memorandum

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

T10/07-164r6

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

Revision History

Revision 0 – Initial document.

Revision 1 – Changes from May 2007 T10 meeting

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

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

Revision 3 – Changes from September T10, Vancouver BC

Revision 4 – Changes from September 16th phone conference

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

Revision 5 – Changes from October 10th phone conference

- Moved EPP bit in VHF parameter data
- Additional standards editorial cleanup
- New definition for configuration of data encryption parameters
- Made encryption key request/decryption key request and key management error mutually exclusive
- Added a clear key timeout bit to the parameters complete page to simplify setting the KTO bit to zero
- Revised encryption error log parameter to include sense data for the error, not RMC sense data
- Made ADC exclusive control a requirement before setting policy values

Revision 6 – Changes from October 31st phone conference

- Moved the request indicators, request policy, and request period to SSC-3 proposal 07-361r4

Related Documents

adc2r07e – Automation/Drive Interface Commands

ssc3r03e – SCSI Stream Commands

07-361r4 – T10 proposal for SSC-3 out of band encryption control effects

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

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.

Per consensus among the ADI working group as of the October 10th phone conference, the requirements and capabilities for automation control of data encryption capabilities and parameters are:

Configuration

a. The ability to mask reporting of all encryption algorithms via RMC device server (only in conjunction with exclusive control via ADC device server). (IBM)
b. The ability to disable use (for all device servers, including ADC) of individual encryption algorithms (but still report them). If an algorithm is disabled it's disabled for all device servers.
c. The ability for ADC device to always determine what algorithms the DT device supports.
d. The ability to prevent any changes to encryption parameters by other than the ADC device server (i.e., only the ADC device can change the parameters). (Establish or clear = change).
e. The ability to establish encryption policy via the ADC device server.

Runtime (all via ADC)

a. The ability to request a key
b. The ability to abort a request
c. The ability to explicitly indicate completion of request servicing (client)
d. The ability to indicate an error
e. The ability to retrieve error information (client)
f. The ability to prevent the drive from writing data at the current media position due to unavailability of a key, and can't change logical position. Allow ADC device server to have DT device notify RMC device to not process any user data or filemarks.
g. The ability to establish or clear data encryption parameters
h. Provide sequence identification for (a) – (d)

In the proposed changes that follow, new text appears in blue or purple, deleted text appears in ~~red strikeout~~, and editorial comments appear in green.

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

Proposed Changes to ADC-2

New Definition 3.1.12, existing definitions shift down:

3.1.12 Configuration of data encryption parameters: Establish data encryption parameters (see SSC-3), or make any change to an existing set of data encryption parameters (i.e., disable encryption or decryption, see SSC-3).

New Definition 3.1.17, existing definitions shift down:

3.1.17 DT device management interface: An interface outside the scope of this standard that allows configuration and control of a DT device.

New Model Clause section 4.10:

4.10 ADC tape data encryption control

4.10.1 ADC tape data encryption control introduction

If the DT device contains a logical unit that contains an RMC device server 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 also may support control of tape data encryption capabilities and data encryption parameters via the ADC device server. Controlling data encryption capabilities or data encryption parameters via the ADC device server is called ADC tape data encryption control. If the DT device supports ADC tape data encryption control, then the ADC device server shall support the:

a) SECURITY PROTOCOL IN command (see SPC-4) specifying the Tape Data Encryption security protocol;
b) SECURITY PROTOCOL IN command specifying the Data Encryption Configuration security protocol;
c) SECURITY PROTOCOL OUT command (see SPC-4) specifying the Tape Data Encryption security protocol; and
d) SECURITY PROTOCOL OUT command specifying the Data Encryption Configuration security protocol.

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

4.10.2 ADC tape data encryption control of data encryption capabilities

4.10.2.1 ADC tape data encryption control of data encryption capabilities introduction

ADC tape data encryption control of data encryption capabilities is used to restrict the ability of the RMC device server or the DT device management interface to configure data encryption. ADC tape data encryption control may be used to configure parameters in the DT device that change the data encryption capabilities.

The SECURITY PROTOCOL OUT command specifying the Data Encryption Configuration security protocol and the Configure Data Encryption Algorithm Support page (see 6.3.5.2) is used to do at least one of the following:

a) establish exclusive control of the configuration of data encryption parameters for the ADC device server (see 4.10.2.2);
b) control the set of data encryption algorithms reported by the device servers (see SSC-3); and
c) disable data encryption algorithms (see 4.10.2.3).

