memorandum

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

T10/08-029r1

To	From	Subject	Date
INCITS T10 Committee	Curtis Ballard, HP Michael Banther, HP	Automation Encryption Control	25 January, 2007

Revision History for previous document number, 07-164
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 page
- 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

Revision 7 – Changes from November T10 Las Vegas
- Renamed parameters control type to control policy and moved it to the policy page
- Specified contents of ASC/ASCQ field in data encryption errors

Revision 8 – Changes from November 14th ADC conference call
- Removed underlines from changes on sections already discussed
- Changed unqualified “device server” to qualified most places – Note a few locations referred to “in the device server” and those statements were not qualified as they refer back to a qualified device server.
- Put in LSB/MSB on sequence identifiers
- Defined a code value in the table for the encryption control policies and reference all set/reports to that table
- Added encryption control policies for exclusive with algorithms removed
- Clarified ABT setting and clearing
- Changed CKTO bit to CKME for clearing all errors instead of just the timeout error.

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

Revision 9 – Changes from November 28th ADC conference call, changes are underlined
ERROR TYPE field in key management error data log parameter changed to 4 bits and moved
Reordered bits in data encryption parameters complete byte 6
Reduced vendor unique range for AUTOMATION COMPLETE RESULTS in parameters complete page
Reformatted table for encryption parameters control policies with a column for control allowed by interface
Combined both modes of ADC exclusive into a single control type
Added text about allowing the control policy to be set to RMC exclusive or DT device mgmt exclusive
New text in 4.10.4.2 to introduce the sequence identifier
Moved all text about control type to 4.10.1 and renumbered sections
New text 4.10.4.3 for sequence for providing data encryption parameters
Reworked text for error case where decryption parameters are not correct
Reworked ABT text
Removed EPE bit and DPE bit from encryption parameters complete page -- covered by results field
Moved DISABLE bit in configure encryption algorithm support page

Revision History for 08-029

Revision 0 – Changes from December 12th ADC conference call, changes are underlined
Changed the policy name from a singular policy to a policy type and updated references
Changed "R = Rejected" in policy type table to "P = Prevented"
Reworked paragraph for assigning a parameters request sequence identifier to a new request
Added requirement that a parameters complete page must clear the pending request or error

Revision 1 – Changes from December 12th ADC conference call, changes are underlined
Changed the policy name from a singular policy to a policy type and updated references

Revision 2 – Changes from January 2008 ADC working group meeting, changes are underlined
Redefined data encryption parameters control policy 0000b to VS
Clarified table y requirement for RMC device behavior on rejected commands
Added model clause paragraph recommending a policy before configuration
Corrected requirements for device server when a timeout occurs – not previously in a sequence and missed a step

Related Documents

adc2r07e – Automation/Drive Interface Commands

ssc3r03e – SCSI Stream Commands

07-361r6 – 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.

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.

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

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.

Proposed Changes to ADC-2

New Definition 3.1.16, existing definitions shift down:

3.1.16 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 ADC tape data encryption control. ADC tape data encryption control may support:

a) restricting the ability to establish or change a set of tape data encryption parameters;
b) establishing or changing tape data encryption parameters via the ADC device server; and
c) disabling tape data encryption algorithms.

If the DT device supports ADC tape data encryption control, then the ADC device server shall support the:

a) SECURITY PROTOCOL IN command specifying the Tape Data Encryption security protocol (see 6.3.2);
b) SECURITY PROTOCOL IN command specifying the Data Encryption Configuration security protocol (see 6.3.3);
c) SECURITY PROTOCOL OUT command (see SPC-4) specifying the Tape Data Encryption security protocol (see 6.3.4); and
d) SECURITY PROTOCOL OUT command specifying the Data Encryption Configuration security protocol (see 6.3.5).

An automation application client uses ADC tape data encryption control to control the tape data encryption capabilities of the DT device and the tape data encryption parameters of the DT device.

If the DT device supports ADC tape data encryption control, then the DT device accessed by the ADC device server shall contain a data encryption parameters control policy parameter. The value in the data encryption parameters control policy parameter controls the ability to establish or change data encryption parameters within the physical device.

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

Table y shows the values of the data encryption parameters control policy.

