To:	INCITS T10 Committee
From:	Paul Entzel, Quantum
Date:	13 September 2006
Document:	T10/06-385r1
Subject:	SSC-3 Modifications to Tape Data Encryption protocol

1 Revision History

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

Revision 1:
Updated with comments from the September 2006 SSC-3 working group meeting:
1. Update to reference SSC-3a.
2. Remove the Random Number page and submit this part of the proposal as a separate request.
3. Include the "current logical position" as something that could make an algorithm invalid.
4. Reduce the number of vendor specific page codes to 256.
5. Describe the mandatory pages by adding a column to the tables instead of in the text.

2 Reference

T10/SSC-3 revision 3a

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 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.

3.3   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 98) 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 if 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 or current logical position, 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 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 94) the following entry:

Code	Description	Reference
0031h - FEFFh	Reserved	
FF00h – 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 108) the following entry:

Code	Description	Reference
0011h - FEFFh	Reserved	
FF00h – FFFFh	Vendor Specific	

4.3 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.

Modify table 94 as shown:

Code	Description	Support	Reference
0000h	Tape Data Encryption In Support page	M	8.5.2.2
0001h	Tape Data Encryption In Support page	M	8.5.2.3
0002h–000Fh	Reserved		
0010h	Data Encryption Capabilities page	E	8.5.2.4
0011h	Supported Key Formats page	E	8.5.2.5
0012h	Data Encryption Management Capabilities page	E	8.5.2.6
0013h-001Fh	Reserved		
0020h	Data Encryption Status page	E	8.5.2.7
0021h	Next Block Encryption Statue page	E	8.5.2.8
0022h-FFFFh			
Support Key:	M – Mandatory for device servers that support the Tape Data Encryption protocol. E – Mandatory for device servers that support the Set Data Encryption page (see 8.5.3.2).		