memorandum

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

T10/07-361r3

To	From	Subject	Date
INCITS T10 Committee	Curtis Ballard, HP Michael Banther, HP	SSC-3 Out of Band Encryption Key Management	29 October, 2007

Revision History

Revision 0 – Initial document.

Revision 1 – Too many changes to list full details
- Changes from feedback before September 07, T10 meetings
- Significant editorial changes
- Changed several check condition values to DATA PROTECT
- Clarified new concept of data encryption capabilities
- Modified disabled and split into disabled and prevented as different concepts
- Added top level indication of algorithms prevented into data encryption status page
- Added indicator of encryption parameters configuration source to data encryption status page

Revision 2 – Removed fatal error state following encryption/decryption error
- Narrowed definition of encryption capabilities to limit it to the values in the Data Encryption Capabilities page
- Defined an SSC application client and replaced references to the SSC device server
- Removed mechanism that allowed external control of a single algorithm while leaving other algorithms open
- Changes parameters configured by field in status page to parameters controlled by

Revision 3 – Changes from October 24 conference call
- Included other sections from SSC-3 that need parameters moved from the device server to the physical device
- Split behavior for disabled and configuration prevented into two sections
- Removed SSC application client throughout and replaced with device server
- Removed sections that allowed for preventing control of a single algorithm

Related Documents

ssc3r03d – SCSI Stream Commands

spc4r11 – SCSI Primary Commands

Background

Discussion in working groups has brought up the issue of methods for encryption key management by devices outside the scope of this standard and a working item on the ADC-3 proposal is "Automation control of encryption performed by data transfer device." Any method for providing data encryption control parameters to a tape device that does not use the existing SECURITY PROTOCOL IN and SECURITY PROTOCOL OUT commands over a primary port will have side effects on the SSC device server including the possibility of key management contention between applications using a primary port and applications using an alternate out of band method for data encryption parameters management.

If data encryption parameters are controlled by an out of band device the data encryption capabilities of the drive may be altered and a method is needed to report that an encryption algorithm is supported but not available. This proposal provides a method for reporting when individual encryption protocols have been disabled. Key management contention may be prevented by disabling support of all encryption protocols over the primary port.

This proposal also provides a model for error condition reporting and recovery when encryption is controlled by an out of band mechanism.

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 SSC-3

3.1.13 data encryption parameters: A set of parameters accessible through the Set Data Encryption page (see 8.4.3.2) that controls the data encryption and decryption process in the physical device~~device server~~. See 4.2.21.8.

New definition 3.1.14. Existing definitions shift down.

3.1.14 data encryption capabilities: A set of capabilities in the physical device that determine the values reported through a SECURITY PROTOCOL IN command specifying the Tape Data Encryption security protocol and the Data Encryption Capabilities page (see 4.2.21.9).

New definition 3.1.25. Existing definitions shift down.

3.1.25 external data encryption control: A capability of the physical device that allows control of the data encryption parameters and the data encryption capabilities through an external interface (e.g. ADC device server or a management interface).

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

4.2.3 Physical Device

Add data encryption parameters and data encryption capabilities to list of items in physical device in figure 8.

