TO:	T10 Membership
FROM:	Paul A. Suhler Quantum Corporation paul.suhler@quantum.com
DATE:	20 October 2006
SUBJECT:	T10/06-412r1, SSC-3 Encryption KAD Lengths, Nonces, and Resets

1 Revisions

0 Initial revision (8 September 2006)

1 Initial revision (20 October 2006)
Removed keyless copying; Kevin Butt will submit a new proposal.

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.
- Keyless copying of encrypted volumes.

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

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. The two obvious options are:

- Avoid padding altogether by rejecting a descriptor shorter than the desired length; or
- Pad the descriptor to the desired length in a consistent manner.

Rather than outlawing either behavior, I propose that SSC-3 add enough detail to avoid ambiguity.

3.2 *Changes*

Insert the following text following the third paragraph after Table 114:

Option A:

Some media formats do not permit the device server reading a volume to determine how much of a key-associated data value or nonce value was provided by the application client and how much was provided by the device server which wrote the medium. If a device server implementing such a format receives a SECURITY PROTOCOL OUT command with parameter data containing a Set Data Encryption page containing a key descriptor in which the length of the KEY DESCRIPTOR field is less than the amount of data required by the medium format, then the device server shall either:

a) Return CHECK CONDITION, set the status sense key to ILLEGAL REQUEST, and set the sense code to INVALID FIELD IN PARAMETER DATA; or

b) Append padding bytes of 00h following the LSB of the value in the KEY DESCRIPTOR field to obtain a value of the length required by the format.

Option B:

If a device server receives a SECURITY PROTOCOL OUT command with parameter data containing a Set Data Encryption page containing a key descriptor in which the length of the KEY DESCRIPTOR field is less than the amount of data required by the medium format and the device server pads the received value to obtain the length required by the medium format, then the device server shall append padding bytes of 00h following the LSB of the value in the KEY DESCRIPTOR field to obtain a value of the length required by the format.

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 optionally 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.

5 Effects of resets on encryption parameters

5.1 *Discussion*

I would like to try for a consensus on whether logical unit resets should clear encryption parameters.

5.2 Changes

Add one item to the lettered list in clause 4.2.19.5:

e) a microcode update is performed on the device;
f) a logical unit reset occurs;
~~f~~g) a power on condition occurs; or
~~g~~h) other vendor-specific events.