary port to control whether ADI encryption control may be enabled.

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

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

Comment: The above reference to SSC-3 requires 07-361 acceptance and incorporation in SSC-3.

4.10.2.3 Disabling tape data encryption control over another port using ADI Tape Data Encryption control

An automation application client may disable DT device tape data encryption over another port by using ADI Tape Data Encryption control of encryption algorithms to

a) remove all supported encryption algorithms (See 4.10.2.2.2); or
b) prevent configuration of encryption parameters using another port for all algorithms (See 4.10.2.2.5).

4.10.3 ADI Tape Data Encryption control of encryption parameters

An automation application client should disable tape data encryption control over another port before configuring any encryption parameters.

An automation application client may use ADI tape data encryption control of encryption parameters by:

1) disabling tape data encryption control over all other ports (See 4.10.2.2);
2) using the SECURITY PROTOCOL OUT command specifying the Data Encryption Configuration security protocol and the Configure Encryption Policy page to configure a read key request policy, write key request policy, and key request period. (See 6.3.5.3);
3) Monitoring the DT Device Status log page and the ADI encryption control status log parameter for read key requests, write key requests, and key management errors;
4) using the SECURITY PROTOCOL OUT command specifying the Tape Data Encryption security protocol and the Set Data Encryption page to provide encryption parameters following a key request; and

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

5) Using the SECURITY PROTOCOL OUT command specifying the Tape Data Encryption security protocol and the Encryption Parameters Complete page to clear a key request.

4.10.3.1 ADI Tape Data Encryption service requirement notification

The ADT device server may notify the automation application client of data encryption events using the DT Device Status log page and the ADI encryption control status log parameter. The ADT device server shall set the ESR bit in DT Device Status log page and the VHF data log parameter when any status field in the ADI encryption control status log parameter is changed (See 6.2.1.4).

Comment: the following two paragraphs need work but I wanted to explain the write and read key request policies.

4.10.3.2 Write Key Request Policies

A write key request policy setting determines when the DT device sets a write key request bit in the EHF log parameter data. (See 6.3.5.3) If the write key request policy is set to 00b (i.e. No write key request), then the ADC device server shall set the WRK bit in the EHF data bit to zero. If the write key request policy is set to 001b the write key request 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 write key request policy is set to 010b the device server shall only request keys as required to enable a single key per tape.

4.10.3.3 Read Key Request Policies

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

4.10.3.4 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 EHF data; and

b) set the EHF bit in the VHF data.

If the DT device has set a key request bit in the EHF data, then the DT device shall not process any data until a SECURITY PROTOCOL OUT command specifying the Tape Data Encryption security protocol and the Set Data Encryption page has been received by the ADC application client. If a SECURITY PROTOCOL OUT command specifying the Tape Data Encryption security protocol and the Set Data Encryption page has not been received before the time specified in the KEY REQUEST PERIOD field of the configure encryption policy page, then the DT device shall set the KME bit in the EHF data and the DT device shall enter an external encryption control error state. (See SSC-3)

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

4.10.3.5 Key management errors

If the automation application client receives a write key request and is unable to retrieve a write key, then the automation application client shall send a SECURITY PROTOCOL OUT command specifying the Data Encryption Configuration security protocol and a Configure Encryption Policy page with the PE bit set to one.

If the automation application client receives a read key request and is unable to retrieve a write key, then the automation application client shall send a SECURITY PROTOCOL OUT command specifying the Data Encryption Configuration security protocol and a Configure Encryption Policy page with the PD bit set to one.

If the KME bit in the EHF data 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. If the KTO bit is not set to one, then the automation application client should compare the key associated data in the cryptographic error descriptor with the key associated data from the last SECURITY PROTOCOL OUT command specifying the Tape Data Encryption security protocol and the Set Data Encryption page. If the key associated data 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 associated data 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 read 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 read 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
0002~~2~~3h-00FFh	Reserved	
100h	Obsolete	
0101h – 0200h	DT device primary port status	6.1.2.~~4~~5
0201h – 7FFFh	Reserved	
8000h – FFFFh	Vendor specific	

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

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

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

6.1.2.4 ADI encryption control status log parameter

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

Table y – 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					ERROR TYPE		
5	WKR	RKR	KME	KTO	ABT	Reserved		
6	KEY REQUEST SEQUENCE COUNT							
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.

The ERROR TYPE field indicates the type of the last cryptographic error reported by the DT device. The error types are shown in table y+2.

Table y+2 – ERROR TYPE field value

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

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.