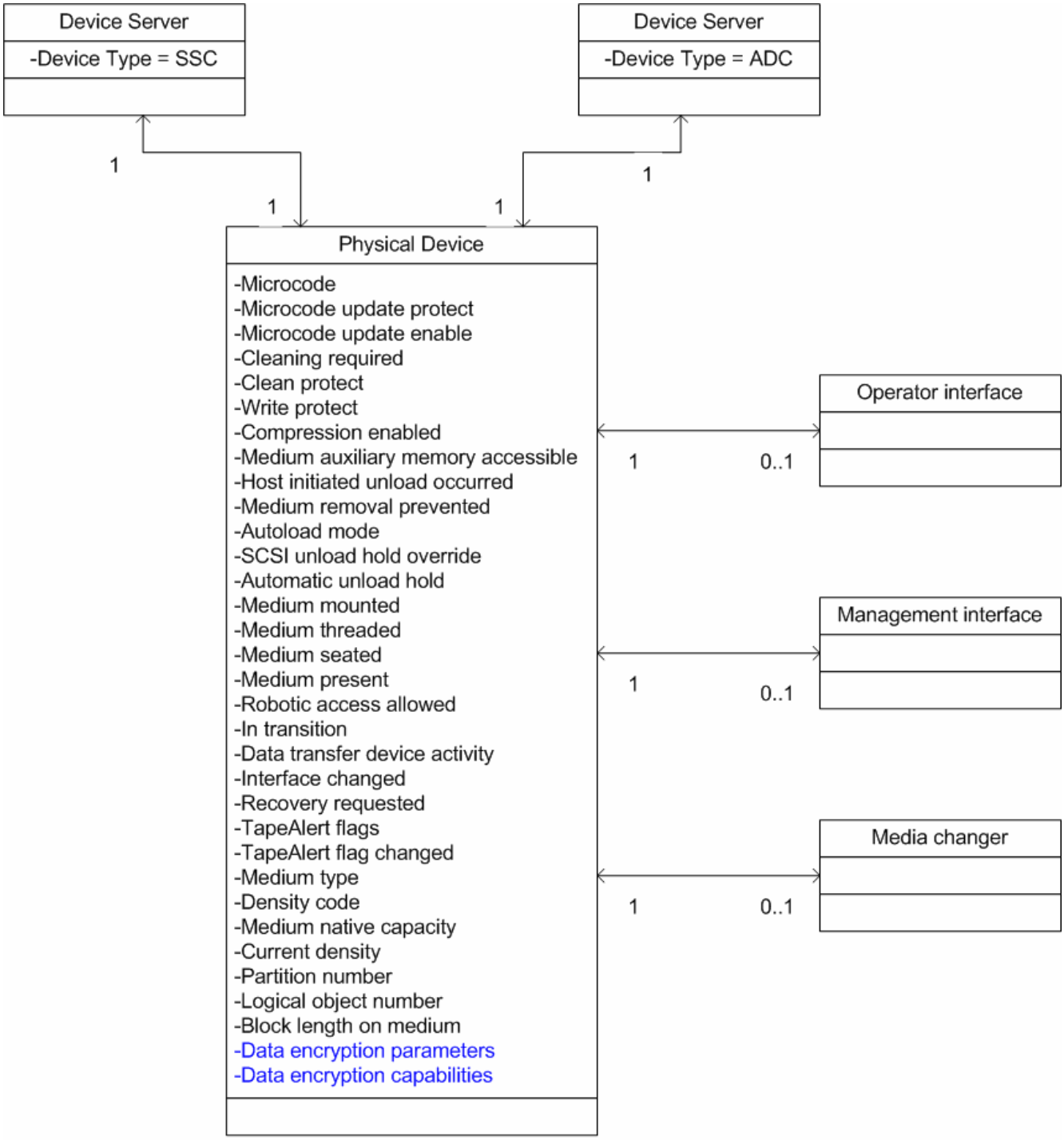

Figure 8 — UML example of SCSI target device and physical device

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

Add data encryption parameters to table 2.

Table 2 specifies the standard that defines each attribute shown in figure 8.

Table 2 – Physical device attributes

Attribute	Reference
Microcode	SPC-4
Microcode update protect	ADC-2
Microcode update enable	ADC-2
Cleaning required	ADC-2
Clean protect	ADC-2
Write protect	ADC-2
Compression enabled	ADC-2
Medium auxiliary memory accessible	ADC-2
Host initiated unload occurred	ADC-2
Medium removal prevented	ADC-2
Autoload mode	SPC-4
SCSI unload hold override	ADC-2
Automatic unload hold	ADC-2
Medium mounted	ADC-2
Medium threaded	ADC-2
Medium seated	ADC-2
Medium present	ADC-2
Robotic access allowed	ADC-2
In transition	ADC-2
Data transfer device activity	ADC-2
Interface changed	ADC-2
Recovery requested	ADC-2
TapeAlert flags	table 10
TapeAlert flag changed	ADC-2
Medium type	7.8.4
Density code	8.2.4.3
Medium native capacity[a]	7.8.3
Current density	ADC-2
Partition number	7.6.3
Logical object number	7.6.3
Block length on medium	SPC-4
Data encryption parameters	4.2.21.8
Data encryption capabilities	4.2.21.9

a) Medium native capacity is the value reported in the CAPACITY field of the density support data block descriptor when the MEDIA bit is one, and a SET CAPACITY command has not been used to affect the capacity of the medium.

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

4.2.21.6 Managing keys within the physical device~~device server~~

To increase the security of keys, the data encryption parameters are volatile in the physical device~~device server~~ and the data encryption keys are never reported to an application client. The physical device~~device server~~ may also have limited resources for storage of keys.

A device server that supports encryption shall support at least one of the key formats that are defined in this standard (see table 121).

A vendor-specific key reference is an identifier that is associated with a specific key. The method by which keys and their associated vendor-specific key references are made available to the device server is outside the scope of this standard. A device server that supports passing keys by vendor-specific key reference shall include the code for vendor-specific key reference format (see table 121) in the SUPPORTED KEY FORMATS LIST field in the Supported Key Formats page (see 8.5.2.5).

