memorandum

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

T10/07-164r8

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

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

Related Documents

adc2r07e – Automation/Drive Interface Commands

ssc3r03e – SCSI Stream Commands

07-361r5 – 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.

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 tape data encryption parameters via the ADC device server. Controlling tape data encryption capabilities or tape 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 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 may use ADC tape data encryption control to control the tape data encryption capabilities of the DT device or to control both the tape data encryption capabilities 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 establishment of data encryption parameters within the physical device.

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

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

Table y – Data encryption parameters control policies

Policy	Code	Description
Unknown	0000b	The data encryption parameters control policy is unknown.
Open	0001b	No interface has taken exclusive control of data encryption parameters. This is the default setting for the data encryption parameters control policy. The DT device shall accept configuration of data encryption parameters from any device server or DT device management interface.
ADC exclusive	0010b	Configuration of data encryption parameters is exclusive to the ADC device server. The DT device shall: a) accept configuration of data encryption parameters from the ADC device server; and b) reject configuration of data encryption parameters from an RMC device server or DT device management interface.
ADC exclusive with algorithms removed	0011b	Configuration of data encryption parameters is exclusive to the ADC device server and all algorithms are removed from the list of algorithms reported by the DT device. The DT device shall: a) remove all algorithms from the list of algorithms reported by the RMC device server; b) accept configuration of data encryption parameters from the ADC device server; and c) reject configuration of data encryption parameters from an RMC device server or DT device management interface.
DT device management interface exclusive	0101b	Configuration of data encryption parameters is exclusive to the DT device management interface. The DT device shall: a) accept configuration of data encryption parameters from the DT device management interface; and b) reject configuration of data encryption parameters from an ADC device server or DT device management interface.
DT device management interface exclusive with algorithms removed	0101b	Configuration of data encryption parameters is exclusive to the DT device management interface and all algorithms are removed from the list of algorithms reported by the DT device. The DT device shall: a) remove all algorithms from the list of algorithms reported by the RMC device server; b) accept configuration of data encryption parameters from the DT device management interface; and c) reject configuration of data encryption parameters from an ADC device server or DT device management interface.
RMC exclusive	0110b	Configuration of data encryption parameters is exclusive to the RMC device server. The DT device shall: a) accept configuration of data encryption parameters from the RMC device server; and b) reject configuration of data encryption parameters from an ADC device server or DT device management interface.
Undefined	0111b – 1111b	Reserved

The data encryption parameters control policy 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

4.10.2 ADC tape data encryption control of data encryption capabilities

4.10.2.1 ADC tape data encryption control of tape 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 establish or change data encryption parameters. ADC tape data encryption control may be used to configure parameters in the DT device that change the tape 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) establish exclusive control of the configuration of data encryption parameters for the ADC device server, and remove all of the algorithms from the list of algorithms reported by the DT device (see 4.10.2.2); and
c) disable data encryption algorithms (see 4.10.2.3).

4.10.2.2 Setting tape data encryption control to ADC exclusive

The data encryption parameters control policy (see 4.10.1) should be set to ADC exclusive before data encryption parameters are established by an automation application client. The data encryption parameters control policy 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 (see 6.3.5.3) to the ADC device server with:

a) the CONTROL POLICY CODE field set to ADC exclusive (see 4.10.1); or
b) the CONTROL POLICY CODE field set to ADC exclusive with algorithms removed.

If the data encryption parameters control policy is ADC exclusive, then the automation application client may set the data encryption parameters control policy to open 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 Open.

4.10.2.3 Disabling 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 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).

4.10.3 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 a page that provides a set of data encryption parameters may be 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).

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

4.10.3.2 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 data encryption control status log parameter (see 6.1.2.4).

4.10.3.3 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), then the ADC device server shall:

1) set the EPR bit in the DT device ADC data encryption control status log parameter to one; 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), then the ADC device server shall:

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

4.10.3.4 Data encryption parameters required values

The ADC device server shall terminate a command 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 is set to ADC exclusive and:

a) the SCOPE field is set to a value other than 10b (i.e., ALL_I_T_NEXUS); or
b) the LOCK bit is set to one.

4.10.3.5 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 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 decryption parameters error (DPE) bit set to one.

The automation application client may retry the decryption key request. If the automation application client performs a retry on a decryption parameters request, then the automation application client shall have an encryption parameters retry limit and shall send a SECURITY PROTOCOL OUT command specifying the Tape Data Encryption security protocol and an Encryption Parameters Complete page with the decryption parameters error (DPE) bit set to one when the retry limit is reached.