A write key request (WKR) bit set to one indicates that the device server requests a write encryption key from the automation application client. The device server shall set the WKR bit to one as specified in the write key request policy (See 6.x.x.x).

The device server shall set the WKR 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 CWKR 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 PE bit in a Configure Encryption Policy page set to one; or

c) after a Key Request Period timeout (See 6.x.x.x).

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

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

a) when a medium becomes mounted; or

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

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

a) it receives a valid SECURITY PROTOCOL OUT command, with the SECURITY PROTOCOL field set to Tape Data Encryption and with the CRKR 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 PD bit in a Configure Encryption Policy 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 WKR bit to one and the automation application client has failed to send a SECURITY PROTOCOL OUT command, with the SECURITY PROTOCOL field set to Tape Data Encryption and with the CRKR 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 WKR bit to one and the automation application client has failed to send a SECURITY PROTOCOL OUT command, with the SECURITY PROTOCOL field set to Tape Data Encryption and with the CRKR 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 ADI encryption control status log parameter or the most recent event resulting in a Logical Unit Reset condition:

a) the device server has set the WKR 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 CWKR bit set to one within the Key Request Period (See 6.3.3.4);

b) the device server has set the RKR bit to one and the automation application client has sent a SECURITY PROTOCOL OUT command with the SECURITY PROTOCOL field set to Tape Data Encryption an Encryption Parameters Complete page with the CRKR bit set to one within the Key Request Period;

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

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

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.x.x.x) 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.x.x.x). A KTO bit set to zero indicates that:

a) the device server has set the WKR 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 CWKR bit set to one within the Key Request Period (See 6.x.x.x);

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

b) the device server has set the RKR bit to one and the automation application client has sent a SECURITY PROTOCOL OUT command with the SECURITY PROTOCOL field set to Tape Data Encryption an Encryption Parameters Complete page with the CRKR bit set to one within the Key Request Period;

c) the device server has not set the WKR bit to one or the RKR bit to one since the last event that caused the KTO bit to be set to zero.

An abort (ABT) bit set to one indicates that the key request specified by the KEY REQUEST SEQUENCE COUNT field has been aborted and the key request has been cleared.

If the WRK bit or the RKR bit is set to one, then the KEY REQUEST SEQUENCE COUNT 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 COUNT field shall contain the value assigned to the key request which has completed with a key management error or abort status.

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 ADI encryption control status log parameter;

b) an unload operation;

c) a SECURITY PROTOCOL OUT command specifying the Data Encryption Configuration security protocol and the Set Data Encryption Policy page; or

d) an event resulting in a Hard Reset condition.

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

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

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

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

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

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+3) specifies the type of report that the application client is requesting.

Table y+3 – 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.

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

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.

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

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	Reserved					PE	PD	Reserved
7	Reserved		READ KEY REQUEST POLICY			WRITE 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.

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

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

The DATA ENCRYPTION POLICY CONFIGURATION LOGICAL UNIT field shall contain the logical unit number for the logical unit that last received a SECURITY PROTOCOL OUT command specifying the Data Encryption Configuration security protocol and the Configure Encryption Algorithm Support page with the PRVNTCFG bit set to 10b (See 6.3.5.2). The DATA ENCRYPTION POLICY CONFIGURATION LOGICAL UNIT field shall be set to the logical unit number of the RMC logical unit upon:

a) a hard reset; or

b) successful completion of a SECURITY PROTOCOL OUT command specifying the Data Encryption Configuration security protocol and the Configure Encryption Algorithm Support page with the PRVNTCFG field set to 01b.

See 6.3.5.3 for the definitions of the PE bit, PD bit, READ KEY REQUEST POLICY, WRITE KEY REQUEST POLICY field and the KEY REQUEST PERIOD field.

The PE bit set to one shall be set to zero following

a) the processing of a command that affects the medium position; or
b) successful completion of an unload operation.

The PD bit set to one shall be set to zero following

a) the processing of a command that affects the medium position; or
b) successful completion of an unload operation.

6.3.4 SECURITY PROTOCOL OUT command specifying Tape Data Encryption security protocol

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

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

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

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

Table y+11 – SECURITY PROTOCOL SPECIFIC field value

CODE	Description	Reference
0000h – 000Fh	Reserved	
0010h	Set Data Encryption page	SSC-3
0011h – 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+4 specifies the format of the Encryption Parameters Complete page.

Table y+4 –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 COUNT							
6	Reserved						CWKR	CRKR
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 COUNT field and is described in table y+5.

Table y+5 – 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 COUNT field shall contain the sequence value for the key request corresponding to these results.