The physical device~~device server~~ shall release the resources used to save a set of data encryption parameters under the following conditions:

a) the CKOD bit is set to one in the saved data encryption parameters and the volume is de-mounted;
b) the CKORL bit is set to one and the key scope is set to LOCAL in the saved data encryption parameters and the I_T nexus that established the set of data encryption parameters loses its reservation;
c) the CKORL bit is set to one and the key scope is set to ALL I_T NEXUS in the saved data encryption parameters and the device server experiences a reservation loss (see 3.1.56);
d) the CKORP bit is set to one in the saved data encryption parameters and the device server processes a PERSISTENT RESERVE OUT command with a service action of either PREEMPT or PREEMPT AND ABORT;
e) a microcode update is performed on the device; or
f) a power on condition occurs.

The physical device~~device server~~ may release the resources used to save a set of data encryption parameters if:

a) a volume is mounted that does not support data encryption using the algorithm specified by the algorithm index in the data encryption parameter; or
b) other vendor-specific events.

If a device server processes a Set Data Encryption page with the ENCRYPTION MODE field set to DISABLE and DECRYPTION MODE field set to DISABLE or RAW, the physical device~~device server~~ shall:

a) release any resources that it had allocated to store data encryption parameters for the I_T nexus associated with the SECURITY PROTOCOL OUT command and shall change the contents of all memory containing a key value associated with the data encryption parameters that are released; and
b) establish a unit attention condition with the additional sense of DATA ENCRYPTION PARAMETERS CHANGED BY ANOTHER INITIATOR for all other I_T nexus that has its registered for encryption unit attentions state set to one (see 4.2.21.7) and is affected by the loss of the key, (i.e., any I_T nexus that is using a data encryption scope of PUBLIC and sharing the keys).

If a device server processes a Set Data Encryption page that includes a key and the SDK bit is set to zero, the device server shall establish a unit attention condition with the additional sense of DATA ENCRYPTION PARAMETERS CHANGED BY ANOTHER INITIATOR for all other I_T nexus that have their registered for encryption unit attentions state set to one (see 4.2.21.7) and are affected by the change of the key (i.e., any I_T nexus that is using a data encryption scope of PUBLIC and sharing the key), and the physical device~~device server~~ shall:

a) release all resources that it had allocated to store a key value set by a previous SECURITY PROTOCOL OUT command from that I_T nexus and shall change the contents of all memory containing a key value associated with the data encryption parameters that are released; and
~~b) establish a unit attention condition with the additional sense of DATA ENCRYPTION PARAMETERS CHANGED BY ANOTHER INITIATOR for all other I_T nexus that have their registered for encryption unit attentions state set to one~~

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

~~(see 4.2.21.7) and are affected by the change of the key (i.e., any I_T nexus that is using a data encryption scope of PUBLIC and sharing the key); and~~

b) ~~c)~~establish a set of data encryption parameters with the values from the Set Data Encryption page.

A physical device~~device server~~ shall save at most one set of data encryption parameters with a key scope of ALL I_T NEXUS. If a device server processes a Set Data Encryption page with the SCOPE field set to ALL I_T NEXUS, the device server shall establish a unit attention condition with the additional sense of DATA ENCRYPTION PARAMETERS CHANGED BY ANOTHER INITIATOR for all other I_T nexus that have their registered for encryption unit attentions state set to on (see 4.2.21.7) and are affected by the change of the key (i.e., any I_T nexus that is using a data encryption scope of PUBLIC and sharing the key) and the physical device~~device server~~ shall:

a) release any resources that it had allocated to store data encryption parameters with a key scope value of ALL I_T NEXUS and shall change the contents of all memory containing a key value associated with the data encryption parameters that are released; and

~~b) establish a unit attention condition with the additional sense of DATA ENCRYPTION PARAMETERS CHANGED BY ANOTHER INITIATOR for all other I_T nexus that have their registered for encryption unit attentions state set to one (see 4.2.21.7) and are affected by the change of the key (i.e. any I_T nexus that is using a data encryption scope of PUBLIC and sharing the key); and~~

b) ~~c)~~establish a set of data encryption parameters with the values from the Set Data Encryption page and a key scope value of ALL I_T NEXUS.

If a vendor-specific event occurs that changes or clears a set of data encryption parameters, the device server shall establish a unit attention condition with the additional sense of DATA ENCRYPTION PARAMETERS CHANGED BY VENDOR SPECIFIC EVENT for any I_T nexus that has its registered for encryption unit attentions state set to one (see 4.2.21.7) and is affected by the change of the key.