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

4.10.2.2 Setting tape data encryption control to ADC exclusive

The data encryption parameters control type (see 4.10.3.2) should be set to ADC exclusive before data encryption parameters are established by an automation application client. The data encryption parameters control type is set to ADC exclusive by sending a SECURITY PROTOCOL OUT command specifying the Data Encryption Configuration security protocol with a Configure Data Encryption Algorithm Support page (see 6.3.5.2) to the ADC device server with:

a) the ENCRYPTION CONTROL field set to 10b (i.e., change the data encryption parameters control type to ADC exclusive); or
b) the ENCRYPTION CONTROL field set to 11b (i.e., change the data encryption parameters control type to ADC exclusive and mask all supported data encryption algorithms from the RMC device server).

Comment: The working group need to determine whether the ENCRYPTION CONTROL is an algorithm configuration parameter since it changes the support of encryption algorithms for other device servers and the values reported in the Data Encryption Capabilities page, or if it is a policy and belongs in the Configure Encryption Policy page.

If the data encryption parameters control type is ADC exclusive, then the automation application client may set the data encryption parameters control type to open by sending a SECURITY PROTOCOL OUT command specifying the Data Encryption Configuration security protocol with a Configure Data Encryption Algorithm Support page to the ADC device server with the ENCRYPTION CONTROL field set to 01b (i.e., change the data encryption parameters control type to open).

4.10.2.3 Disabling use of a supported data encryption algorithm

The automation application client may disable a data encryption algorithm (see SSC-3) by sending a SECURITY PROTOCOL OUT command specifying the Data Encryption Configuration security protocol with a Configure Data Encryption Algorithm Support page to the ADC device server with the ALGORITHM INDEX field in a data encryption algorithm support descriptor set to the algorithm index for the selected data encryption algorithm and the DISABLE bit set to one.

4.10.2.4 Detecting DT device data encryption algorithm support

A SECURITY PROTOCOL IN command specifying the Tape Data Encryption security protocol and the Data Encryption Capabilities page processed by the ADC device server shall return the set of data encryption algorithms supported by the DT device (see SSC-3).

4.10.3 ADC tape data encryption control of data encryption parameters

4.10.3.1 ADC tape data encryption control of data encryption parameters introduction

The SECURITY PROTOCOL OUT command specifying the Data Encryption Configuration security protocol and the Configure Encryption Policy page (see 6.3.5.3) may be used to configure a decryption parameters request policy, encryption parameters request policy, and encryption parameters request period (see SSC-3).

The SECURITY PROTOCOL OUT command specifying the Tape Data Encryption security protocol and the Set Data Encryption page or the SA Encapsulation page may be used to provide a set of data encryption parameters for encryption, or provide a set of data encryption parameters for decryption (see SSC-3).

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

4.10.3.2 Data encryption parameters control type

If the DT device supports ADC tape data encryption control, then the physical device (see SSC-3) accessed by the ADC device server shall contain a data encryption parameters control type parameter. The value in the data encryption parameters control type parameter controls the establishment of data encryption parameters within the physical device.

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

Table y – Data Encryption parameters control types

Mode	Description
Open	No interface has taken exclusive control of data encryption parameters. This is the default setting for the data encryption parameters control type. The DT device shall accept configuration of data encryption parameters from any device server.
ADC exclusive	Configuration of data encryption parameters is exclusive to the ADC device server. The DT device shall accept configuration of data encryption parameters from the ADC device server and shall reject configuration of data encryption parameters or changes to data encryption parameters from an RMC device server or DT device management interface.
RMC exclusive	Configuration of data encryption parameters is exclusive to the RMC device server. The DT device shall accept configuration of data encryption parameters from the RMC device server and shall reject configuration of data encryption parameters or changes to data encryption parameters from an ADC device server or DT device management interface. How the data encryption parameters control type is set to RMC exclusive is beyond the scope of this standard.
DT device management interface exclusive	Configuration of data encryption parameters is exclusive to the DT device management interface. The DT device shall accept configuration of data encryption parameters from the DT device management interface and shall reject configuration of data encryption parameters or changes to data encryption parameters from an ADC device server or RMC device server. How the data encryption parameters control type is set to DT device management interface exclusive is beyond the scope of this standard.

