memorandum

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

T10/08-200r1

To	From	Subject	Date
INCITS T10 Committee	Curtis Ballard, HP	ADC-3 Clarifications for automation encryption control	6 June, 2008

Revision History
Revision 0 – Initial document

Revision 1 – Changes from ADI working group meeting May, 2008 San Jose, CA. See 08-223 for details

Related Documents
ADC3r00a – Automation/Drive Interface Commands

Background
The document will be used to capture any areas where clarification to the automation encryption control specification is required.

Proposed Changes to ADC-3 section 6.1.2.4

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 21.

Table 21 – 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 21.

The PARAMETER LENGTH field shall be set to 08h.

The SERVICE REQUEST INDICATORS field is shown in table 22.

Table 22: SERVICE REQUEST INDICATORS field

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

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

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.

An 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).

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 sequence 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 value in the PARAMETERS REQUEST SEQUENCE IDENTIFIER field has been aborted. If the ABT bit is set to one, then the automation application client should abort processing the data encryption parameters

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

request associated with 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 the clear abort (CABT) bit set to one.

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 data encryption parameters request 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 data encryption parameters request 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 data encryption 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 remains set until:

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

The PARAMETERS REQUEST SEQUENCE IDENTIFIER field shall contain the data encryption parameters request sequence identifier:

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

The data encryption parameters request sequence identifier shall be a value assigned by the ADC device server that uniquely identifies the data encryption parameters request.

~~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 PARAMETERS REQUEST SEQUENCE IDENTIFIER field shall be ignored if:

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

Proposed Changes to ADC-3 section 6.3.2.4

6.3.2.4 Data Encryption Parameters Complete page.

Table 67 specifies the format of the Data Encryption Parameters Complete page.

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

Table 67 – Data Encryption Parameters Complete page

Bit / Byte	7	6	5	4	3	2	1	0
0	(MSB)			PAGE CODE (0030h)				
1								(LSB)
2	(MSB)			PAGE LENGTH (0Ch)				
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.

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. The AUTOMATION COMPLETE RESULTS field shall be set to a value specified in table 68.

Table 68 – Automation complete results codes

Code	Description	Additional sense code
00h	No results (e.g., the automation application client has set the CABT bit to one)	n/a
01h	The automation application client has successfully completed servicing the request.	n/a
02h	The automation application client has experienced an unknown error servicing the request.	EXTERNAL DATA ENCRYPTION CONTROL ERROR
03h	The automation application client experienced an unrecoverable error in attempting to access the key manager.	EXTERNAL DATA ENCRYPTION KEY MANAGER ACCESS ERROR
04h	The key manager returned an error status when access to the key was attempted.	EXTERNAL DATA ENCRYPTION KEY MANAGER ERROR
05h	The requested key was not found.	EXTERNAL DATA ENCRYPTION KEY 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).	INCORRECT DATA ENCRYPTION KEY
07h	Request not authorized (~~e.g.~~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).	EXTERNAL DATA ENCRYPTION REQUEST NOT AUTHORIZED
08h – EFh	Reserved	Reserved
F0h – FFh	Vendor specific	Vendor specific

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

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 additional 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 value specified in table 68; or

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

No further changes are proposed to this section

Proposed Changes to ADC-3 section 6.3.5.2

6.3.5.2 Configure Data Encryption Algorithm Support page.

Table 70 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 PARAMETER LIST~~CDB~~, and the sense key specific FIELD POINTER field set to the PAGE CODE field.

Table 70 – 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)							

No further changes are proposed to this section

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

Proposed Changes to ADC-3 section 6.3.5.3

6.3.5.3 Configure Encryption Policy page.

Table 72 specifies the format of the Configure Encryption Policy page.

Table 72 – Configure Encryption Policy page

Bit / Byte	7	6	5	4	3	2	1	0
0	(MSB)			PAGE CODE (0011h)				
1								(LSB)
2	(MSB)			PAGE LENGTH (8)				
3								(LSB)
4	Reserved				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, and the sense key specific FIELD POINTER field set to the CONTROL POLICY CODE field.

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.

No further changes are proposed to this section