4.2.21.7 Saved information per I_T nexus

If the device server supports data encryption it shall save the following information on a per I_T nexus basis:

a) data encryption scope;
b) lock;
c) key instance counter value at lock;
d) key instance counter value assigned to the last key established by a Set Data Encryption page for this I_T nexus with a scope value of LOCAL and the SDK bit is set to zero; and
e) registered for encryption unit attentions state.

The set of possible data encryption scope values for an I_T nexus is:

a) PUBLIC;
b) LOCAL; or
c) ALL I_T NEXUS

If an I_T nexus data encryption scope is set to PUBLIC it indicates the physical device~~device server~~ does not have a saved set of data encryption parameters that were established by that I_T nexus. Device servers that support encryption shall support an I_T nexus data encryption scope of PUBLIC.

A device server shall set the data encryption scope for an I_T nexus to LOCAL when it successfully completes the processing of a Set Data Encryption page with a scope of LOCAL from that I_T nexus. The device server shall only use the data encryption parameters established by the Set Data Encryption page with a scope of LOCAL for processing commands from the I_T nexus that established the parameters. A physical device~~device server~~ shall revert to using default data encryption parameters for an I_T nexus that is configured with a data encryption scope of LOCAL if the resources used to save the data encryption parameters for the I_T nexus are released.

A device server shall set the data encryption scope for an I_T nexus to ALL I_T NEXUS when it successfully completes the processing of Set Data Encryption page with a scope value of ALL I_T NEXUS from that I_T nexus. At most, one I_T nexus shall be assigned the data encryption scope of ALL I_T NEXUS. If the physical device~~device server~~ releases resources used to store a set of data encryption parameters with a key scope of ALL I_T NEXUS, it shall change the data encryption scope for the I_T

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

nexus that established that set of data encryption parameters to PUBLIC. Device servers that support encryption shall support an I_T nexus data encryption scope of ALL I_T NEXUS.

By default, the physical device~~device server~~ shall set the saved I_T nexus parameters data encryption scope value to PUBLIC and lock value to zero.

The registered for encryption unit attentions state is a single bit state variable that indicates if the device server shall generate unit attention conditions related to encryption status for the I_T nexus. The device server shall set the registered for encryption unit attentions state to one for an I_T nexus if the device server processes a:

a) SECURITY PROTOCOL IN command specifying the Tape Data Encryption protocol from the I_T nexus; or
b) SECURITY PROTOCOL OUT command specifying the Tape Data Encryption protocol from the I_T nexus.

The device server shall set the registered for encryption unit attentions state to zero for an I_T nexus if an I_T nexus loss occurs. The device server shall set the registered for encryption unit attentions state to zero for all I_T nexus if the device server processes a logical unit reset.

4.2.21.8 Data encryption parameters

A device server that supports data encryption shall have the ability to save the following information in the physical device as a set of data encryption parameters when a Set Data Encryption page is processed:

a) for SCSI transport protocols where SCSI initiator device port names are required, the SCSI initiator device port name; otherwise, the SCSI initiator device port identifier;
b) indication of the SCSI target port through which the data encryption parameters were established;
c) key scope;
d) encryption mode;
e) decryption mode;
f) key;
g) supplemental decryption keys where supported;
h) algorithm index;
i) key instance counter;
j) CKOD;
k) CKORL;
l) CKORP;
m) U-KAD;
n) A-KAD;
o) M-KAD;
p) nonce;
q) raw decryption mode disable where supported; and
r) check external encryption mode where supported.

A physical device~~device server~~ may have limited resources for storage of sets of data encryption parameters (i.e., it may not have enough resources to store a unique set of data encryption parameters for every I_T nexus that it is capable of managing). A physical device~~device server~~ may release a previously established set of data encryption parameters when a Set Data Encryption page is processed and there are no unused resources available. The method of choosing which set of data encryption parameters to release is vendor specific. If the physical device~~device server~~ does release a previously established set of data encryption parameters to free the resource, ~~it shall~~ the device server shall establish a unit attention condition for every affected I_T nexus (see 4.2.21.6) that has its registered for encryption unit attentions state set to one (see 4.2.21.7). A physical device~~device server~~ is not required to have separate resources to store data encryption parameters for every scope that is supported.

A device server shall support an encryption key scope value of ALL I_T NEXUS and the physical device shall have resources to save one set of data encryption parameters with this scope.

If the device server supports an encryption key scope value of LOCAL, ~~it~~ the device server shall have resources to save one or more sets of data encryption parameters with this scope.