Table y – Data encryption parameters control policy

Policy Type	Policy Code	Description	Parameters Control		
			ADC Device Server	RMC Device Server	DT Device Management Interface
Vendor Specific	0000b	Vendor specific	VS	VS	VS
Open	0001b	No interface has taken exclusive control of data encryption parameters. This is the default setting for the data encryption parameters control policy.	A	A	A [c]
ADC exclusive	0010b	The ADC device server has exclusive control of the ability to establish or change data encryption parameters and shall report all data encryption algorithms in the list of algorithms reported by the DT device with the ENCRYPT_C field set to capable with external control and the DECRYPT_C field set to capable with external control.	A	P [b]	P [d]
	0011b	The ADC device server has exclusive control of the ability to establish or change data encryption parameters and all algorithms are removed from the list of algorithms reported by the DT device (see SSC-3).	A	P [b]	P [d]
RMC exclusive	0100b	The RMC device server has exclusive control of the ability to establish or change data encryption parameters.	P [a]	A	P [d]
DT device management interface exclusive	0101b	The DT device management interface has exclusive control of the ability to establish or change data encryption parameters.	P [a]	P [b]	A [c]
	0110b – 1111b	Reserved			

Parameters Control Key: A = Allowed
the DT device shall process a command from this device server or DT device management interface attempting to establish or change a set of data encryption parameters.
P = Prevented
the DT device shall reject a command from this device server or DT device management interface attempting to establish or change a set of data encryption parameters.

[a] The ADC device server shall terminate a SECURITY PROTOCOL OUT command that attempts to establish or change a set of data encryption parameters with CHECK CONDITION status with the sense key set to ILLEGAL REQUEST, and the additional sense code set to DATA ENCRYPTION CONFIGURATION PREVENTED.
[b] The RMC device server shall terminate a SECURITY PROTOCOL OUT command that attempts to establish or change a set of data encryption parameters. See the appropriate command set standard (e.g., SSC-3).
[c] The commands for establishing or changing a set of data encryption parameters via a DT device management interface are beyond the scope of this standard.
[d] The method for rejecting a command from a DT device management interface is beyond the scope of this standard.

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

a) hard reset condition; or
b) other vendor specific events.

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

An application client or DT device management interface should set the data encryption parameters control policy type to a value other than Open or Unknown before sending a SECURITY PROTOCOL OUT command containing a page attempting to establish a set of data encryption parameters. An application client or DT device management interface may set the data encryption parameters control policy type to Open to return the data encryption parameters control policy to the default setting.

The data encryption parameters control policy type is set to Open by sending a SECURITY PROTOCOL OUT command specifying the Data Encryption Configuration security protocol with a Configure Encryption Policy page (see 6.3.5.3) to the ADC device server with the CONTROL POLICY CODE field set to 0001b.

The data encryption parameters control policy type is set to ADC exclusive by sending a SECURITY PROTOCOL OUT command specifying the Data Encryption Configuration security protocol with a Configure Encryption Policy page to the ADC device server with:

a) the CONTROL POLICY CODE field set to 0010b; or
b) the CONTROL POLICY CODE field set to 0011b.

The data encryption parameters control policy type is set to RMC exclusive by sending a SECURITY PROTOCOL OUT command specifying the Data Encryption Configuration security protocol with a Configure Encryption Policy page to the ADC device server with the CONTROL POLICY CODE field set to 0100b.

The data encryption control policy type is set to DT device management interface exclusive by:

a) sending a SECURITY PROTOCOL OUT command specifying the Data Encryption Configuration security protocol with a Configure Encryption Policy page to the ADC device server with the CONTROL POLICY CODE field set to 0101b; or
b) other vendor specific methods (e.g., a DT device management interface command beyond the scope of this standard).

4.10.2 Disabling a supported data encryption algorithm

The automation application client disables 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.

4.10.3 Reporting 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 returns the set of data encryption algorithms supported by the physical device (see SSC-3).

4.10.4 ADC tape data encryption control of data encryption parameters

4.10.4.1 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) is 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 a page that provides a set of data encryption parameters is used to establish or change a set of data encryption parameters for encryption, and establish or change a set of data encryption parameters for decryption (see SSC-3).

4.10.4.2 Reporting data encryption parameters requests

When configured to do so, the ADC device server shall notify the automation application client of data encryption parameters requests (e.g., the DT device includes an SSC-3 compliant device server and has a data encryption parameters for encryption request indicator set to TRUE or has a data encryption parameters for decryption 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 data encryption control status log parameter (see 6.1.2.4).

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

When processing an encryption parameters request, the ADC device server shall assign a data encryption parameters request sequence identifier to uniquely identify the encryption parameters request (see 6.1.2.4). The ADC device server shall maintain the data encryption parameters sequence identifier until it processes a:

a) SECURITY PROTOCOL OUT command with a Data Encryption Parameters Complete page and a matching value in the PARAMETERS REQUEST SEQUENCE IDENTIFIER field; or
b) new encryption parameters request; or
c) hard reset condition.

If the DT device requires a set of data encryption parameters for data encryption, then the ADC device server shall:

1) set the encryption parameters request (EPR) bit in the DT device ADC data encryption control status log parameter to one; and
2) set the encryption service request (ESR) bit in the VHF data to one.

