To: INCITS Technical Committee T10
From: Gideon Avida, Decru
Date: May 15, 2007
Document: T10/07-254r0
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

4.1. Addition to model clause

4.2.21.2 Encryption key protection using Security Associations

A device server that supports data encryption may protect data encryption keys and associated data encryption parameters from disclosure and modification by using a Security Association (see SPC-4).

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

Note: best practices (e.g. SP800-57 Part 1, section 5.6.3) discourage combining non-comparable strength algorithms because the weakest algorithm and key size used to provide cryptographic protection determines the strength of the protection.

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	Encapsulated Set Data Encryption 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 Encapsulated Set Data Encryption Page

The Encapsulated Set Data Encryption 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 USAGE TYPE SA PARAMETER.

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

Table T - Encapsulated Set Data Encryption Page

Bit Byte	7	6	5	4	3	2	1	0
0	(MSB)	PAGE CODE (0011h)						
1								LSB
2	(MSB)	PAGE LENGTH (m-3)						
3								(LSB)
4	(MSB)	DS_SAI						
7								(LSB)
8	(MSB)	DS_SQN						
11								(LSB)
12	(MSB)	INITIALIZATION VECTOR						
s-1								(LSB)
s	SCOPE			Reserved				LOCK
s+1	Reserved				SDK	CKOD	CKORP	CKORL
s+2	ENCRYPTION MODE							
s+3	DECRYPTION MODE							
s+4	ALGORITHM INDEX							
s+5	KEY FORMAT							
s+6	Reserved							
s+13								
s+14	(MSB)	KEY LENGTH (n-15)						
s+15								(LSB)
s+16	KEY							
s+n								
s+n+1	KEY-ASSOCIATED DATA DESCRIPTORS LIST							
p-1								
p	PADDING (Optional)							
i-1								
i	(MSB)	INTEGRITY CHECK VALUE						
m								(LSB)

See SPC-4 for a description of the DS_SAI, DS_SQN, INITIALIZATION VECTOR, PADDING and INTEGRITY CHECK VALUE fields. The bytes in the range s to i-1 shall be considered as the ENCRYPTED OR AUTHENTICATED DATA field of the ESP-SCSI data-out descriptor.

See 8.5.3.2 for a description of the SCOPE, LOCK, SDK, CKOD, CKORP, CKORL, ENCRYPTION MODE, DECRYPTION MODE, ALGORITHM INDEX, KEY FORMAT, KEY LENGTH, KEY and KEY-ASSOCIATED DATA DESCRIPTORS LIST fields.