To: INCITS T10 Committee

From: Paul Entzel, Quantum

Date: 22 August 2006

Document: T10/06-385r0

Subject: SSC-3 Modifications to Tape Data Encryption protocol

1 Revision History

Revision 0:
Posted to the T10 web site on 22 August 2006.

2 Reference

T10/SSC-3 revision 3
T10/06-051r7, *The Requirement for More than One Decryption Key*

3 General

While implementing the Tape Data Encryption security protocol, several issues and question have arose that should be addressed in the standard. This proposal suggests changes and clarifications to this protocol.

Proposed additions or changes to the SSC-3 standard are shown in blue text; proposed deletions are shown in ~~red crossed out text~~, changed test are shown in red.

3.1 Dealing with volumes that can not support encryption

The current draft of SSC does not include distinguish between a device server that is capable of encryption and a tape format that is. Since it is possible, even likely, that new devices that support data encryption will need to be able to read and write volumes that do not support encryption (i.e. volumes that use formats that do not define encryption), the standard should explain:

1. How to report if the currently mounted volume can support encryption or any specific algorithms.
2. How do deal with a Set Data Encryption page that attempts to enable encryption or decryption when a volume is mounted that does not support it.
3. How mounting a volume that does not support encryption or does not support the selected algorithm should affect key management in the device server.

3.2 Add a Tape Data Encryption protocol page to return a random number

Many tape drives have available within them a pretty good entropy source making the generation of a good random number a fairly straight forward process. Since a random number source this good is not always available to the application clients through other means, it would be helpful to at least offer access to the random number generator through SCSI.

3.3 Add vendor specific pages to the Tape Data Encryption protocol

The entire range of pages in the Tape Data Encryption protocol is either defined or reserved. We should add a range of vendor specific pages to facilitate vendor specific features.

3.4 Defining a set of Tape Data Encryption pages as mandatory

Currently no mention is made about which of the Tape Data Encryption protocol pages are mandatory and which are optional. It would make the job of using the Tape Data Encryption protocol easier if we were to define a reasonable set of the pages as mandatory for devices that support encryption. Since

support for encryption is not (and can not be) mandatory, we can't make any pages mandatory without some clarification as to when the pages are mandatory. This proposal ties the requirement to support certain pages to the fact that the device server supports the Set Data Encryption page.

4 Changes to SSC-3

4.1 Dealing with volumes that don't support an encryption algorithm

In 4.2.19.5, add to the lettered list of conditions that cause a set of data encryption parameters to be released, renumbering the items below e):

e) a volume is mounted that does not support data encryption using the algorithm specified by the algorithm index in the data encryption parameter;

In 8.5.2.4 (Data Encryption Capabilities page), add a bit field the Data Encryption Algorithm descriptor table (table 97) in byte 4, bit 7. Name the bit "AVFMV". Add a paragraph describing the bit below the table:

The algorithm valid for mounted volume (AVFMV) bit shall be set to one of there is a volume currently mounted in the device and the encryption algorithm being described is valid for that volume. The AVFMV bit shall be set to zero if there is no volume mounted in the device or the algorithm is not valid for the currently mounted volume.

In 8.5.3.2 (Set Data Encryption page), add the following paragraph after the paragraph that describes the ALGORITHM INDEX field:

If a volume is mounted in the device and the combination of the ENCRYPTION MODE, DECRYPTION MODE, and ALGORITHM INDEX fields is not valid for the mounted volume, the device server shall terminate the command with CHECK CONDITION status, with the sense key set to ILLEGAL REQUEST, and the addition sense code set to INVALID FIELD IN PARAMETER DATA.

4.2 Add a Tape Data Encryption protocol page to return a random number

Add a new page to return a random number. Support for this page is optional.

In 8.5.2.1 (SECURITY PROTOCOL IN command specifying Tape Data Encryption security protocol overview), add to the security protocol specific field values table (table 93) the following entry:

Code	Description	Reference
0021h	Next Block Encryption Status page	8.5.2.8
0022h – 002Fh	Reserved	
0030h	Random Number page	8.5.2.9
0031h - FFFFh	Reserved	

Add the following subclause:

8.5.2.9 Random Number page

Table X specifies the format of the Random Number page.

Table X – Random Number page

Bit / Byte	7	6	5	4	3	2	1	0
0	(MSB)			PAGE CODE (0030h)				
1								(LSB)
2	(MSB)			PAGE LENGTH (32)				
3								(LSB)
4				RANDOM NUMBER				
35								

The RANDOM NUMBER contains a random number calculated by the device server using a source of entropy available within the device. Each request for the Random Number page shall return a different value in the RANDOM NUMBER field.

Editor's note: Should we add a note to the standard to instruct the application client how to generate a longer or shorter random number by either truncating or concatenating?

4.3 Add vendor specific pages to the Tape Data Encryption protocol

In 8.5.2.1 (SECURITY PROTOCOL IN command specifying Tape Data Encryption security protocol overview), add to the security protocol specific field values table (table 93) the following entry:

Code	Description	Reference
0031h - 7FFFh	Reserved	
8000h – FFFFh	Vendor Specific	

In 8.5.3.1 (SECURITY PROTOCOL OUT command specifying Tape Data Encryption security protocol overview), add to the security protocol specific field values table (table 107) the following entry:

Code	Description	Reference
0011h - 7FFFh	Reserved	
8000h – FFFFh	Vendor Specific	

4.4 Defining a set of Tape Data Encryption pages as mandatory

In 8.5.2.1 (SECURITY PROTOCOL IN command specifying Tape Data Encryption security protocol overview), add the following paragraph:

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. A device server that supports the Tape Data Encryption protocol in the SECURITY PROTOCOL IN command shall support the following pages:

a) Tape Data Encryption In Support page; and
b) Tape Data Encryption Out Support page.

In 8.5.3.2 (Set Data Encryption page), add the following paragraph:

A device server that supports the Set Data Encryption page shall also support the following Tape Data Encryption protocol pages:

a) Data Encryption Capabilities page;
b) Supported Key Formats page;
c) Data Encryption Management Capabilities page;
d) Data Encryption Status page; and
e) Next Block Encryption Status page.