If the DT device requires a set of data encryption parameters for data decryption, then the ADC device server shall:

1) set the decryption parameters request (DPR) bit in the DT device ADC data encryption control status log parameter; and
2) set the encryption service request (ESR) bit in the VHF data to one.

4.10.4.3 Providing a set of data encryption parameters

An automation application client may use ADC tape data encryption control to provide a set of data encryption parameters by:

1) monitoring the DT Device Status log page and the DT device ADC data encryption control status log parameter for the encryption parameters request (EPR) bit to be set to one, or the decryption parameters request (DPR) bit to be set to one;
2) sending a SECURITY PROTOCOL OUT command specifying the Tape Data Encryption security protocol and the Set Data Encryption page to the ADC device server to provide a set of tape data encryption parameters; and
3) sending a SECURITY PROTOCOL OUT command specifying the Tape Data Encryption security protocol and the Data Encryption Parameters Complete page to the ADC device server with the clear encryption parameters request (CEPR) bit set to one or the clear decryption parameters request bit (CDPR) set to one.

4.10.4.4 Data encryption parameters required values

The ADC device server shall terminate a SECURITY PROTOCOL OUT command (see SPC-4) attempting to establish or change a set of data encryption parameters with CHECK CONDITION status, with the sense key set to ILLEGAL COMMAND, and the additional sense code set to INVALID FIELD IN PARAMETER LIST if the data encryption parameters control policy type is set to ADC exclusive and:

a) the SCOPE field (see SSC-3) is set to a value other than 10b (i.e., ALL I_T NEXUS); or
b) the LOCK bit (see SSC-3) is set to one.

4.10.4.5 Key management errors

If the automation application client processes a DT device ADC data encryption control status log parameter (see 6.1.2.4) with the encryption parameters request (EPR) bit set to one 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 (see 6.3.4.2) with the AUTOMATION COMPLETE RESULTS field set to the code indicating the reason that it was unable to provide a set of data encryption parameters for encryption.

If the automation application client processes a DT device ADC data encryption control status log parameter with the decryption parameters request (DPR) bit set to one and is unable to provide 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 AUTOMATION COMPLETE RESULTS field set to the code indicating the reason that it was unable to provide a set of data encryption parameters for decryption.

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

If the automation application client receives a DT device ADC data encryption control status log parameter with the decryption parameters request (DPR) bit set to one and:

1) provides a set of data encryption parameters for decryption; and
2) the next DT devie ADC data encryption control status log parameter contains a decryption parameters request for the same logical block (e.g., the value in the LOGICAL OBJECT NUMBER field in a Next Block Encryption Status page, see SSC-3,),

then the automation application client shall:

a) send a SECURITY PROTOCOL OUT command specifying the Tape Data Encryption security protocol and an Encryption Parameters Complete page with the AUTOMATION COMPLETE RESULTS field set to 06h (see table y+12); or
b) provide a set of data encryption parameters (e.g., a different set of data encryption parameters with the same key associated data, see SSC-3).

If the automation application client detects that the set of data encryption parameters was not correct for the next logical block and provides a set of data encryption parameters, then the automation application client shall have an encryption parameters retry limit. When the encryption parameters retry limit is reached 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 AUTOMATION COMPLETE RESULTS field set to 06h (see table y+12).

If the data encryption parameters period has expired in the DT device (e.g., 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:

1) set the ERROR TYPE field in the key management error data log parameter (see 6.1.2.5) to:
   a) 0001b (i.e., encryption parameters request error) if the encryption parameters request (EPR) bit in the DT device ADC data encryption control status log parameter (see 6.1.2.4) is set to 1; or
   b) 0010b (i.e., decryption parameters request error) if the decryption parameters request (DPR) bit in the DT device ADC data encryption control status log parameter is set to 1.
2) set the key timeout (KTO) bit in the key management error data log parameter (see 6.1.2.5) to one; and
3) set the key management error (KME) bit in the DT device ADC data encryption control status log parameter to one.

If the KME bit is set to one in the DT device ADC data encryption control status log parameter, then the automation application client should read the key management error data log parameter.

The PARAMETERS REQUEST ERROR SEQUENCE IDENTIFIER field of the key management error data log parameter indicates the sequence identifier of the request that has failed. If the PARAMETERS REQUEST SEQUENCE IDENTIFIER does not match a known sequence identifier, then the key management error was for a previous data encryption parameters request and shall be ignored. If the sequence identifier is known, then the automation application client should abort processing the DT device ADC data encryption control status log parameter with the matching sequence identifier. The parameters request sequence specified by the PARAMETERS REQUEST ERROR SEQUENCE IDENTIFIER has failed for:

a) a data encryption parameters request timeout if the KTO bit is set to one; or
b) the reason specified in the SENSE KEY field, ADDITIONAL SENSE CODE field, and the ADDITIONAL SENSE CODE QUALIFIER field if the KTO bit is set to zero.

