TO: T10 Membership
FROM: Paul A. Suhler
Quantum Corporation
paul.suhler@quantum.com
DATE: 8 September 2006
SUBJECT: T10/06-412r0, SSC-3 Keyless Copying of Encrypted Media and Other Topics

1 Revisions

0 Initial revision (8 September 2006)

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

3.2 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.

3.3 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:

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

4.2 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.

4.3 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

5.2 Discussion

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

5.3 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.

6 Keyless copying of encrypted volumes

6.2 Discussion

The process for performing a keyless copy of an encrypted volume needs more detail in order to increase the chances that implementations will interoperate.

6.3 Changes

4

4.2

4.2.19

4.2.19.3 Reading encrypted data on the medium

.

.

.

If the device server is capable of distinguishing encrypted blocks from unencrypted blocks and the decryption mode is set to DECRYPT ~~or RAW~~, an attempt to read or verify an unencrypted block shall cause the device server to terminate the command with CHECK CONDITION status, with the sense key set to DATA PROTECT, and the additional sense code set to UNENCRYPTED DATA ENCOUNTERED WHILE DECRYPTING. The device server shall establish the logical position at the BOP side of the unencrypted block.

.

.

.

4.2.19.4 Keyless copy of encrypted data

In some scenarios it is desirable to copy data from one volume to another without needing knowledge of the encryption keys or the associated key-associated data used to encrypt the data on the volume. To accomplish this the source device decryption mode shall be set to RAW and the destination device shall be set to encryption mode EXTERNAL.

Some raw formats may be self-describing and do not need notification when changing from encrypted blocks to unencrypted blocks. Some formats may need notification when changing from encrypted blocks to unencrypted blocks so the encryption mode can be set to DISABLE on the destination device.

4.2.19.4.1 Formats that require notification of a change from an encrypted block to an unencrypted block

If the format requires notification of a change from an encrypted block to an unencrypted block, and if the device server is capable of distinguishing encrypted blocks from unencrypted blocks and the decryption mode is set to RAW, an attempt to read or verify an unencrypted block shall cause the device server to terminate the command with CHECK CONDITION status, with the sense key set to DATA PROTECT, and the additional sense code set to UNENCRYPTED DATA

ENCOUNTERED WHILE DECRYPTING. The device server shall establish the logical position at the BOP side of the unencrypted block. Any attempt to read or verify this block prior to the device server having successfully processed a Security Protocol Out command, Set Data Encryption page with the DECRYPTION MODE field set to DISABLE, shall cause the device server to terminate the command with CHECK CONDITION status, with the sense key set to DATA PROTECT, and the additional sense code set to UNENCRYPTED DATA ENCOUNTERED WHILE DECRYPTING. The device server shall establish the logical position at the BOP side of the encrypted block.

A device server that supports encryption and has been configured to read data with a decryption mode of RAW should be capable of determining when there is a change of the KAD data. If the device server is capable of determining when there is a change of the KAD data, an attempt to read or verify an encrypted block whose KAD data is different from the last block read or verified shall cause the device server to terminate the command with CHECK CONDITION status, with the sense key set to DATA PROTECT, and the additional sense code set to KAD CHANGED. The device server shall establish the logical position at the BOP side of the encrypted block. Any attempt to read or verify this block prior to the device server having successfully processed a Security Protocol Out command, Set Data Encryption page with the DECRYPTION MODE field set to RAW, shall cause the device server to terminate the command with CHECK CONDITION status, with the sense key set to DATA PROTECT, and the additional sense code set to KAD CHANGED. The device server shall establish the logical position at the BOP side of the encrypted block.