If the encryption parameters period has expired in the DT device (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 DT device ADC data 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 DT device ADC data 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 DT device ADC encryption control status log parameter is set to one, then a command has failed for a data encryption parameters request timeout and the automation application client should abort the data encryption parameters request with the matching PARAMETERS REQUEST SEQUENCE IDENTIFIER. If the KTO bit is set to zero, then the automation application client should compare the data encryption parameters request sequence identifier specified in the PARAMETERS REQUEST SEQUENCE IDENTIFIER field with the

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

data encryption parameters request sequence identifier from the most recent DT device ADC data encryption control status log parameter received with a EPR bit set to one or a DPR bit set to one. If the data encryption parameters request sequence identifier matches, then the command that caused the EPR bit to be set to one or the command that caused the DPR bit set to one has failed for the reason specified in the SENSE KEY field, ADDITIONAL SENSE CODE field, and the ADDITIONAL SENSE CODE QUALIFIER field. If the data encryption parameters request sequence identifier does not match the data encryption parameters request sequence identifier from the most recent DT device ADC data encryption control status log parameter received, then the key management error was for a previous data encryption parameters request and shall be ignored.

If the 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 an EPR bit is set to one or a 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.

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~~4~~h-00FFh	Reserved	
100h	Obsolete	
0101h – 0200h	DT device primary port status	6.1.2.~~4~~6
0201h – 7FFFh	Reserved	
8000h – FFFFh	Vendor specific	

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

6.1.2.2 Very high frequency data log parameter

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

Table 16 – Very high frequency data log parameter format

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

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

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

The PARAMETER LENGTH field shall be set to 04h.

The VHF data descriptor is defined in table 17.

Table 17 – VHF data descriptor

Bit / Byte	7	6	5	4	3	2	1	0
0	PAMR	HIU	MACC	CMPR	WRTP	CRQST	CRQRD	DINIT
1	INXTN	Rsvd	RAA	MPRSNT	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 or the DECRYPTION MODE field set to a value other than DISABLE. 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 or the DECRYPTION MODE field set to a value other than DISABLE (see SSC-3).

An encryption service request (ESR) bit set to one indicates that 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. The ADC device server shall set the ESR bit to zero after successful completion of a command requesting 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.

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

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	(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

Bit / Byte	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 may 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 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 encryption parameters error (EPE) bit in an Encryption Parameters Complete page set to one; 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 may 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 decryption parameters error (DPE) bit in an Encryption Parameters Complete page set to one; 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:

a) The data encryption parameters period has expired (e.g., the DT Device includes an SSC-3 compliant device server and has the data encryption period timer expired indicator set to TRUE); or
b) other vendor specific events.

If the KME bit is set to one, then the key management error data log parameter shall contain information about the key management error. The PARAMETERS REQUEST ERROR SEQUENCE IDENTIFIER in the key management error data log parameter shall be used to identify the data encryption parameters request that has completed with a key management error. 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:

a) after 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; or
b) as part of the processing of a Hard Reset condition.

If the EPR bit is set to one or the 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 DT device shall set the ABT bit to one when the command that initiated the data encryption parameters request specified by the PARAMETERS REQUEST SEQUENCE IDENTIFIER field has been aborted and the application client may abort the encryption parameters request with the sequence identifier that matches the value in the PARAMETERS REQUEST SEQUENCE IDENTIFIER field. If the ABT bit is set to one, then the EPR bit shall be set to zero, the DPR bit shall be set to zero, and the KME bit shall be set to zero. An ABT bit set to one shall not affect the current set of data encryption parameters. The ADC device server shall set the ABT bit to zero upon completion of a SECURITY PROTOCOL OUT command specifying the Tape Data Encryption security protocol and the Encryption Parameters Complete page with a sequence identifier that matches the sequence identifier value in the PARAMETERS REQUEST SEQUENCE IDENTIFIER field.

Note: If the automation application client aborts a parameters request following receipt of an ABT bit set to one with a matching sequence identifier, then the automation application client may never send an Encryption Parameters Complete page for that sequence and the ABT bit will be set until the next parameters request.

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

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 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 DPR bit is set to one; or
c) the value assigned to the data encryption parameters request that has completed with abort status if the ABT bit is set to one.

The DT device ADC data encryption control status log parameter shall not be 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 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

Byte \ Bit	7	6	5	4	3	2	1	0
0	(MSB)							
1	PARAMETER CODE (0003h)							(LSB)
2	DU (0)	DS (1)	TSD (0)	ETC (0)	TMC (00)		LBIN (1)	LP (1)
3	PARAMETER LENGTH (0Ch)							
4	Reserved				KTO	ERROR TYPE		
5	Reserved							
6	(MSB)							
9	PARAMETERS REQUEST ERROR SEQUENCE IDENTIFIER							(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 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.

