memorandum

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

T10/08-350r1

To	From	Subject	Date
INCITS T10 Committee	Curtis Ballard, HP	SSC-3 Resolve LB comments QTM-rbw-103 and SYM-022	15 October, 2008

Revision History

Revision 0 – Initial document.

Revision 1 – Changes from face to face meeting September 9, 2008
Moved notes to normative text in introduction

Related Documents

ssc3r04a – SCSI Stream Commands

Background

This proposal will introduce changes to address the following letter ballot comments.

QTM-rbw-103	T	81	Note 13	NOTE 13 The SECURITY PROTOCOL IN command specifying the Tape Data Encryption security protocol and the Data Encryption Status page may be used to determine whether external data encryption control has been used to provide a set of data encryption parameters.	Limited to just provide, or includes establish, change, or control? (as in previous wording)
SYM-022	edit	61	4.2.22 External data encryption control	This section should identify how an application client determines that a physical device has the capability for external data encryption control BEFORE it happens.	

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

Proposed Changes to SSC-3

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., an 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

If the physical device has a saved set of data encryption parameters associated with this device server or has a medium mounted, then the physical device shall not allow external data encryption control of data encryption capabilities. If the physical device does not have a set of data encryption parameters associated with this device

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

server and does not have a medium mounted, then external data encryption control may be used to change the data encryption capabilities.

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 4.2.21.7).

Note to editor: The working group discussed that it may be best if the following two new paragraphs are moved into a new subclause for detecting external data encryption control.

The SECURITY PROTOCOL IN command specifying the Tape Data Encryption security protocol and the Data Encryption Capabilities page may be used to determine whether the device server supports external data encryption control.

The SECURITY PROTOCOL IN command specifying the Tape Data Encryption security protocol and the Data Encryption Status page may be used to determine which device server has control of the data encryption parameters and whether external data encryption control has been used to establish or change a set of data encryption parameters.

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

If a supported encryption algorithm has been disabled then:

a) the physical device shall not accept data encryption parameters specifying that algorithm; and
b) the device server shall:
    A) not report the disabled data encryption algorithm in the Data Encryption Capabilities page; or
    B) report the encryption algorithm in the Data Encryption Capabilities page with the DISABLED bit set to one.

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 that attempts to establish or clear a set of data encryption parameters with CHECK CONDITION status, with the sense key set to ILLEGAL REQUEST, and the additional sense code set to DATA ENCRYPTION CONFIGURATION PREVENTED; and
b) set the CFG_P (see 8.2.5.4) field in the Data Encryption Capabilities page to 10b (i.e., The physical device is configured to not allow this device server to establish or change data encryption parameters) and:
    A) not report any encryption algorithms in the Data Encryption Capabilities page; or
    B) report all of the supported data encryption algorithms in the Data Encryption Capabilities page with the DECRYPT_C field set to capable with external control and the ENCRYPT_C field set to capable with external control.

~~Note 13 The SECURITY PROTOCOL IN command specifying the Tape Data Encryption security protocol and the Data Encryption Status page may be used to determine whether external data encryption control has been used to provide a set of data encryption parameters.~~