To: INCITS T10 Committee

From: Paul Entzel, Quantum

Date: 10 May 2006

Document: T10/06-108r3

Subject: SPC-4: Add security protocol and additional sense for tape encryption

1 Revision History

Revision 0:
Posted to the T10 web site on 20 February 2006.

Revision 1:
Posted to the T10 web site on 29 March 2006. Changes recommended by the CAP working group at the March 2006 meeting and by the SSC-3 Working Group:

1. Added a General section.
2. Only request one protocol each for the SECURITY PROTOCOL IN and SECURITY PROTOCOL OUT commands.
3. Changed the name of additional sense code value 74h/04h.
4. Added sections 3.1 and 3.5.

Revision 2:
Posted to the T10 web site on 30 March 2006. Changes recommended by the SSC-3 working group at the 30 March 2006 conference call:

1. Fix several spelling and grammatical errors.
2. Update to state that 06-172 has been approved for inclusion in SSC-3.
3. Add another additional sense code MAXIMUM NUMBER OF SUPPLEMENTAL DECRYPTION KEYS EXCEEDED.

Revision 3:
Posted to the T10 web site on 10 May 2006. Changes from the discussion in the 10 May 2006 CAP WG meeting:

1. Change reference from IEEE 1619.1 to NIST SP 800-38C and NIST SP 800-38D.
2. Change additional sense code 74/00 to SECURITY ERROR and moved ERROR DECRYPTING DATA to 74/05. Changed INITIATOR to I_T NEXUS in additional sense code 2A/11.
3. Changed the Security Protocol Identifiers subclause to a model subclause. Renamed the table Security Algorithms. Changed the references to NIST documents. Changed the values to the 2 codes that are defined and added a footnote as to how the number was derived.

2 General

Proposal 06-172 that has been approved for inclusion in SSC-3 by the SSC-3 working group added the capability for the application client to control encryption of data at rest in tape drives. The proposal defines a series of pages both in and out under a new security protocol of the SECURITY PROTOCOL IN and SECURITY PROTOCOL OUT commands. This proposal requests the assignment of a security protocol code value to support this.

Additionally, several new additional sense code values are requested to report exceptions associated with data encryption.

Finally, a new subclause in SPC-4 is proposed to contain a table that defines code values associated with data encryption algorithms used by T10 standards.

In this proposal, blue text indicates additions to the standard and red text indicates changed text.

3 Changes to SPC-4

All references are to SPC-4 revision 3.

3.1 Changes to References under development subclause (2.3)

Add:

NIST Special Publication 800-38C, Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality.

NIST Special Publication 800-38D, Recommendation for Block Cipher Modes of Operation: Galois/Counter (GCM) Mode for Confidentiality and Authentication. (this one is under development)

Note to the editor: web index: http://csrc.nist.gov/publications/nistpubs/index.html

3.2 Changes to SECURITY PROTOCOL IN command subclause (6.28)

Modify table 173 as shown:

Code	Description	Reference
00h	Security protocol information	6.28.2
01h-06h	Defined by TCG	3.1.121
07h-1Fh	Reserved	
20h	Tape Data Encryption security protocol	SSC-3
21h-EFh	Reserved	
F0h-FFh	Vendor Specific	

3.3 Changes to SECURITY PROTOCOL OUT command subclause (6.29)

Modify table 178 as shown:

Code	Description	Reference
00h	Reserved	
01h-06h	Defined by TCG	3.1.121
07h-1Fh	Reserved	
20h	Tape Data Encryption security protocol	SSC-3
21h-EFh	Reserved	
F0h-FFh	Vendor Specific	

3.4 Changes to Sense key and sense code definitions

Add the following additional sense code definitions to table 28 and table D.2. The codes chosen are only suggestions, the editor may chose codes that are deemed more appropriate. The ASC code of 74h is new.

ASC	ASCQ	D T L P W R O M A E B K V F	Description
26h	10h	T	DATA DECRYPTION KEY FAIL LIMIT REACHED
26h	11h	T	INCOMPLETE KEY-ASSOCIATED DATA SET
26h	12h	T	VENDOR SPECIFIC KEY REFERENCE NOT FOUND
2Ah	11h	T	DATA ENCRYPTION PARAMETERS CHANGED BY ANOTHER I_T NEXUS
2Ah	12h	T	DATA ENCRYPTION PARAMETERS CHANGED BY VENDOR SPECIFIC EVENT
2Ah	13h	T	DATA ENCRYPTION KEY INSTANCE COUNTER HAS CHANGED
55h	08h	T	MAXIMUM NUMBER OF SUPPLEMENTAL DECRYPTION KEYS EXCEEDED
74h	00h	T	SECURITY ERROR
74h	01h	T	UNABLE TO DECRYPT DATA
74h	02h	T	UNENCRYPTED DATA ENCOUNTERED WHILE DECRYPTING
74h	03h	T	INCORRECT DATA ENCRYPTION KEY
74h	04h	T	CRYPTOGRAPHIC INTEGRITY VALIDATION FAILED
74h	05h	T	ERROR DECRYPTING DATA

3.5 New subclause for data encryption algorithms

5.13 Security Protocol identifiers

Table X describes security algorithm identifiers for use in security protocol parameter data.

Table X Security Algorithms

Code	Description	Reference
00010010h[a]	AES-CCM with a 16 byte MAC	NIST SP 800-38C
00010014h[a]	AES-GCM with a 16 byte MAC	NIST SP 800-38D
00000400h – 0000FFFFh	Vendor Specific	
	All other values are reserved	

[a] The lower order 16 bits of this code value are assigned to match an IANA assigned value for an equivalent IKEv2 encryption algorithm and the high order 16 bits match the IANA assigned IKEv2 transform type (i.e., 1, Encryption Algorithms).