If the abort (ABT) bit is set to one in the DT device ADC data encryption control status log parameters, then the automation application client should abort all data encryption parameters requests.

If the encryption parameters request (EPR) bit is set to one or the decryption parameters request (DPR) bit is set to one in the DT device ADC data encryption control status log parameter and a data encryption parameters request is in progress, then the automation application client should abort any data encryption parameters request with a data encryption parameters request sequence identifier that does not match the data encryption parameters request sequence identifier in the most recent DT device ADC data encryption control status log parameter.

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

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							
N								

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

6.1.2.2 Very high frequency data log parameter

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

Table 16 – Very high frequency data log parameter format

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

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

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

The PARAMETER LENGTH field shall be set to 04h.

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

The VHF data descriptor is defined in table 17.

Table 17 – VHF data descriptor

Byte \ Bit	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 are 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 with either the ENCRYPTION MODE field set to a value other than DISABLE (see SSC-3) or the DECRYPTION MODE field set to a value other than DISABLE (see SSC-3) associated with any I_T nexus or a DT device management interface. An EPP bit set to zero indicates that the DT device does not have a set of saved data encryption parameters with either the ENCRYPTION MODE field set to a value other than DISABLE or the DECRYPTION MODE field set to a value other than DISABLE associated with any I_T nexus or a DT device management interface.

An encryption service request (ESR) bit set to one indicates that:

a) at least one bit in the SERVICE REQUEST INDICATORS field in the DT device ADC data encryption control status log parameter has been set to one since the last retrieval of the DT device ADC data encryption control status log parameter (see 6.1.2.4) by this I_T nexus; and
b) at least one bit in the SERVICE REQUEST INDICATORS field in the DT device ADC data encryption control status log parameter is set to one.

The ADC device server sets the ESR bit to zero after retrieval of the DT device ADC data 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 DT device ADC data encryption control status log parameters have been set to one since the last retrieval of the DT device ADC data encryption control status log parameter by this I_T nexus or that no bits in the SERVICE REQUEST INDICATORS field in the DT device ADC data encryption control status log parameter are set to one.

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 DT device ADC data encryption control status log parameter

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

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

Byte \ Bit	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	(MSB)			PARAMETERS REQUEST SEQUENCE IDENTIFIER				
9								(LSB)
10	Reserved							
11								

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

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

The PARAMETER LENGTH field shall be set to 08h.

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

Table y + 2: SERVICE REQUEST INDICATORS field

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

An encryption parameters request (EPR) bit set to one indicates that the ADC device server requests a set of data encryption parameters for encryption from the automation application client. The ADC device server shall set the EPR bit to one when the DT device indicates a set of data encryption parameters for encryption is required (e.g., the DT device includes an SSC-3 compliant device server and has the data encryption parameters for encryption request indicator set to TRUE, see SSC-3). If the EPR bit is set to one, then the automation application client should abort any data encryption parameters request in progress with a data encryption parameters request identifier that is different from the value specified in the PARAMETERS REQUEST SEQUENCE IDENTIFIER field. If the EPR bit is set to one, then the abort (ABT) bit shall be set to zero.

A EPR bit set to zero indicates that the ADC device server does not request a set of data encryption parameters for encryption from the automation application client. The ADC device server shall set the EPR bit to zero and shall set the data encryption parameters for encryption request indicator in the DT device to FALSE when:

a) it successfully processes a SECURITY PROTOCOL OUT command, with the SECURITY PROTOCOL field set to Tape Data Encryption and with the clear encryption parameters request (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 Tape Data Encryption and with the AUTOMATION COMPLETE RESULTS field in an Encryption Parameters Complete page set to a non-zero value; or
c) the data encryption parameters for encryption indicator in the DT device is set to FALSE (e.g., the DT Device includes an SSC-3 compliant device server and has set the data encryption parameters for encryption indicator to FALSE after a data encryption parameters timer has expired).

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

A decryption parameters request (DPR) bit set to one indicates that the ADC 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 one when the DT device indicates a set of data encryption parameters for decryption is required (e.g., the DT device includes an SSC-3 compliant device server and has the data encryption parameters for encryption request indicator set to TRUE, see SSC-3). If the DPR bit is set to one, then the automation application client should abort any data encryption parameters request in progress with a data encryption parameters request identifier that is different from the value specified in the PARAMETERS REQUEST SEQUENCE IDENTIFIER field. If the DPR bit is set to one, then the ABT bit shall be set to zero.