The data encryption parameters control type shall be set to open following a:

a) bus reset;
b) power cycle; or
c) other vendor specific events

4.10.3.3 ADC data encryption service requests

When configured to do so, the ADC device server shall notify the automation application client of ADC data encryption service requests (e.g., the DT device includes an SSC-3 compliant device server and has a data encryption parameters request indicator set to TRUE, see SSC-3) using the DT Device Status log page very high frequency data log parameter ESR bit (see 6.1.2.2), and the DT device ADC encryption control status log parameter (see 6.1.2.4).

Comment: The VHF data is not tape specific and the DT Device Status log page is not tape specific so this section needs to be technology independent whenever possible. Currently external data encryption control service requests are only defined in SSC-3 so we have to point there.

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

4.10.3.4 Data encryption parameters required values

A SECRUITY PROTOCOL OUT command processed by the ADC device server shall contain a SCOPE field set to 2 and a LOCK bit set to zero.

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

4.10.3.5 Key exchange process

If the DT device requires a set of data encryption parameters for data encryption (i.e., the DT device includes an SSC-3 compliant device server and the data encryption parameters for encryption request indicator is set to TRUE, see SSC-3), the ADC device server shall:

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

If the DT device requires a set of data encryption parameters for data decryption (i.e., the DT device includes an SSC-3 compliant device server and the data encryption parameters for decryption request indicator is set to TRUE, see SSC-3), the ADC device server shall:

1) set the DPR bit in the ADC encryption control status log parameter;
2) set the ESR bit in the VHF data.

4.10.3.6 Key management errors

If the automation application client receives a request for a set of data encryption parameters for encryption and is unable to provide a set of data encryption parameters for encryption, 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 EPE bit set to one.

If the automation application client receives a request for a set of data encryption parameters for decryption and is unable to retrieve a set of data encryption parameters for decryption, 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 DPE bit set to one.

The automation application client may retry the decryption key request until the exhaustive key search limit has been reached (see SSC-3).

If the DT device indicates that the encryption parameters period has expired (i.e., the DT device includes an SSC-3 compliant device server and the data encryption period timer expired indicator is set to TRUE, see SSC-3), then the ADC device server shall set the:

a) KME bit to one in the ADC encryption control status log parameter; and
b) KTO bit to one in the key management error data log parameter;

If the KME bit is set to one in the ADC encryption control status log parameter, then the automation application client should read the DT Device Status log page and the key management error data log parameter. If the KTO bit in the ADC encryption status log parameter is set to one, then a command has failed for a key request timeout and the automation application client should abort the key lookup process for the key request with the matching KEY REQUEST SEQUENCE IDENTIFIER. If the KTO bit is set to zero, then the automation application client should compare the key request sequence identifier specified in the KEY REQUEST SEQUENCE IDENTIFIER field with the key request sequence identifier for the key lookup process in progress. If the key request sequence identifier matches, then a 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.

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

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

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

Modifications to 6.1.2:

6.1.2 DT Device Status log page

6.1.2.1 DT Device Status log page overview

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

Table 14 – DT Device Status log page

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

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

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

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	ADC encryption control status	6.1.2.4
0003h	Key management error data	6.1.2.5
0002~~2~~4h-00FFh	Reserved	
100h	Obsolete	
0101h – 0200h	DT device primary port status	6.1.2.~~4~~6
0201h – 7FFFh	Reserved	
8000h – FFFFh	Vendor specific	

6.1.2.2 Very high frequency data log parameter

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

Table 16 – Very high frequency data log parameter format

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

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

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

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

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

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

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

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 DT device ADC encryption control status log parameter

The DT device ADC encryption control status log parameter format is shown in table y+1.

Table y+1 – DT device ADC encryption control status log parameter format

Bit / Byte	7	6	5	4	3	2	1	0
0	(MSB)	PARAMETER CODE (0002h)						
1								(LSB)
2	DU (0)	DS (1)	TSD (0)	ETC (0)	TMC (00)		LBIN (1)	LP (1)
3	PARAMETER LENGTH (08h)							
4	SERVICE REQUEST INDICATORS							
5								
6	KEY REQUEST SEQUENCE IDENTIFIER							
9								
10	Reserved							
11								

The PARAMETER CODE field shall be set to 0002h to indicate the DT device ADC encryption control status log parameter.

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

See SPC-3 for descriptions of the DU bit, DS bit, TSD bit, ETC bit, TMC field, LBIN bit, and LP bit. These bits and fields shall be set to the values shown in table y+1.

