To: INCITS Technical Committee T10
From: Kevin Butt
Date: December 18, 2006 3:17 pm
Document: T10/06-462r1 — SSC-3: Keyless Copy

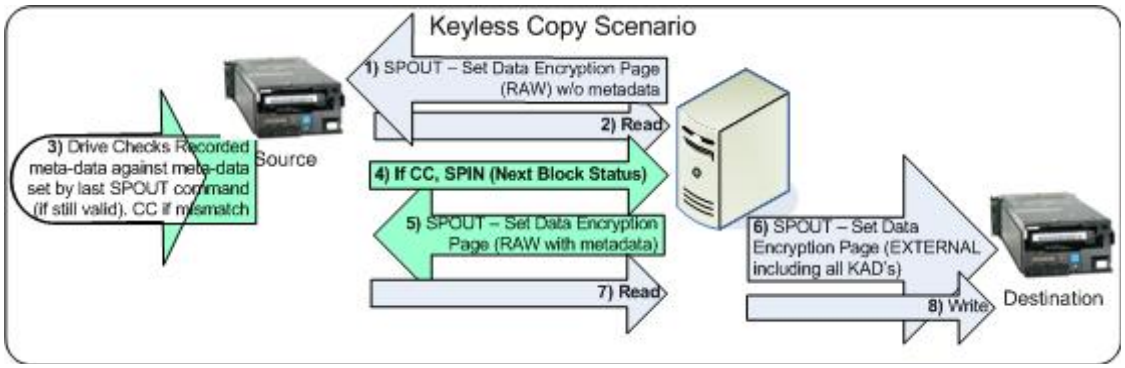
1. Revisions

1. 06-412r0 Initial revision (8 September 2006)
2. 06-412r1 Initial revision (?? October 2006)
3. 06-462r0 Split Keyless Copy from 06-412r1
4. 06-462r1 Worked with Paul Entzel to modify method via suggestion in 06-502r0.

2. Introduction

During the SSC working group meeting in November, Paul Entzel expressed some significant concerns about the direction this keyless copy proposal was heading. He presented 06-502r0 as an alternative approach. I agreed to work with Paul offline and see if we could come to an agreement on a simpler method of accomplishing the keyless copy. Paul and I have corresponded back and forth and I believe that this proposal is now much simpler and more accomodating to various formats.

To describe the proposed solution I will use a picture and description of each step here and then the proposal portion will attempt to capture the necessary modifications/additions to make it work.



1. The application sends a SPOUT command setting the decryption mode to RAW. No KAD descriptors are sent.
2. The application begins reading.
3. The drive checks to see if any KAD descriptors are required for a successful RAW read to EXTERNAL write. If yes (the format requires KAD descriptors sent), then the drive returns a CC with the sense key set to DATA PROTECT, and the additional sense code set to INCORRECT DATA ENCRYPTION KEY. If no (the format contains all data within the block), the drive returns the read data and skips to step 6.
4. The application sends a SPIN command requesting Next Block Status. This would potentially include KAD descriptor 0x03.

5. The application sends a SPOUT command setting the decryption mode RAW and the KAD descriptors to the KAD descriptors returned in step 4. Since the data manager is required to set the KAD descriptors (if there are any), there is an explicit action required.
6. The application sends a SPOUT command setting the encryption mode to EXTERNAL and, if step 4 was required, all the KAD descriptors returned in step 4.
7. The application reads data until finished or the next CC. If a CC is returned for incorrect data encryption key then go to step 4.
8. The application writes the data read (either in step 7 or step 2).

Additionally, we should be absolutely clear on what KAD data is compared. For instance, let's assume a format supports A-KAD, U-KAD, and some assorted other metadata that is neither of these. Let's say the format includes the A-KAD in the raw block, but does not include U-KAD and the other metadata in the raw block. The SPIN command will return descriptors for the A-KAD, the U-KAD, and the additional meta-data. We have to assume the application client does not know which of these will be included in the raw record and which will not, so it will send all 3 descriptors to both the source and the destination drive. Is the source drive required to compare the A-KAD for every block, even though it is passed in the raw block? We would prefer not, but how do we specify that?

3. Proposal

4.19.13 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 parameters used to encrypt the data on the volume. To accomplish this the source device server decryption mode shall be set to RAW and the destination device server encryption mode shall be set to EXTERNAL.

If the format in use by the device server requires key-associated data descriptors to be used while encrypting in EXTERNAL mode, an attempt to read or verify an encrypted block shall cause the device server to compare the key-associated data descriptors that are required when encrypting in EXTERNAL mode to the same key-associated data descripors that are part of the current encryption parameters. Key-associated data descriptors required to be compared by the format that do not match 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 INCORRECT ENCRYPTION PARAMETERS. The device server shall establish the logical position at the BOP side of the unencrypted block.

Editors Note: INCORRECT ENCRYPTION PARAMETERS in a new additional sense code. This should have an ASC of 74h.

4.2.19.22 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 volume to another.

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

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.

8.5.4.2 Tape Data Encryption descriptors format

.

.

.

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	

8.5.4.6 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).