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

a) it successfully processes a SECURITY PROTOCOL OUT command, with the SECURITY PROTOCOL field set to Tape Data Encryption and with the clear decryption parameters request (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 Tape Data Encryption and with the AUTOMATION COMPLETE RESULTS field in an Encryption Parameters Complete page set to a non-zero value; or
c) the data encryption parameters for decryption indicator in the DT device is set to FALSE (e.g., the DT Device includes an SSC-3 compliant device server and has set the data encryption parameters for decryption indicator to FALSE after a data encryption parameters timer has expired).

A key management error (KME) bit set to one indicates that the ERROR TYPE field in the key management error data log parameters (see 6.1.2.5) is set to a non-zero value. If the KME bit is set to one, then the ABT bit shall be set to zero.

The ADC device server shall set the KME bit to zero when the ERROR TYPE field in the key management error data log parameter is set to zero.

If the encryption parameters request (EPR) bit is set to one or the decryption parameters request (DPR) bit is set to one, and the KME bit is set to one, then the automation application client should process the key management error before processing the encryption parameters request.

The ADC device server shall set the abort (ABT) bit to one when the DT device notifies the ADC device server that the data encryption parameters request associated with the sequence identifier in the PARAMETERS REQUEST SEQUENCE IDENTIFIER field has been aborted. If the the ABT bit is set to one, then the automation application client should abort processing the data encryption parameters request with the sequence identifier that matches the value in the PARAMETERS REQUEST SEQUENCE IDENTIFIER field. An ABT bit set to one shall not affect the current set of data encryption parameters. If the ABT bit is set to one, then:

a) the encryption parameters request (EPR) bit shall be set to zero;
b) the decryption parameters request (DPR) bit shall be set to zero; and
c) the key management error (KME) bit shall be set to zero.

The ADC device server shall set the ABT bit to zero upon successful completion of a SECURITY PROTOCOL OUT command specifying the Tape Data Encryption security protocol and the Data Encryption Parameters Complete page with a sequence identifier that matches the sequence identifier value in the PARAMETERS REQUEST SEQUENCE IDENTIFIER field and the clear abort (CABT) bit set to one.

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

The automation application client may support aborting processing of data encryption parameters requests. If the ABT bit is set to one, and the application client supports aborting processing of data encryption parameters requests, then the automation application client shall send a SECURITY PROTOCOL OUT command specifying the Tape Data Encryption security protocol and the Data Encryption Parameters Complete page with a sequence identifier that matches the sequence identifier value in the PARAMETERS REQUEST SEQUENCE IDENTIFIER field and the CABT bit set to one when:

a) the automation application client processes the abort event and aborts processing the data encryption parameters request with the sequence identifier that matches the value in the PARAMETERS REQUEST SEQUENCE IDENTIFIER field; or
b) the automation application client attempts to process the abort event and there is no matching parameters request sequence identifier (e.g., the automation application client completed processing the data encryption parameters request before starting to process the abort event).

If the ABT bit is set to one and the automation application client does not process the data encryption parameters abort event, then the ABT bit shall remain set until:

a) the next data encryption parameters request; or
b) a hard reset condition.

The PARAMETERS REQUEST SEQUENCE IDENTIFIER field shall contain:

a) a value assigned by the ADC device server to uniquely identify the data encryption parameters request if the encryption parameters request (EPR) bit is set to one;
b) a value assigned by the ADC device server to uniquely identify the data encryption parameters request if the decryption parameters request (DPR) bit is set to one; or
c) the value assigned by the ADC device server that uniquely identifies the data encryption parameters request that has been aborted by the ADC device server if the ABT bit is set to one.

The PARAMETERS REQUEST SEQUENCE IDENTIFIER field shall be set to zero if:

a) the encryption parameters request (EPR) bit is set to zero;
b) the decryption parameters request (DPR) bit is set to zero; and
c) the abort (ABT) bit is set to zero.

The DT device ADC data encryption control status log parameter shall not be changed with the use of a LOG SELECT command.

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

6.1.2.5 Key management error data log parameter

If the key management error (KME) bit is set to one in the DT device ADC data 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 (0003h)				
1								(LSB)
2	DU (0)	DS (1)	TSD (0)	ETC (0)	TMC (00)		LBIN (1)	LP (1)
3	PARAMETER LENGTH (0Ch)							
4	ERROR TYPE				KTO	Reserved		
5	Reserved							
6	(MSB)			PARAMETERS REQUEST ERROR SEQUENCE IDENTIFIER				
9								(LSB)
10	Reserved				SENSE KEY			
11	ADDITIONAL SENSE CODE							
12	ADDITIONAL SENSE CODE QUALIFIER							
13	Reserved							
15								

The PARAMETER CODE field shall be set to 0003h 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 0Ch.