The PARAMETER LENGTH field shall be set to 08h.

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

Table y + 2: SERVICE REQUEST INDICATORS field

Bit / Byte	7	6	5	4	3	2	1	0
0	Reserved							
1	EPR	DPR	KME	ABT	Reserved			

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

A EPR bit set to zero indicates that the device server does not request a set of data encryption parameters for encryption from the automation application client. The device server shall set the EPR bit to zero if:

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

A decryption parameters request (DPR) bit set to one indicates that the device server requests a set of encryption parameters for decryption from the automation application client. The ADC device server shall set the DPR bit to as specified in the decryption parameters request policy. If the DPR bit is set to one, then the automation application client may abort any key request in progress. If the DPR bit is set to one, then the KME bit shall be set to zero.

A DPR bit set to zero indicates that the device server does not request a set of data encryption parameters for decryption from the automation application client. The device server shall set the DPR bit to zero if:

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

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

a) the device server has set the EPR bit to one in the ADC encryption control status log parameter and the automation application client has failed to send a SECURITY PROTOCOL OUT command, with the SECURITY PROTOCOL field set to Tape Data Encryption and with the CEPR bit in an Encryption Parameters Complete page set to one within the Key Request Period;
b) the device server has set the DPR bit to one in the ADC encryption control status log parameter and the automation application client has failed to send a SECURITY PROTOCOL OUT command, with the SECURITY PROTOCOL field set to Tape Data Encryption and with the CDPR bit in an Encryption Parameters Complete page set to one within the Key Request Period; or
c) other vendor specific events.

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

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

The device server shall set the KME bit to zero:

a) upon completion of a LOG SENSE command that reports the key management error data log parameter; or
b) as part of the processing of a Logical Unit Reset condition.

Comment: In a conference call we decided that it would be useful to have the KME bit set to one if a set of data encryption parameters in provided following a read key request and the first attempt to use those parameters determines that the parameters are invalid. That doesn't work with our current method of using a sequence identifier because KME entries need an identifier to report which key request had the error but a new key request needs a new sequence identifier and the drive needs to be able to set another key request. KME can only be used in cases where the drive has failed the command.

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 EPR bit is set to one or the DPR bit is set to one, then the ABT bit shall be set to zero.

If the ERK bit is set to one or the DPR 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 is set to one 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 EPR bit, DPR bit, KME bit, and ABT bit shall not be set to zero or changed with the use of a LOG SELECT command.

6.1.2.5 Key management error data log parameter

If the KME bit is set to one in the ADC encryption control status log parameter, then the key management error data log parameter shall contain valid information pertaining to the error that caused the KME bit to be set to one. The key management error log parameter format is shown in table y+3.

Table y+3 – Key management error data log parameter

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

The PARAMETER CODE field shall be set to 3h to indicate the key management error data log parameter.

See SPC-3 for descriptions of the DU bit, DS bit, TSD bit, ETC bit, TMC field, LBIN bit, and LP bit. These bits and fields shall be set to the values shown in table y+2.

The PARAMETER LENGTH field shall be set to 08h.

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

The key timeout (KTO) bit shall be set to one if the event that caused the KME bit to be set to one in the ADC encryption control status log parameter was a timeout event (see 4.10.3.6). The key timeout error (KTO) shall be set to zero:

a) if the event that caused the KME bit to be set to on in the ADC encryption control status log parameter was not a timeout event; or
b) upon processing a SECURITY PROTOCOL OUT command specifying the Tape Data Encryption security protocol and the Data Encryption Parameters Complete page with the CKTO bit set to one.

The ERROR TYPE field indicates the type of the last event that caused the KME bit in the ADC encryption control status log parameter to be set to one. 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

The device server shall set the ERROR TYPE field to zero following successful completion of:

a) an unload operation;
b) a SECURITY PROTOCOL OUT command specifying the Data Encryption Configuration security protocol and the Configure Encryption Policy page;
c) a SECURITY PROTOCOL OUT command specifying the Tape Data Encryption security protocol and the Data Encryption parameters complete page with the CKTO bit set to one and the KTO bit is set to one; or
d) a Hard Reset Event (see SAM-3).

The KEY REQUEST SEQUENCE IDENTIFIER field shall contain the value assigned by the ADC device server in the ADC encryption control status log parameter to identify the key request associated with the event that caused the KME bit in the ADC encryption control status log parameter to be set to one.

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 event that caused the KME bit to be set to one in the ADC encryption control status log parameter.