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

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

If the clear read key request (CRKR) bit is set to one the read key request for the indicated key request sequence shall be cleared. If the CRKR bit is set to zero the write 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+12) specifies the type of page that the application client is sending.

Table y+12 – SECURITY PROTOCOL SPECIFIC field value

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

If the SECURITY PROTOCOL SPECIFIC field is set to a reserved or unsupported value, the ADC device server shall terminate the command with CHECK CONDITION status, with the sense key set to ILLEGAL REQUEST, and the additional sense code set to INVALID FIELD IN CDB.

6.3.5.2 Configure Encryption Algorithm Support page

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

Table y+13 – Configure Encryption Algorithm Support page

Bit / Byte	7	6	5	4	3	2	1	0
0	(MSB)			PAGE CODE (0010h)				
1								(LSB)
2	(MSB)			PAGE LENGTH (n-3)				
3								(LSB)
4	Reserved				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) specifies the encryption control state of the DT Device.

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

Table y – PRVNTCFG field values

CODE	Description
00b	Do not change the encryption control state
01b	Change the encryption control state to allow configuration.
10b	Change the encryption control state to prevent configuration.
11b	Reserved

Each Encryption Algorithm Support descriptor (see table y+14) shall contain configuration settings for a data encryption algorithm supported by the RMC logical unit. If more than one descriptor is included, they shall be 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+14 – Encryption Algorithm Support descriptor

Bit / Byte	7	6	5	4	3	2	1	0
0	ALGORITHM INDEX							
1	Reserved							
2	(MSB)			DESCRIPTOR LENGTH (4)				
3								(LSB)
4	Reserved					DECRYPT_D		ENCRYPT_D
6	Reserved				RMV	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+15) specifies the decryption configuration that the RMC device server shall apply for the specified algorithm index.

Table y+15 – DECRYPT_D field values

CODE	Description
00b	The RMC device server shall enable decryption capabilities using this algorithm
01b	The RMC device server 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.

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

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

a) report a 0 or 3 in the DECRYPT_C field in the Data Encryption Algorithm descriptor for the specified algorithm index in response to a SECURITY PROTOCOL IN command; and
b) terminate a SECURITY PROTOCOL OUT command specifying the Tape Data Encryption security protocol and the Set Data Encryption page that attempts to set a decryption mode other than DISABLE for the specified algorithm with CHECK CONDITION status, the sense key set to ILLEGAL REQUEST, the additional sense code set to INVALID FIELD IN PARAMETER LIST, and the sense key specific FIELD POINTER field set to the DECRYPTION MODE field.

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

Table y+16 – ENCRYPT_D field values

CODE	Description
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 but have the DISABLED status bit set to one if the DECRYPT_D field is set to 01b and the and the ENCRYPT_D field is set to 01b. If the RMV bit is set to one, the algorithm shall not be included in the list of supported algorithms if the DECRYPT_D field is set to 01b and the and the ENCRYPT_D field is set to 01b.D

Comment: This doesn't say that the SSC device server should follow the behavior described in SSC-3 for a disabled algorithm, just that the bit should be set. Will requiring that the bit is set be sufficient to cause the SSC device server to follow the behavior for a disabled algorithm?

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

6.3.5.3 Configure Encryption Policy page

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

Table y+17 – Configure Encryption Policy page

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

c) When the PE bit is set to one, the RMC device server shall terminate a write type command with CHECK CONDITION status, the sense key set to DATA PROTECT, the additional sense code set to CRYPTOGRAPHIC KEY UNAVAILABLE.

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

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

The READ KEY REQUEST POLICY field indicates the policy the device server shall use for acquiring read decryption keys from the automation application client. The read key request policy values are defined in table y+18.

Table y+18 – READ KEY REQUEST POLICY field values

Value	Policy Name	Description
000b	No read key request	The DT device shall never set the RKR bit in the extended high frequency data log parameter.
001b	Request read key as needed	Request read 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 WRITE KEY REQUEST POLICY field indicates the policy the device server shall use for acquiring write encryption keys from the automation application client. The write key request policy values are defined in table y+11.

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

Table y+11 – WRITE KEY REQUEST POLICY field values

Value	Policy Name	Description
000b	No write key request	Do not request write keys
001b	Request write key every reposition	Request write key when the DT device processes a command that will perform a write operation following a command to reposition the media. The DT Device shall request a new write key after a space/locate/read or rewind operation. The ADC device server shall request a new write key after an event which causes the loss of the data encryption parameters.
010b	Request write 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 a write 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 RKR 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 a write key or requesting a read 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.