The key timeout (KTO) bit set to one indicates that the data encryption period timer expired indicator in the DT device is set to TRUE. The KTO bit set to zero indicates that the encryption parameters period expired indicator in the DT device is set to FALSE. The KTO bit shall be set to zero:

a) if the event that caused the key management error (KME) bit to be set to one in the DT device ADC data encryption control status log parameter was not caused by an encryption parameters period expired indicator in the DT device; or
b) upon successfully processing a SECURITY PROTOCOL OUT command specifying the Tape Data Encryption security protocol and the Data Encryption Parameters Complete page with the clear key management error (CKME) bit set to one.

The ERROR TYPE field indicates the type of the last key management error event (see 4.10.4.5). The error types defined for the ERROR TYPE field are shown in table y+4.

Table y+4 – ERROR TYPE field value

Code	Description
0000b	No error
0001b	encryption parameters request error
0010b	decryption parameters request error
0011b – 1011b	Reserved
1100b – 111b	Vendor specific

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

The ADC 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 clear key management error (CKME) bit set to one; or
d) a hard reset condition (see SAM-3).

The PARAMETERS REQUEST ERROR SEQUENCE IDENTIFIER field shall contain the encryption parameters request sequence identifier assigned by the ADC device server that uniquely identifies the data encryption parameters request associated with the last key management error event.

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 DT device ADC data encryption control status log parameter.

The key management error data log parameter data shall not be changed with the use of a LOG SELECT command.

If the ERROR TYPE field is set to zero, then the 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 (see SPC-4).

6.3.2 SECURITY PROTOCOL IN command specifying Tape Data Encryption security protocol

The SECURITY PROTOCOL IN command (see SPC-4) specifying Tape Data Encryption security protocol (i.e., 20h) requests the ADC 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.

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

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

Table y+5 – SECURITY PROTOCOL SPECIFIC field values

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 ADC 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.

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

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

Table y+6 – SECURITY PROTOCOL SPECIFIC field values

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

Byte \ Bit	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	(MSB)			Data Encryption Configuration In Support page code (first)				
5								(LSB)
n-1	(MSB)			Data Encryption Configuration In Support page code (last)				
n								(LSB)

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 ADC device server supports for the SECURITY PROTOCOL IN command specifying the Data Encryption Configuration security protocol in ascending order beginning with page code 0000h (see table y+6).

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	(MSB)			Data Encryption Configuration Out Support page code (first)				
5								(LSB)
n-1	(MSB)			Data Encryption Configuration Out Support page code (last)				
n								(LSB)

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 ADC device server supports for the SECURITY PROTOCOL OUT command specifying the Data Encryption Configuration security protocol in ascending order (see table y+13).

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	Reserved				CONTROL POLICY CODE			
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 CONTROL POLICY CODE field (see table y) contains information on the data encryption parameters control policy (see 4.10.1). 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.

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

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+10) specifies the page that the application client is sending.

Table y+10 – 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, 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.

6.3.4.2 Data Encryption Parameters Complete page.

Table y+11 specifies the format of the Data Encryption Parameters Complete page.

Table y+11 – Data Encryption Parameters Complete page

Byte \ Bit	7	6	5	4	3	2	1	0
0	(MSB)			PAGE CODE (0030h)				
1								(LSB)
2	(MSB)			PAGE LENGTH (10h)				
3								(LSB)
4	AUTOMATION COMPLETE RESULTS							
5	Reserved							
6	Reserved				CABT	CKME	CEPR	CDPR
7	Reserved							
8	(MSB)			PARAMETERS REQUEST SEQUENCE IDENTIFIER				
11								(LSB)
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.

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

The AUTOMATION COMPLETE RESULTS field indicates the results of the data encryption parameters request with the request identifier matching the value in the PARAMETERS REQUEST SEQUENCE IDENTIFIER field and is described in table y+12.

Table y+12 – AUTOMATION COMPLETE RESULTS field value

Code	Description
00h	No results
01h	The automation application client has successfully completed servicing the request.
02h	The automation application client has experienced an unknown error servicing the request.
03h	The automation application client experienced an unrecoverable error in attempting to access the key manager.
04h	The key manager returned an error status when access to the key was attempted.
05h	The requested key was not found.
06h	A set of data encryption parameters was provided but the DT device was not able to process any logical blocks using the set of data encryption paremeters (see 4.10.4.5).
07h	Request not authorized (e.g. the automation application client received an encryption parameters for encryption request and the volume mounted in the DT device does not support encryption but the policy is set to encrypt all data).
08h – EFh	Reserved
F0h – FFh	Vendor specific

If the AUTOMATION COMPLETE RESULTS field is set to 00h, then:

a) the clear abort (CABT) bit shall be set to one;
b) the clear key management error (CKME) bit shall be set to one;
c) the clear encryption parameters request (CEPR) bit shall be set to one; or
d) the clear decryption parameters request (CDPR) bit shall be set to one;

