TO: T10 Membership
FROM: Paul A. Suhler, Quantum Corporation
DATE: 16 January 2007
SUBJECT: T10/06-412r3, SSC-3 Encryption KAD Lengths and Nonces

1 Revisions

0 Initial revision (8 September 2006)

1 Second revision (20 October 2006) Incorporated changes from 12 September 2006 working group meeting.
Removed keyless copying; Kevin Butt will submit a new proposal. Minor tweaks to KAD length.

2 Third revision (8 November 2006). Incorporated comments from 7 November 2006 working group meeting. Changes are with respect to SSC-3, rev. 3b.

3 Fourth revision (16 January 2007). Incorporated comments from 16 January 2007 working group meeting. Changes are with respect to SSC-3, rev. 3b.
Removed section on effects of resets.

2 General

Discussions in the LTO community have uncovered a number of ambiguities and difficulties in the encryption sections of SSC-3, rev. 3a:

- Lengths of key-associated data.
- Making reporting of nonce descriptors optional.
- Effects of resets on encryption parameters. [Not addressed in final proposal.]
- Keyless copying of encrypted volumes. [Not addressed in final proposal.]

Thanks to Kevin Butt for providing the keyless copy section of the original proposal.

Thanks to Paul Entzel for advice on specifying KAD length.

Markup convention:

Blue text is added text.

~~Red Strikethrough is deleted text~~

Black is existing text

3 Key-associated data lengths

3.1 Discussion

An application client must be able to send a descriptor (in a Set Data Encryption page), read it back (e.g., in an Encryption Status page), and compare the values for correctness. An ambiguity arises for formats that assume fixed length values, with no indication of the length of data provided by the application client. To compare (longer) read values with (shorter) written values, the application client must known how the written data was padded.

Currently, there is no guidance in SSC-3 on how a device server should process a key descriptor (KADs or nonces) which is shorter than the length required by the medium format. I propose to add two bits to the Data Encryption Algorithm descriptor for the device server to specify whether the length of A-KAD and U-KAD must match the maximum lengths allowed, and to require the application client to send the descriptors in the Set Data Encryption page when the bits are set.

3.2 Changes

Change Table 99 – Data Encryption Algorithm descriptor:

Byte	Bits 7	6	5	4	3	2	1	0
0	Algorithm Index (00h)							
1	Reserved							
2	(MSB)	Descriptor Length (14h)						
3								(LSB)
4	AVFMV	SDK_C	MAC_C	DED_C	DECRYPT_C		ENCRYPT_C	
5	Reserved		NONCE_C		Reserved		UKADF	AKADF
6	(MSB)	Maximum Unauthenticated Key-Associated Bytes						
7								(LSB)
8	(MSB)	Maximum Authenticated Key-Associated Bytes						
9								(LSB)
10	(MSB)	Key Size (0020h)						
11								(LSB)
12		Reserved						
19								
20	(MSB)	Encryption Algorithm Identifier						
23								(LSB)

Add the following two paragraphs after Table 102 – NONCE_C field values:

The U-KAD Fixed (UKADF) bit shall be set to one if the device server requires the length of U-KAD in the parameter data for a SECURITY PROTOCOL OUT command to equal the value in the MAXIMUM UNAUTHENTICATED KEY-ASSOCIATED BYTES field. If the UKADF bit is set to one, then the MAXIMUM UNAUTHENTICATED KEY-ASSOCIATED BYTES field shall contain a non-zero value. If the UKADF bit is set to zero and the value in the MAXIMUM UNAUTHENTICATED KEY-ASSOCIATED BYTES field is non-zero, then the length of the U-KAD, if present in the parameter data for a SECURITY PROTOCOL OUT command, shall be a value between one and the value in the MAXIMUM UNAUTHENTICATED KEY-ASSOCIATED BYTES field.

The A-KAD Fixed (AKADF) bit shall be set to one if the device server requires the length of A-KAD in the parameter data for a SECURITY PROTOCOL OUT command to equal the value in the MAXIMUM AUTHENTICATED KEY-ASSOCIATED BYTES field. If the AKADF bit is set to one, then the MAXIMUM AUTHENTICATED KEY-ASSOCIATED BYTES field shall contain a non-zero value. If the AKADF bit is set to zero and the value in the MAXIMUM AUTHENTICATED KEY-ASSOCIATED BYTES field is non-zero, then the length of the A-KAD, if present in the parameter data for a SECURITY PROTOCOL OUT command, shall be a value between one and the value in the MAXIMUM AUTHENTICATED KEY-ASSOCIATED BYTES field.

In clause 8.5.3.2 (Set Data Encryption page), add text to the fourth and fifth paragraphs after Table 115 – KEY field contents with KEY FORMAT field set to 00h:

An unauthenticated key-associated data descriptor (see 8.5.4.3) may be included if any unauthenticated key-associated data is to be associated with logical blocks encrypted with the algorithm and key. The AUTHENTICATED field is reserved. The KEY DESCRIPTOR field shall contain the U-KAD value associated with the encrypted block. 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 FIELD IN PARAMETER DATA if the UKADF bit is set

to one in the data encryption algorithm descriptor, the ENCRYPTION MODE field is set to ENCRYPT, and:

a) the length of the KEY DESCRIPTOR field is not equal to the value in the MAXIMUM UNAUTHENTICATED KEY-ASSOCIATED BYTES field of the data encryption algorithm descriptor; or
b) the parameter data does not contain an unauthenticated key-associated data descriptor.

An authenticated key-associated data descriptor (see 8.5.4.4) may be included if any authenticated key-associated data is to be associated with logical blocks encrypted with the algorithm and key. The AUTHENTICATED field is reserved. The KEY DESCRIPTOR field shall contain the A-KAD value associated with the encrypted block. 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 FIELD IN PARAMETER DATA if the AKADF bit is set to one in the data encryption algorithm descriptor, the ENCRYPTION MODE field is set to ENCRYPT, and:

a) the length of the KEY DESCRIPTOR field is not equal to the value in the MAXIMUM UNAUTHENTICATED KEY-ASSOCIATED BYTES field of the Data Encryption Algorithm descriptor; or
b) the parameter data does not contain an authenticated key-associated data descriptor.

4 Optional nonce reporting

4.1 Discussion

SSC-3 specifies that under certain conditions the device server shall include a nonce descriptor in the Next Block Encryption Status page. We have determined that reporting a nonce is not always useful and is thus not worth the implementation effort. I propose that reporting nonces in this page be made optional.

4.2 Changes

Change the final paragraph in clause 8.5.2.8 as follows:

~~A nonce value descriptor (see 8.5.4.5) shall be included if a nonce value was not generated by the device server (i.e., it was established by a nonce value descriptor that was included with the key and algorithm identifier used to encrypt the logical block.) or if the device server can not determine if the nonce was generated by the device server that encrypted the logical block. A nonce value descriptor may be included if the nonce value was generated by the device server that encrypted the logical block.~~ ~~The~~ The page may include a nonce value descriptor (see 8.5.4.5). If one is included, then the AUTHENTICATED field shall indicate the status of the authentication done by the device server (see table 117). The KEY DESCRIPTOR field shall contain the nonce value associated with the encrypted block.