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

The data encryption parameters that shall be used for an I_T nexus shall be established by the following order of precedence:

a) if the data encryption scope for the I_T nexus is set to LOCAL or ALL I_T NEXUS (see 4.2.21.7), the data encryption parameters set by the last Set Data Encryption page from that I_T nexus; or
b) if the data encryption scope for the I_T nexus is set to PUBLIC:
    1) the data encryption parameters that have been saved by the physical device~~device server~~ with a key scope of ALL I_T NEXUS if any data encryption parameters have been saved with this key scope; or
    2) the default data encryption parameters.

New model clause section 4.2.21.9. Existing clauses shift down.

4.2.21.9 Data encryption capabilities

A physical device that supports data encryption shall have a set of data encryption capabilities (see 3.1.14).

The data encryption capabilities include:

a) algorithm index values;
b) encryption capable;
c) decryption capable; and
d) other vendor specific data encryption capabilities.

Comment: this list could list all of the values reported in a Data Encryption Algorithm descriptor or could just reference the Data Encryption Algorithm descriptor but the values listed here are all that need to be configurable for this proposal so the list was restricted to the minimum set to simplify.

4.2.21.10 ~~4.2.21.9~~Key instance counter

The device server shall keep a counter for each key that it is managing called the key instance counter. All key instance counters shall be set to zero when a power on condition occurs. Any other event that sets, clears, or changes a parameter in a set of data encryption parameters, except the supplemental decryption keys, shall cause the key instance counter for that set of data encryption parameters to be incremented. The value of the key instance counter associated with the currently selected key for an I_T nexus is reported in the Data Encryption Status page of the SECURITY PROTOCOL IN command. The key instance counters are 32 bits and shall roll over to zero when incremented past their maximum value.

4.2.21.11 ~~4.2.21.10~~Encryption mode locking

There are conditions outside of the control of an application client which cause the physical device~~device server~~ to release the resources used to save the data encryption parameters (see 4.2.21.6) or change the data encryption parameters used to control the encryption of logical blocks. Each of these conditions cause the device server to establish a unit attention condition to report the change of operating mode, but the unit attention condition may not always be reported to the application client through protocol bridges and driver stacks.

The LOCK bit in the Set Data Encryption page is set to one to lock the I_T nexus that issued the SECURITY PROTOCOL OUT command to the set of data encryption parameters established at the completion of the processing of the command. The I_T nexus remains locked to that set of data encryption parameters and key instance counter value until a hard reset condition occurs or another SECURITY PROTOCOL OUT command including a Set Data Encryption page from the same I_T nexus is processed.

If the device server processes a WRITE(6) or WRITE(16) command for an I_T nexus that is locked to a set of data encryption parameters and key instance counter, and the key instance counter value has changed since the time it was locked, the device server shall terminate the command with CHECK CONDITION status, with the sense key set to DATA PROTECT, and the additional sense code set to DATA ENCRYPTION KEY INSTANCE COUNTER HAS CHANGED. All subsequent WRITE(6) and WRITE(16) commands shall also be terminated in this manner until a hard reset condition occurs or a SECURITY PROTOCOL OUT command including a Set Data Encryption page from the same I_T nexus is processed.

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

4.2.21.12 ~~4.2.21.11~~Nonce generation

For a given encryption algorithm, the physical device ~~device server~~ may:

a) not require a nonce value;
b) generate its own nonce value;
c) require a nonce value or part of the nonce value be provided by the application client; or
d) be configurable with respect to the source of the nonce value.

The physical device ~~device server~~ reports its capability with respect to nonce values in the Data Encryption Algorithm descriptor(s) (see 8.5.2.4). If the physical device ~~device server~~ reports that it requires a nonce value from the application client and a Set Data Encryption page is processed that does not include a nonce value descriptor, the device server shall terminate the command with CHECK CONDITION, with the sense key set to ILLEGAL REQUEST, and the additional sense code set to INCOMPLETE KEY-ASSOCIATED DATA SET.

Note: No further sections of 4.2.21 require changes to device server statements so they are not repeated here

New model clause section 4.2.22. Existing clause 4.2.22 shifts down to become 4.2.23:

4.2.22 External data encryption control

4.2.22.1 External data encryption control overview

A physical device that supports data encryption may support external data encryption control and provide the ability for an external entity to configure data encryption capabilities or data encryption parameters using an external interface not specified by this standard (e.g., ADC device server or a management interface).