The ADC device server shall terminate the command with CHECK CONDITION status, with the sense key set to ILLEGAL REQUEST, and the addition sense code set to INVALID FIELD IN PARAMETERS LIST if the AUTOMATION COMPLETE RESULTS field is set to 00h, and:

a) the CABT bit is set to zero;
b) the CKME bit is set to zero;
c) the CEPR bit is set to zero; and
d) the CDPR bit is set to zero;

The ADC device server:

1) shall set the external data encryption control additional sense code (e.g., see SSC-3) in the DT device to:

   a) EXTERNAL DATA ENCRYPTION KEY MANAGER ACCESS ERROR if an AUTOMATION COMPLETE RESULTS value of 03h is reported;
   b) EXTERNAL DATA ENCRYPTION KEY MANAGER ERROR if an AUTOMATION COMPLETE RESULTS value of 04h is reported;
   c) EXTERNAL DATA ENCRYPTION KEY NOT FOUND if an AUTOMATION COMPLETE RESULTS value of 05h is reported;
   d) INCORRECT DATA ENCRYPTION KEY if an AUTOMATION COMPLETE RESULTS value of 06h is reported;
   e) LOGICAL UNIT ACCESS NOT AUTHORIZED if an AUTOMATION COMPLETE RESULTS value of 07h is reported; or

Comment: It was requested at the working group meeting that I not use the LOGICAL UNIT ACCESS NOT AUTHORIZED additional sense but I contacted the author of the proposal that introduced it and there is no use of this code yet but the planned use is exactly the case we have here where a security setting prevents the current read or write command but other access is allowed. If necessary we may ask if the name can be changed but I don't want to request a new additional sense code with the exact same meaning as an existing code.

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

2) may set the external data encryption control additional sense code in the DT device to an additional sense code other than NO ADDITIONAL SENSE INFORMATION if an AUTOMATION COMPLETE RESULTS value of F0h – FFh is reported; or

3) shall set the external data encryption control additional sense code in the DT device to EXTERNAL DATA ENCRYPTION CONTROL ERROR.

Comment: EXTERNAL DATA ENCRYPTION KEY MANAGER ACCESS ERROR, EXTERNAL DATA ENCRYPTION KEY MANAGER ERROR, and EXTERNAL DATA ENCRYPTION KEY NOT FOUND are new additional sense codes.

A clear abort (CABT) bit set to one indicates that the ABT bit in the DT device ADC data encryption control status log parameter shall be set to zero. A CABT bit set to zero does not indicate that the ABT bit in the DT device ADC data encryption control status log parameter shall be set to zero.

A clear key management error (CKME) bit set to one indicates that the key management error (KME) bit in the DT device ADC data encryption control status log parameter shall be set to zero. If the CKME bit is set to one, then:

a) the key timeout KTO bit and the ERROR TYPE field in the key management error data log parameter shall be set to zero; and
b) the data encryption parameters period expired indicator in the DT device shall be set to FALSE.

A CKME bit set to zero does not indicate that the KME bit in the DT device ADC data encryption control status log parameter shall be set to zero.

If the clear encryption parameters request (CEPR) bit is set to one and the encryption parameters request sequence identifier matches the encryption parameters request sequence identifier in the DT device ADC data encryption control status log parameter, then the ADC device server shall set the encryption parameters request (EPR) bit in the DT device ADC data encryption control status log page to zero and shall set the encryption parameters for encryption request indicator in the DT device to FALSE. If the encryption parameters request sequence identifier does not match the encryption parameters request indicator in the DT device ADC data encryption control status log parameter, then the ADC device server shall ignore the CEPR bit. If the CEPR bit is set to zero, then the ADC device server is not being requested to clear the encryption parameters for encryption request for the indicated key request sequence.

If the clear decryption parameters request (CDPR) bit is set to one and the encryption parameters request sequence identifier matches the encryption parameters request sequence identifier in the DT device ADC data encryption control status log parameter, then the ADC device server shall set the decryption parameters request (DPR) bit in the DT device ADC data encryption control status log page to zero and shall set the encryption parameters for decryption request indicator in the DT device to FALSE. If the encryption parameters request sequence identifier does not match the encryption parameters request indicator in the DT device ADC data encryption control status log parameter, then the ADC device server shall ignore the CDPR bit. If the CDPR bit is set to zero, then the ADC device server is not being requested to clear the encryption parameters for decryption key request for the indicated key request sequence.

The PARAMETERS REQUEST SEQUENCE IDENTIFIER field shall contain the data encryption parameters sequence identifier for the data encryption parameters request that corresponds 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 a value of 21h (i.e., the Data Encryption Configuration security protocol) 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.

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

The SECURITY PROTOCOL SPECIFIC field (see table y+13) specifies the page that the application client is sending.