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 DT device ADC data encryption control status log parameter was caused by an encryption parameters period expired indicator in the DT device (see 4.10.3.5). 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.

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

The ERROR TYPE field indicates the type of the last event that caused the key management error (KME) bit in the DT device ADC data encryption control status log parameter to be set to one. The error types defined for the ERROR TYPE field 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	Reserved
100b – 111b	Vendor specific

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 Event (see SAM-3).

The PARAMETERS REQUEST ERROR SEQUENCE IDENTIFIER field shall contain the value assigned by the ADC device server in the DT device ADC data encryption control status log parameter to identify the data encryption parameters request associated with the event that caused the KME bit in the DT device ADC data 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 DT device 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 (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	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 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.

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

Byte \ Bit	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 ADC 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

Byte \ Bit	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			EPE	DPE	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 REQUEST 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 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	The encryption parameters retry limit was reached (see 4.10.3.5).
06h – 7Fh	Reserved
80h – FFh	Vendor specific

The ADC device server shall set an external data encryption control additional sense code (see SSC-3) in the DT device to:

a) EXTERNAL DATA ENCRYPTION KEY MANAGER ACCESS ERROR if an AUTOMATION COMPLETE RESULTS value of 02h is reported;
b) EXTERNAL DATA ENCRYPTION KEY MANAGER ERROR if an AUTOMATION COMPLETE RESULTS value of 03h is reported;
c) EXTERNAL DATA ENCRYPTION KEY NOT FOUND if an AUTOMATION COMPLETE RESULTS value of 04h is reported;
d) EXTERNAL DATA ENCRYPTION KEY RETRY LIMIT REACHED if an AUTOMATION COMPLETE RESULTS value of 05h is reported; or
e) EXTERNAL DATA ENCRYPTION CONTROL ERROR.

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. An EPE bit set to zero indicates that the automation application client did not encounter 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 request. A DPE bit set to zero indicates that the automation application client did not encounter an error while processing a data encryption parameters for decryption request.

A clear key management error (CKME) bit is set to one indicates that the 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 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.

If the CKME bit is set to zero, then:

a) the KME bit in the DT device ADC data encryption control status log parameter shall not be changed; and
b) the KTO bit and the ERROR TYPE field in the key management error data log parameter shall not be changed.

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 for the most recent DT device ADC data encryption control status log parameters, then the ADC device server shall set the 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 for the most recent DT device ADC data encryption control status log parameters, then the ADC device server shall ignore the CEPR bit. If the CEPR bit is set to zero, then the encryption parameters for encryption request for the indicated key request sequence shall not be cleared.

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 for the most recent DT device ADC data encryption control status log parameters, then the ADC device server shall set the DPR bit in the DT device ADC data encryption control status log

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

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 for the most recent DT device ADC data encryption control status log parameters, then the ADC device server shall ignore the CDPR bit. If the CDPR bit is set to zero, then the encryption parameters for decryption key request for the indicated key request sequence shall not be cleared.

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 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+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, 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+14 – 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				
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.

Table y+15 – 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.

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 indicates that the DT device shall disable the data encryption algorithm for the algorithm index in the ALGORITHM INDEX field (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). A DISABLE bit set to zero indicates that the DT device shall not disable the specified

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

encryption algorithm. If the DISABLE bit is set to zero and the specified data encryption algorithm is disabled, 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 (see table y) specifies the encryption control policy of the DT Device. 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 if the CONTROL POLICY CODE field is set to Open and:

a) the encryption parameters request (EPR) bit in the DT device ADC encryption control status log parameter is set to one; or
b) the decryption parameters request (DPR) bit in the DT device ADC encryption control status log parameter is set to one.

Upon successful processing of a Configure Encryption Policy page with the CONTROL POLICY CODE field set to Open, the DT device shall clear the set of data encryption parameters associated with the ADC device server, and the ADC device server shall:

a) clear the encryption parameters request indicator in the DT device;
b) clear the decryption parameters request indicator in the DT device;
c) clear 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; and
d) clear the key timeout (KTO) bit and the ERROR TYPE field 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)
000b	No data decryption parameters request
001b	Request data decryption parameters as needed
010b – 111b	

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

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)
000b	No data encryption parameters request
001b	Request data encryption parameters every reposition
010b	Request data encryption parameters when not set
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 not set to ADC exclusive, then the DECRYPTION PARAMETERS REQUEST POLICY, ENCRYPTION PARAMETERS REQUEST POLICY, and ENCRYPTION PARAMETERS REQUEST PERIOD fields shall be ignored.