The key management error data log parameter shall not be 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 are undefined.

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

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

If the SECURITY PROTOCOL SPECIFIC field is set to a reserved or unsupported value, then 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 encryption configuration in the device server. The command supports a series of pages that are requested individually. An application client requests a page by using a SECURITY PROTOCOL IN command with the SECURITY PROTOCOL field set to Data Encryption Configuration security protocol and the SECURITY PROTOCOL SPECIFIC field set to the page code requested.

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

The SECURITY PROTOCOL SPECIFIC field (see table y+6) specifies the type of report that the application client is requesting.

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

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

6.3.3.2 Data Encryption Configuration In Support page.

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

Table y+7 – Data Encryption Configuration In Support page

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

The PAGE CODE field shall be set to 0000h to indicate the Data Encryption Configuration in support page.

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

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

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

6.3.3.3 Data Encryption Configuration Out Support page.

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

Table y+8 – Data Encryption Configuration Out Support page

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

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

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

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

6.3.3.4 Report Data Encryption Policy page.

The Report Data Encryption Policy page indicates the current encryption policy configuration for the DT device. Table y+9 specifies the format of the Report Data Encryption Policy page.

Table y+9 – Report Data Encryption Policy page

Bit / Byte	7	6	5	4	3	2	1	0
0	(MSB)			PAGE CODE (0010h)				
1								(LSB)
2	(MSB)			PAGE LENGTH (8)				
3								(LSB)
4	ENCRYPTION PARAMETERS CONTROL TYPE							
5	Reserved							
6								
7	Reserved			DECRYPTION PARAMETERS REQUEST POLICY		ENCRYPTION PARAMETERS REQUEST POLICY		
8	(MSB)			ENCRYPTION PARAMETERS REQUEST PERIOD				
9								(LSB)
10	Reserved							
11								

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

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

The ENCRYPTION PARAMETERS CONTROL TYPE field contains information on the data encryption parameters control type (see 4.10.3.2). Table y+10 shows the values of the ENCRYPTION PARAMETERS CONTROL TYPE field.

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

Table y+10 – ENCRYPTION PARAMETERS CONTROL TYPE field values

CODE	Description
00h	Data encryption parameters control type is set to Open.
01h	Data encryption parameters control type is set to ADC exclusive.
02h	Data encryption parameters control type is set to RMC exclusive.
03h	Data encryption parameters control type is set to DT device management interface exclusive.
04h – FFh	Reserved

See 6.3.5.3 for the definitions of the DECRYPTION PARAMETERS REQUEST POLICY, ENCRYPTION PARAMETERS REQUEST POLICY field and the ENCRYPTION PARAMETERS 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	Support	Reference
0000h – 000Fh	Reserved		
0010h	Set Data Encryption page	O	SSC-3
0011h	SA Encapsulation page	O	SSC-3
0012h – 002Fh	Reserved		
0030h	Data Encryption Parameters Complete	M	6.3.4.2
0031h – FEFFh	Reserved		
FF00h – FFFFh	Vendor specific		
Support key: M – mandatory for device servers that support the Tape Data Encryption security protocol O – optional for device servers that support the Tape Data Encryption security protocol			

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

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

6.3.4.2 Data Encryption Parameters Complete page.

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

Table y+12 – Data Encryption Parameters Complete page

Bit / Byte	7	6	5	4	3	2	1	0
0	(MSB)			PAGE CODE (0030h)				
1								(LSB)
2	(MSB)			PAGE LENGTH (12)				
3								(LSB)
4	AUTOMATION COMPLETE RESULTS							
5	Reserved							
6	Reserved			EPE	DPE	CKTO	CEPR	CDPR
7	Reserved							
8	KEY REQUEST SEQUENCE IDENTIFIER							
11								
12	Reserved							
15								

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

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

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

Table y+13 – AUTOMATION COMPLETE RESULTS field value

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

An encryption parameters error (EPE) bit set to one indicates that the automation application client encountered an error while processing a data encryption parameters for encryption request.

A decryption parameters error (DPE) bit set to one indicates that the automation application client encountered an error while processing a data encryption parameters for decryption key request.

If the clear key timeout (CKTO) bit is set to one and the KTO bit in the key management error data log parameter is set to one, then the KTO bit and the ERROR TYPE field in the key management error data log parameter shall be set to zero. If the CKTO bit is set to one and the KTO bit in the key management error data log parameter is set to zero, the ERROR TYPE field shall not be changed. If the CKTO bit is set to zero the KTO bit in the key management error data log parameter shall not be set to zero and the ERROR TYPE field shall not be changed.