4.2.22.2 External data encryption control of data encryption capabilities

4.2.22.2.1 External data encryption control of data encryption capabilities introduction

External data encryption control may be used to change the data encryption capabilities of the physical device that are reported in response to a SECURITY PROTOCOL IN command (see SPC-4) specifying the Tape Data Encryption security protocol and the Data Encryption Capabilities page.

If external data encryption control is used to change any of the data encryption capabilities of the physical device, then the device server shall establish a unit attention condition with the additional sense code of DATA ENCRYPTION CAPABILITIES CHANGED for all I_T nexus that have their registered for encryption unit attentions state set to one (see 4.2.20.7).

Comment: DATA ENCRYPTION CAPABILITIES CHANGED is a new ASC/ASCQ.

4.2.22.2.2 External data encryption control of encryption algorithm support

External data encryption control may be used to change the device server encryption algorithm support by configuring the physical device to:

a) disable a supported encryption algorithm; or
b) prevent device server control of data encryption parameters.

If a supported encryption algorithm has been disabled, then the physical device shall not accept data encryption parameters specifying that algorithm and the device server shall:

a) remove the encryption algorithm from the list of supported encryption algorithms returned in the Data Encryption Capabilities page; or
a) report the encryption algorithm in the list of supported encryption algorithms returned in the Data Encryption Capabilities page with the DISABLED bit set to one.

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

If external data encryption control has been used to configure the physical device to prevent device server control of data encryption parameters, then the device server shall:

a) terminate a SECURITY PROTOCOL OUT command specifying the Tape Data Encryption security protocol that passes a Set Data Encryption page with CHECK CONDITION status, with the sense key set to ILLEGAL REQUEST, and the additional sense code set to DATA ENCRYPTION CONFIGURATION PREVENTED;
b) set the CFG_P (see 8.2.5.4) field in the Data Encryption Capabilities page to 2 (i.e., The physical device is configured to not allow this device server to establish or change data encryption parameters); and
    A) remove the encryption algorithm from the list of supported encryption algorithms returned in the Data Encryption Capabilities page; or
    B) report the encryption algorithm in the list of supported encryption algorithms returned in the Data Encryption Capabilities page with the DECRYPT_C field set to 3 (i.e., The physical device has the capability to decrypt data using this algorithm but control of the data encryption parameters by this device server is prevented) and the ENCRYPT_C field set to 3 (i.e., The physical device has the capability to encrypt data using this algorithm but control of the data encryption parameters by this device server is prevented).

Comment: DATA ENCRYPTION CONFIGURATION PREVENTED is a new ASC/ASCQ.

Note: If external data encryption control has been used to configure the physical device to prevented device server control of the data encryption parameters, the data encryption parameters may be controlled by a device outside the scope of this standard. The encryption status may be read using the SECURITY PROTOCOL IN command specifying the Tape Data Encryption security protocol and the Data Encryption Status page.

4.2.22.3 External data encryption control of data encryption parameters

If external data encryption control is used to configure the physical device to prevent control of the data encryption parameters by this device server, then the external data encryption control data encryption parameters lookup process shall be allowed to complete before the device server:

a) changes the logical position as part of the processing of a READ(6), READ(16), READ REVERSE(6), READ REVERSE(16), VERIFY(6), or VERIFY(16), command; or
b) transfer any data or filemarks into the buffer as part of the processing of a WRITE(6), WRITE(16), or WRITE FILEMARKS, ~~ERASE~~ command .

If external data encryption control is used to configure the physical device to prevent control of the data encryption parameters by this device server, then the device server shall respond to a SECURITY PROTOCOL IN command specifying the Tape Data Encryption security protocol and the Data Encryption Status page with the PARAMETERS CONTROL field set to 3 or 4.

Note: The external data encryption control data encryption parameters lookup process is beyond the scope of this standard.

4.2.22.4 External data encryption control error conditions

If external data encryption control is being used to control the data encryption parameters and the external data encryption control data encryption parameters lookup process returns an error, then the device server shall terminate the command that initiated the data encryption parameters lookup process with CHECK CONDITION status, with the sense key set to DATA PROTECT, and the additional sense code set to EXTERNAL DATA ENCRYPTION CONTROL ERROR.

Comment: EXTERNAL DATA ENCRYPTION CONTROL ERROR is a new additional sense code. It may be useful to define multiple ASC/ASCQ combinations that can be returned so different error conditions such as failure to access the key manager, key manager reported an error, or media does not support encryption may be returned.

If external data encryption control is being used to control the data encryption parameters and the external data encryption control data encryption parameters lookup process does not complete before a timeout period, then the device server shall terminate the command that initiated the data encryption parameters lookup process with CHECK CONDITION status, with the sense key set to DATA PROTECT, and the additional sense code set to EXTERNAL DATA ENCRYPTION CONTROL TIMEOUT.