NOTE: KAD CHANGED is a new additional sense code (74/XX)

A device server that supports encryption and has been configured to read data with a decryption mode of RAW shall consider the processing of a space or locate type command a change of the KAD data. A subsequent attempt to read or verify an encrypted block shall cause the device server to terminate the command with CHECK CONDITION status, with the sense key set to DATA PROTECT, and the additional sense code set to KAD CHANGED. The device server shall establish the logical position at the BOP side of the encrypted block. Any attempt to read or verify this block prior to the device server having successfully processed a Security Protocol Out command, Set Data Encryption page with the DECRYPTION MODE field set to RAW, shall cause the device server to terminate the command with CHECK CONDITION status, with the sense key set to DATA PROTECT, and the additional sense code set to KAD CHANGED. The device server shall establish the logical position at the BOP side of the encrypted block.

A device server that supports encryption and has been configured to read data with a decryption mode of RAW shall consider the processing of a space or locate type command a change of the KAD data. A subsequent attempt to read or verify an unencrypted block shall cause the device server to terminate the command with CHECK CONDITION status, with the sense key set to DATA PROTECT, and the additional sense code set to UNENCRYPTED DATA ENCOUNTERED WHILE DECRYPTING. The device server shall establish the logical position at the BOP side of the unencrypted block. Any attempt to read or verify this block prior to the device server having successfully processed a Security Protocol Out command, Set Data Encryption page with the DECRYPTION MODE field set to DISABLE, shall cause the device server to terminate the command with CHECK CONDITION status, with the sense key set to DATA PROTECT, and the additional sense code set to UNENCRYPTED DATA ENCOUNTERED WHILE DECRYPTING. The device server shall establish the logical position at the BOP side of the unencrypted block.

If an application client that is copying data gets a CHECK CONDITION status, with the sense key set to DATA PROTECT, and the additional sense code set to KAD CHANGED, it should:

1) issue to the source drive a Security Protocol In command requesting the Next Block Encryption Status page,

2) issue to the destination drive a Security Protocol Out command, Set Data Encryption page with the ENCRYPTION MODE field set to EXTERNAL and the KEY-ASSOCIATED

DATA DESCRIPTORS LIST set to all the KAD descriptors received from the Next Block Encryption Status page from the source drive,

3) issue to the source drive a Security Protocol Out command, Set Data Encryption page with the DECRYPTION MODE field set to RAW which acknowledges the state change and allows continued reading, and

4) continue copying the volume.

If an application client that is copying data gets a CHECK CONDITION status, with the sense key set to DATA PROTECT, and the additional sense code set to UNENCRYPTED DATA ENCOUNTERED WHILE DECRYPTING, it should:

1) issue to the destination drive a Security Protocol Out command, Set Data Encryption page with the ENCRYPTION MODE field set to DISABLE and the KEY-ASSOCIATED DATA DESCRIPTORS LIST set to all the KAD descriptors received from the Next Block Encryption Status page from the source drive, if any,

2) issue to the source drive a Security Protocol Out command, Set Data Encryption page with the DECRYPTION MODE field set to DISABLE which acknowledges the state change and allows continued reading, and

3) continue copying the volume.

4.2.19.4.2 Formats that do not require notification of a change from an encrypted block to an unencrypted block

A device server that supports encryption and has been configured to read data with a decryption mode of RAW should be capable of determining when there is a change of the KAD data. If the device server is capable of determining when there is a change of the KAD data, an attempt to read or verify a block whose KAD data is different from the last block read or verified shall cause the device server to terminate the command with CHECK CONDITION status, with the sense key set to DATA PROTECT, and the additional sense code set to KAD CHANGED. The device server shall establish the logical position at the BOP side of the block. Any attempt to read or verify this block prior to the device server having successfully processed:

1) a Security Protocol In command requesting the Next Block Encryption Status page, and

2) a Security Protocol Out command, Set Data Encryption page with the DECRYPTION MODE field set to RAW,

shall cause the device server to terminate the command with CHECK CONDITION status, with the sense key set to DATA PROTECT, and the additional sense code set to KAD CHANGED. The device server shall establish the logical position at the BOP side of the block.