If the clear encryption parameters request (CEPR) bit is set to one the encrypt key request for the indicated key request sequence shall be cleared. If the CEPR bit is set to zero the encrypt 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 decryption parameters request (CDPR) bit is set to one the decrypt key request for the indicated key request sequence shall be cleared. If the CDPR bit is set to zero the encrypt key request for the indicated key request sequence shall not be cleared.

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

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 DT device. The command supports a series of pages that are sent individually. An application client requests to send a page by using a SECURITY PROTOCOL OUT command with the SECURITY PROTOCOL field set to Data Encryption Configuration security protocol and the SECURITY PROTOCOL SPECIFIC field set to the page code requested.

The security protocol specific field (see table y+14) specifies the type of page that the application client is sending.

Table y+14 – SECURITY PROTOCOL SPECIFIC field value

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

If the SECURITY PROTOCOL SPECIFIC field is set to a reserved or unsupported value, then 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 Data Encryption Algorithm Support page

Table y+15 specifies the format of the Configure Data Encryption Algorithm Support page. If the DT device has a saved set of data encryption parameters associated with any I_T nexus, or has a volume mounted, then the ADC device server shall terminate a SECURITY PROTOCOL OUT command specifying the Configure Data Encryption Algorithm Support page with CHECK CONDITION status and set the sense key to ILLEGAL REQUEST, the additional sense code to INVALID FIELD IN CDB, and the sense key specific FIELD POINTER field set to the PAGE CODE field.

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

Table y+15 – Configure Data 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						ENCRYPTION CONTROL	
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 Data Encryption Algorithm Support page.

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

The ENCRYPTION CONTROL field (see table y+16) specifies the encryption control type of the DT Device.

Table y+16 – ENCRYPTION CONTROL field values

CODE	Description
00b	Do not change the encryption parameters control type.
01b	Change the encryption parameters control type to Open (see 4.10.3.2).
10b	Change the encryption parameters control type to ADC Exclusive.
11b	Change the encryption parameters control type to ADC Exclusive and remove all encryption algorithms from the list of supported data encryption algorithms reported to all other device servers.

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 Encryption Algorithm Support descriptors are not included for all algorithms supported by the DT device.

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							
5	Reserved					DISABLE	Reserved	
6	Reserved							
7								

Comment: The DISABLE bit in the middle of an otherwise reserved field looks odd but that allows this descriptor to be a mirror image of the Data Encryption Capabilities page that will be reported with a SPIN. That field could be moved anywhere if the symmetry is not helpful.

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

The ALGORITHM INDEX field specifies 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.

The DESCRIPTORS LENGTH field indicates the length of the data to follow.

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

6.3.5.3 Configure Encryption Policy page

Table y+20 specifies the format of the Configure Encryption Policy page. If the data encryption parameters control type is not set to ADC exclusive, then the ADC device server shall terminate the command with CHECK CONDITION status with the sense key set to INVALID COMMAND and the additional sense code set to INVALID FIELD IN CDB.

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			DECRYPTION PARAMETERS REQUEST POLICY		ENCRYPTION PARMETERS REQUEST POLICY		
8	(MSB)			ENCRYPTION PARAMETERS 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 DECRYPTION PARAMETERS REQUEST POLICY field specifies the policy that the DT device shall use for acquiring a set of data encryption parameters for decryption from the automation application client (see SSC-3). The decryption parameters request policy values are defined in table y+21.

Table y+21 – DECRYPTION PARAMETERS REQUEST POLICY field values

Value	Policy Name
000b	No decryption parameters requests (see SSC-3)
001b	Request decryption parameters as needed
010b – 111b	

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.

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

Table y+22 – ENCRYPT KEY REQUEST POLICY field values

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

The ENCRYPTION PARAMETERS REQUEST PERIOD field indicates the maximum time, in 100 millisecond increments, the DT device shall wait after requesting an set of data encryption parameters for encryption or requesting a set of data encryption parameters (see 4.10.3.6) for decryption from the automation application client (e.g., the data encryption parameters period time if the DT device includes an SSC-3 compliant device server, see SSC-3). A ENCRYPTION PARAMETERS REQUEST PERIOD field value of 0000h indicates the key request period shall be infinite.