Comment: EXTERNAL DATA ENCRYPTION CONTROL TIMEOUT is a new additional sense code.

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

Comment: No text specific to abort is provided as it appears that abort handling to be normal from the SSC application client perspective.

An application client may use the DTD Status log page to get information about the error that occurred (see ADC-3).

Changes to clause 8.5.2.4:

8.2.5.4 Data Encryption Capabilities page

Table 98 specifies the format of the Data Encryption Capabilities page.

Table 98 – Data Encryption Capabilities 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						CFG_P	
5	Reserved							
19								
Data Encryption Algorithm descriptor list								
20	Data Encryption Algorithm descriptor (first)							
	Data Encryption Algorithm descriptor (last)							
n								

See SPC-4 for a description of the PAGE LENGTH field.

See SPC-4 for a description of the PAGE CODE field, the PAGE CODE field shall be set to the value indicated in table 98.

The configuration prevented (CFG_P) field (see table y) indicates the data encryption parameters configuration capabilities for this device server.

Table y – CFG_P field values

CODE	Description
0	The data encryption parameters configuration capabilities are not reported.
1	The physical device is configured to allow this device server to establish or change data encryption parameters.
2	The physical device is configured to not allow this device server to establish or change data encryption parameters.
3	Reserved

Each Data Encryption Algorithm descriptor (see table 99) contains information about a data encryption algorithm supported by the device server. If more than one descriptor is included, they shall be sorted in ascending order of the value in the ALGORITHM INDEX field.

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

Table 99 -- Data Encryption Algorithm descriptor

Bit / Byte	7	6	5	4	3	2	1	0
0	ALGORITHM INDEX							
1	Reserved							
2	(MSB)							
3	DESCRIPTOR LENGTH (20)							(LSB)
4	AVFMV	SDK_C	MAC_C	DED_C	DECRYPT_C		ENCRYPT_C	
5	AVFCLP		NONCE_C		Reserved		UKADF	AKADF
6	(MSB)							
7	MAXIMUM UNAUTHENTICATED KEY-ASSOCIATED DATA BYTES							(LSB)
8	(MSB)							
9	MAXIMUM AUTHENTICATED KEY-ASSOCIATED DATA BYTES							(LSB)
10	(MSB)							
11	KEY SIZE							(LSB)
12	Reserved				RDMC_C			EAREM
13	(MSB)							
19	Reserved							(LSB)
20	(MSB)							
23	SECURITY ALGORITHM CODE							(LSB)

Comment: fields that are not changed are not repeated here.

The DECRYPT_C field (see table 100) specifies the decryption capabilities of the device server.

Table 100 – DECRYPT_C field values

CODE	Description
0	The ~~device server~~ physical device has no data decryption capability using this algorithm. This value shall be returned if the specified algorithm is disabled.
1	The ~~device server~~ physical device has the capability to decrypt data using this algorithm in software.
2	The ~~device server~~ physical device has the capability to decrypt data using this algorithm in hardware.
3	The physical device has the capability to decrypt data using this algorithm but control of the data encryption parameters by this device server is prevented.

The ENCRYPT_C field (see table 101) specifies the data encryption capabilities of the device server.

Table 101 – ENCRYPT_C field value

CODE	Description
0	The ~~device server~~ physical device has no data encryption capability using this algorithm. This value shall be returned if the specified algorithm is disabled.
1	The ~~device server~~ physical device has the capability to encrypt data using this algorithm in software.
2	The ~~device server~~ physical device has the capability to encrypt data using this algorithm in hardware.
3	The physical device has the capability to encrypt data using this algorithm but control of the data encryption parameters by this device server is prevented.

Changes to clause 8.5.2.7:

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

8.5.2.7 Data Encryption Status page

Table 107 specifies the format of the Data Encryption Status page.

Table 107 — Data Encryption Status page

Bit / Byte	7	6	5	4	3	2	1	0
0	(MSB)			PAGE CODE (0020h)				
1								(LSB)
2	(MSB)			PAGE LENGTH (n-3)				
3								(LSB)
4	I_T NEXUS SCOPE			Reserved		KEY SCOPE		
5	ENCRYPTION MODE							
6	DECRYPTION MODE							
7	ALGORITHM INDEX							
8	(MSB)			KEY INSTANCE COUNTER				
11								(LSB)
12	Reserved		PARAMETERS CONTROL			CEEMS		RDMD
13	Reserved							
23								
24	KEY-ASSOCIATED DATA DESCRIPTORS LIST							
n								

Comment: Fields that are not changed are not repeated here.