Table y+13 – SECURITY PROTOCOL SPECIFIC field value

Code	Description	Support	Reference
0000h – 000Fh	Reserved		
0010h	Configure Data Encryption Algorithm Support page	O	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 an 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+14 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 a DT device management interface, 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.

Table y+14 – Configure Data Encryption Algorithm Support page

Byte \ Bit	7	6	5	4	3	2	1	0
0	(MSB)			PAGE CODE (0010h)				
1								(LSB)
2	(MSB)			PAGE LENGTH (n-3)				
3								(LSB)
4				Reserved				
19								
Encryption Algorithm Support descriptor list								
20	Encryption Algorithm Support descriptor (first)							
n	Encryption Algorithm Support descriptor (last)							

The PAGE CODE field shall be set to 0010h to indicate the Configure Data Encryption Algorithm Support page.

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

Each Encryption Algorithm Support descriptor (see table y+15) shall contain configuration settings for a data encryption algorithm supported by the DT device. If more than one descriptor is included, then 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.

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

Table y+15 – Encryption Algorithm Support descriptor

Byte \ Bit	7	6	5	4	3	2	1	0
0	ALGORITHM INDEX							
1	Reserved							
2	(MSB)			DESCRIPTOR LENGTH (0004h)				
3								(LSB)
4	DISABLE	Reserved						
5	Reserved							
7								

The ALGORITHM INDEX field specifies which of the data 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 data encryption algorithm, 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.

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

A DISABLE bit set to one specifies that the DT device shall disable the data encryption algorithm for the algorithm index in the ALGORITHM INDEX field (e.g., 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 DECRYPT_C field set to no capability and the ENCRYPT_C set to no capability, see SSC-3). A DISABLE bit set to zero specifies that the DT device shall not disable the specified encryption algorithm. If the DISABLE bit is set to zero, then the DT device shall enable the specified data encryption algorithm.

6.3.5.3 Configure Encryption Policy page

Table y+16 specifies the format of the Configure Encryption Policy page.

Table y+16 – Configure Encryption Policy page

Byte \ Bit	7	6	5	4	3	2	1	0
0	(MSB)			PAGE CODE (0011h)				
1								(LSB)
2	(MSB)			PAGE LENGTH (8)				
3								(LSB)
4	Reserved				CONTROL POLICY CODE			
5	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 CONTROL POLICY CODE field specifies the data encryption parameters control policy for the DT device (see 4.10.1). If the DT device has a saved set of data encryption parameters or has a volume mounted 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 PARAMETER LIST.

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

Upon successful processing of a Configure Encryption Policy page with the CONTROL POLICY CODE field set to a policy code for the Open policy type or a policy code for the RMC exclusive policy type, then the DT device shall clear the set of data encryption parameters associated with this I_T nexus, and the ADC device server shall:

a) set the encryption parameters request indicator in the DT device to zero;
b) set the decryption parameters request indicator in the DT device to zero;
c) set the encryption parameters request (EPR) bit, decryption parameters request bit (DPR) bit, key management error bit (KME), and the abort (ABT) bit in the DT device ADC data encryption control status log parameter to zero; and
d) set the key timeout (KTO) bit to zero and the ERROR TYPE field to 00b in the key management error data log parameter.

The DECRYPTION PARAMETERS REQUEST POLICY field specifies the policy that the DT device shall use for requesting 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+17.

Table y+17 – DECRYPTION PARAMETERS REQUEST POLICY field values

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

The ENCRYPTION PARAMETERS REQUEST POLICY field specifies the policy that the DT device shall use for requesting a set of data encryption parameters for encryption from the automation application client (see SSC-3). The encryption parameters request policy values are defined in table y+18.

Table y+18 – ENCRYPTION PARAMETERS REQUEST POLICY field values

Value	Policy Name (see SSC-3)	Reference
000b	No data encryption parameters request	SSC-3
001b	Request data encryption parameters every reposition	SSC-3
010b	Request data encryption parameters when not set	SSC-3
011b – 111b	Reserved	

The ENCRYPTION PARAMETERS REQUEST PERIOD field indicates the maximum time, in 100 millisecond increments, the DT device shall wait after requesting a set of data encryption parameters for encryption (see 6.1.2.4) or requesting a set of data encryption parameters 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). An ENCRYPTION PARAMETERS REQUEST PERIOD field value of 0000h indicates the data encryption parameters request period shall be infinite.

If the CONTROL POLICY CODE field is set to a policy code for the Open policy type or is set to a policy code for the RMC exclusive policy type, then the DECRYPTION PARAMETERS REQUEST POLICY, ENCRYPTION PARAMETERS REQUEST POLICY, and ENCRYPTION PARAMETERS REQUEST PERIOD fields shall be ignored.