NOTE: KAD CHANGED is a new additional sense code (74/XX)

A device server that supports encryption and has been configured to read data with a decryption mode of RAW shall consider the processing of a space or locate type command a change of the KAD data. A subsequent attempt to read or verify a block shall cause the device server to terminate the command with CHECK CONDITION status, with the sense key set to DATA PROTECT, and the additional sense code set to KAD CHANGED. The device server shall establish the logical position at the BOP side of the block. Any attempt to read or verify this block prior to the device server having successfully processed:

1) a Security Protocol In command requesting the Next Block Encryption Status page, and

2) a Security Protocol Out command, Set Data Encryption page with the DECRYPTION MODE field set to RAW,

shall cause the device server to terminate the command with CHECK CONDITION status, with the sense key set to DATA PROTECT, and the additional sense code set to KAD CHANGED. The device server shall establish the logical position at the BOP side of the block.

If an application client that is copying data gets a CHECK CONDITION status, with the sense key set to DATA PROTECT, and the additional sense code set to KAD CHANGED, it should:

1) issue to the source drive a Security Protocol In command requesting the Next Block Encryption Status page,

2) issue to the destination drive a Security Protocol Out command, Set Data Encryption page with the ENCRYPTION MODE field set to EXTERNAL and the KEY-ASSOCIATED DATA DESCRIPTORS LIST set to all the KAD descriptors received from the Next Block Encryption Status page,

3) issue to the source drive a Security Protocol Out command, Set Data Encryption page with the DECRYPTION MODE field set to RAW, and

4) continue copying the volume.

4.2.19.5 Exhaustive-search attack prevention

4.2.19.6 Managing keys within the device server

4.2.19.7 Saved information per I_T nexus

4.2.19.8 Data encryption parameters

4.2.19.9 Key instance counter

4.2.19.10 Encryption mode locking

4.2.19.11 Nonce generation

4.2.19.12 Unauthenticated key-associated data (U-KAD) and authenticated key-associated data (A-KAD)

4.2.19.13 Meta-data key-associated data (M-KAD)

Some encryption algorithms allow or require the use of additional data which is associated with the key and the key-associated data descriptors for a keyless copy of encrypted data from one piece of medium to another.

This data shall be contained in an M-KAD field.

8.5.4.2 Tape Data Encryption descriptors format

.

.

.

Table 116 — KEY DESCRIPTOR TYPE field values

Code	Description	Reference
00h	Unauthenticated key-associated data	8.5.4.3
01h	Authenticated key-associated data	8.5.4.4
02h	Nonce value	8.5.4.5
03h	Meta-data key-associated data	8.5.4.6

04-BFh	Reserved	
C0h-FFh	Vendor specific	

.

.

.

8.5.3.2 Set Data Encryption page.

.

.

.

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.

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.

If a nonce value descriptor (see 8.5.4.5) is included and the algorithm and the device server supports application client generated nonce values, the value in the KEY DESCRIPTOR field shall be used as the nonce value for the encryption process. If a nonce value descriptor is included and the encryption algorithm or the device server does not support application client generated nonce values, the device server shall terminate the command with CHECK CONDITION, with the sense key set to ILLEGAL REQUEST, and the additional sense code set to INVALID FIELD IN PARAMETER LIST. If the encryption algorithm or the device server requires an application client generated nonce value and a nonce value descriptor is not included, the device server shall terminate the command with CHECK CONDITION, with the sense key set to ILLEGAL REQUEST, and the additional sense code set to INCOMPLETE KEY-ASSOCIATED DATA SET. If a nonce value descriptor is included, the AUTHENTICATED field is reserved. The KEY DESCRIPTOR field shall contain the nonce value associated with the encrypted block.

A meta-data key-associated data descriptor (see 8.5.4.6) may be included if any meta-data 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 M-KAD value associated with the encrypted block.

8.5.4 SECURITY PROTOCOL IN and SECURITY PROTOCOL OUT descriptors

.

.

.

8.5.4.6 Meta-data key-associated data key descriptor

The AUTHENTICATED field in a meta-data key-associated data descriptor shall be set to 2h.

The KEY DESCRIPTOR field of a meta-data key-associated data descriptor shall contain all information needed to successfully perform a keyless copy of encrypted data (see 4.2.19.4).