The PARAMETERS CONTROL field contains information on how the data encryption parameters are controlled. Table y+2 shows the values of the PARAMETERS CONTROL field.

Table y+2 – PARAMETERS CONTROL field values

CODE	Description
0	Data encryption parameters control is not reported.
1	Data encryption parameters are not controlled by external data encryption control.
2	Data encryption parameters are controlled by the SSC device server.
3	Data encryption parameters are controlled by the ADC device server.
4	Data encryption parameters are controlled by a management interface.
5-7	Reserved

Comment: Fields could be added to describe the current state if in an error state and those could report the same values as a command on the primary interface. That would consume quite a bit of space so I haven't added those fields since the CHECK CONDITION on the primary interface would have already reported the condition and defining multiple additional sense codes could remove the need for detailed additional information.

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

Changes to clause 8.5.3.1:

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

Comment: Only table 114 is changed so the rest of the text is not repeated here

The SECURITY PROTOCOL SPECIFIC field (see table 114) specified the type of page that the application client is sending.

Table 114 – SECURITY PROTOCOL SPECIFIC field values

CODE	Description	Reference
0000h—000Fh	Reserved	
0010h	Set Data Encryption page	8.5.3.2
0011h	SA Encapsulation page	8.5.3.3~~2~~
0012h—~~FEFFh~~002Fh	Reserved	
0030h—003Fh	Restricted	ADC-3
0040h—FEFFh	Reserved	
FF00h—FFFFh	Vendor Specific	

Changes to clause 8.4.3.2.1:

8.5.3.2 Set Data Encryption page

8.5.3.2.1 Set Data Encryption page overview

: sections not changed skipped

If the physical device~~device server~~ does not currently have a saved set of data encryption parameters associated with the I_T nexus that sent the Set Data Encryption page or the scope or decryption mode values do not match the values in that set of saved data encryption parameters, the device server shall terminate the command with CHECK CONDITION status and set the sense key to ILLEGAL REQUEST and the additional sense code to INVALID FIELD IN PARAMETER LIST.

: sections not changed skipped

If the clear key on de-mount (CKOD) bit is set to one the physical device~~device server~~ shall set the data encryption parameters to default values upon completion of a volume de-mount. If the CKOD bit is set to zero, the de-mounting of a volume shall not affect the data encryption parameters. If the CKOD bit is set to one and there is no volume mounted in the device, the device server shall terminate the command with CHECK CONDITION status and set the sense key to ILLEGAL REQUEST and the additional sense code to INVALID FIELD IN PARAMETER DATA.

If the clear key on reservation preempt (CKORP) bit is set to one the physical device~~device server~~ shall set the data encryption parameters to default values when a persistent reservation is preempted (i.e., a PERSISTENT RESERVE OUT command specifying a service action of PREEMPT or PREEMPT AND ABORT is processed). If the CKORP bit is set to zero, a preemption of a persistent reservation shall not affect the data encryption parameters. If the CKORP bit is set to one and there is no persistent reservation in effect for the I_T nexus associated with the SECURITY PROTOCOL OUT command, the device server shall terminate the command with CHECK CONDITION status and set the sense key to ILLEGAL REQUEST and the additional sense code to INVALID FIELD IN PARAMETER DATA.

If the clear key on reservation loss (CKORL) bit is set to one the physical device~~device server~~ shall set the data encryption parameters to default values on a reservation loss (see 3.1.56). If the CKORL bit is set to zero, a reservation loss shall not affect the data encryption parameters. If the CKORL bit is set to one and there is no reservation in effect for the I_T nexus associated with the SECURITY PROTOCOL OUT command, the device server shall terminate the command with CHECK CONDITION status and set the sense key to ILLEGAL REQUEST and the additional sense code to INVALID FIELD IN PARAMETER DATA.

: sections not changed skipped

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

If the device server is not capable of distinguishing encrypted blocks from unencrypted blocks using the algorithm specified in the ALGORITHM INDEX field and the DECRYTPTION MODE field is set to MIXED, the 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 DATA.

If the ENCRYPTION MODE field is set to EXTERNAL or ENCRYPT, or the DECRYPTION MODE field is set to RAW, DECRYPT, or MIXED, and the algorithm specified in the ALGORITHM INDEX field is disabled, the device server shall terminate the command with CHECK CONDITION status, with the sense key set to ILLEGAL REQUEST, and the sense code set to ENCRYPTION ALGORITHM DISABLED.

Comment: ENCRYPTION ALGORITHM DISABLED is a new additional sense code.