To: INCITS Technical Committee T10
From: Gideon Avida, Decru
Date: July 16, 2007
Document: T10/07-254r1
Subject: SSC-3 Set Data Encryption Parameters through an SA.

1. Revision History

Revision 0:
Initial revision posted to the T10 web site on May 15, 2007.

2. References

T10/SSC-4 revision 3c
T10/07-169r0 ESP-SCSI for Parameter Data
T10/06-225r7 SSC-3: Key Entry using Encapsulating Security Payload (ESP)
FIPS 140-2 SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES
NIST SP800-57 Recommendation for Key Management – Part 1: General, March 2007

3. General

On May 8, 2007, the SSC-3 working group approved proposal 06-225r7 for inclusion in SSC-3. The purpose of the proposal is to provide a way for the application client to pass an encrypted key to the device server. However, by limiting the encapsulation only to the raw key material, the proposal violates security best practices.

Best practices require that the association between a key and its usage be maintained for the lifetime of the key and the data it protects. E.g. SP800-57 Part 1 section 6.1 specifies:

Association protection **shall** be provided for a cryptographic security service by ensuring that the correct keying material is used with the correct data in the correct application or equipment. Guidance for the selection of appropriate association protection is given in Sections 6.2.1.4 and 6.2.2.4.

Additionally, FIPS 140-2 section 4.7.4 Key Entry and Output specifies:

A cryptographic module shall associate a key (secret, private, or public) entered into or output from the module with the correct entity (i.e., person, group, or process) to which the key is assigned.

This proposal attempts to fix this oversight.

This proposal should be used to replace 06-225r7.

4. Changes to SSC-3

4.0 Add references to NIST documents (same as in SPC-4):

2.4 NIST References

Copies of the following approved NIST standards may be obtained through the National Institute of Standards and Technology (NIST) at http://csrc.nist.gov/publications/nistpubs/index.html.

NIST SP (Special Publication) 800-57 Recommendation for Key Management – Part 1: General, March 2007

4.1. Addition to model clause

4.2.21.2 Encryption key protection using Security Associations

Security Associations (see SPC-4) may be used to protect data encryption keys and associated data encryption parameters from disclosure and modification.

A device server that supports SAs as a way to protect keys may require that all key operations be protected using an SA.

Note: NIST SP800-57 Part 1 discourages combining non-comparable strength algorithms.

4.2. Changes to table 112

Table 112 — 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
001~~1~~2h-FEFFh	Reserved	
FF00h-FFFFh	Vendor specific	

4.3. New section: 8.5.3.3 Encapsulated Set Data Encryption Page

8.5.3.3 SA Encapsulation Page

The SA Encapsulation page shall contain an ESP-SCSI out descriptor (see SPC-4) that has been encrypted in accordance with an SA that has been created in the device server (see SPC-4). The SA shall use an encryption algorithm other than ENCR_NULL.

If the USAGE_TYPE SA parameter in the SA associated with the value in the DS_SAI field in the ESP-SCSI out w/o length descriptor is not set to 0081h (i.e. Tape Data Encryption), then 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 SA USAGE.

Table T specifies the format of the Encapsulated Set Data Encryption Page.

Table T - SA encapsulation Page

Bit / Byte	7	6	5	4	3	2	1	0
0	(MSB)	PAGE CODE (0011h)						
1								LSB
2		ESP-SCSI out descriptor (see SPC-4)						
m								

The page code field (0011h) specifies a page being transferred.

The ESP-SCSI out descriptor is defined in SPC-4. The encrypted or authenticated data field in the ESP-SCSI out descriptor contains any Tape Data Encryption security protocol SECURITY PROTOCOL OUT command page except the page with page code 0011h (i.e., this page)