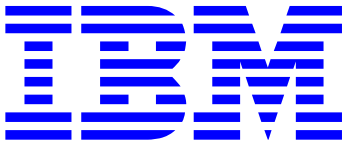
To: INCITS Technical Committee T10
From: Kevin Butt
Date: May 9, 2007 8:44 am
Document: T10/06-462r8 — SSC-3: Keyless Copy



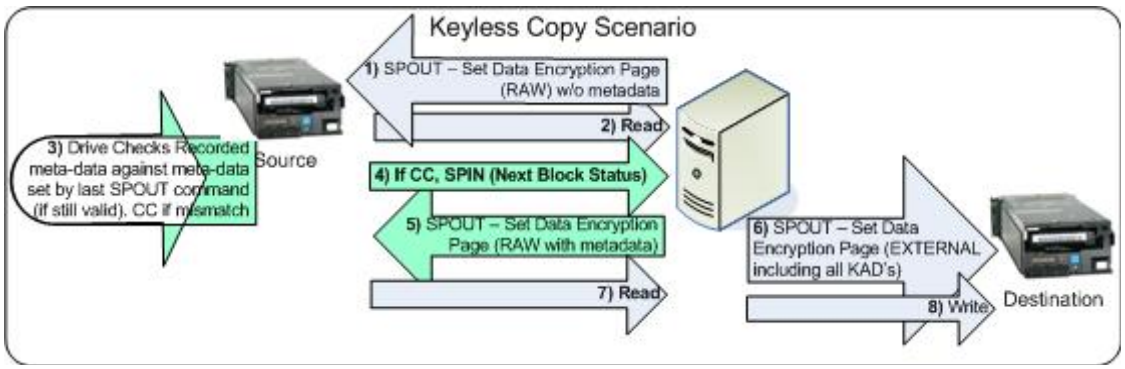
1. Revisions

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.
5. 06-462r2 Incorporated comments from January 2007 SSC-3 Working Group. Of major note is the addition of a flow chart that describes the steps in order to perform a keyless copy
6. 06-462r3 Incorporated comments from 14 February Teleconference. This revision has an informative flowchart for the application client. This revision does not include normative state diagrams for the source and target LUNs but attempts to describe things sufficiently to not need them. If state diagrams are still desired, it is requested that this proposal be allowed to be passed without them and an additional proposal be started for the state diagrams.
7. 06-462r4 Incorporated feedback from Paul Entzel received 05 Mar 2007. Cleaned up the informative flowchart for better efficiency, use the same acronyms as in the normative text, and made cleanup of encryption parameters happen in all exit modes. Changed KCSLUN/KCDLUN to KCSLU/KCDLU. Added descriptions of how the M-KAD may be used in the Data Encryption Status page and the Next Block Encryption status page.
8. 06-462r5 Modified the figure to describe an example of how an application client might implement a keyless copy, listed where to return to the flowchart for ILI and FM Check Conditions.
9. 06-462r6 Incorporated feedback from Paul Entzel - Yes, I even simplified the header text. Paul had issues with the paragraph “All algorithms that permit keyless copy shall require that all of the key-associated descriptors that are required to be set in the data encryption parameters when the encryption mode is set to EXTERNAL are also required to be set when performing a read operation while the decryption mode is set to RAW.“ However, this is what my notes tell me the working group told be to do. Therefore, I have not changed it. Probably a point to review.
10. 06-462r7 Correct list for detecting errors in the Set Data encryption pages that contain M-KAD. Modify flowchart to show transitions between unencrypted data and encrypted data during a keyless copy.
11. 06-462r8 Edits from May working group meeting. This is the version approved for inclusion into SSC-3

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 metadata. 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

~~**3.1.a keyless copy source logical unit (KCSLUN):** An entity that controls configuration and data flows related to the volume from which the encrypted data is copied (see Section 4.2.20.4).~~

~~**3.1.b keyless copy destination logical unit (KCDLUN):** An entity that controls configuration and data flows related to the volume to which the encrypted data is being copied (see Section 4.2.20.4).~~

3.2 Acronyms

M-KAD meta-data key associated data

4.2.20.4 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 parameters used to encrypt the data on the volume.

A keyless copy logical unit (KCLU) controls configuration and data flows related to a volume that is either a source or destination for encrypted data being transferred without requiring application client knowledge of an encryption key.

A keyless copy source logical unit (KCSLU) controls configuration and data flows related to the volume from which the encrypted data is copied without requiring ~~application client~~ device server knowledge of an encryption key when the decryption mode is set to RAW.

A keyless copy destination logical unit (KCDLU) controls configuration and data flows related to the volume to which the encrypted data is being copied without requiring ~~application client~~ device server knowledge of an encryption key when the encryption mode is set to EXTERNAL.

To accomplish a keyless copy operation an application client sets the KCSLU decryption mode to RAW and the KCDLU encryption mode to EXTERNAL. The application client then reads one or more logical objects from the KCSLU and writes those logical objects to the KCDLU. During this process if the KCSLU detects a mismatch between the key-associated data in the data encryption parameters and the key-associated data on the medium during a read operation, the KCSLU returns a CHECK CONDITION status to the application client to notify it that some action is required. An example of this is shown in the informative flowchart in Figure 1 on page 5.

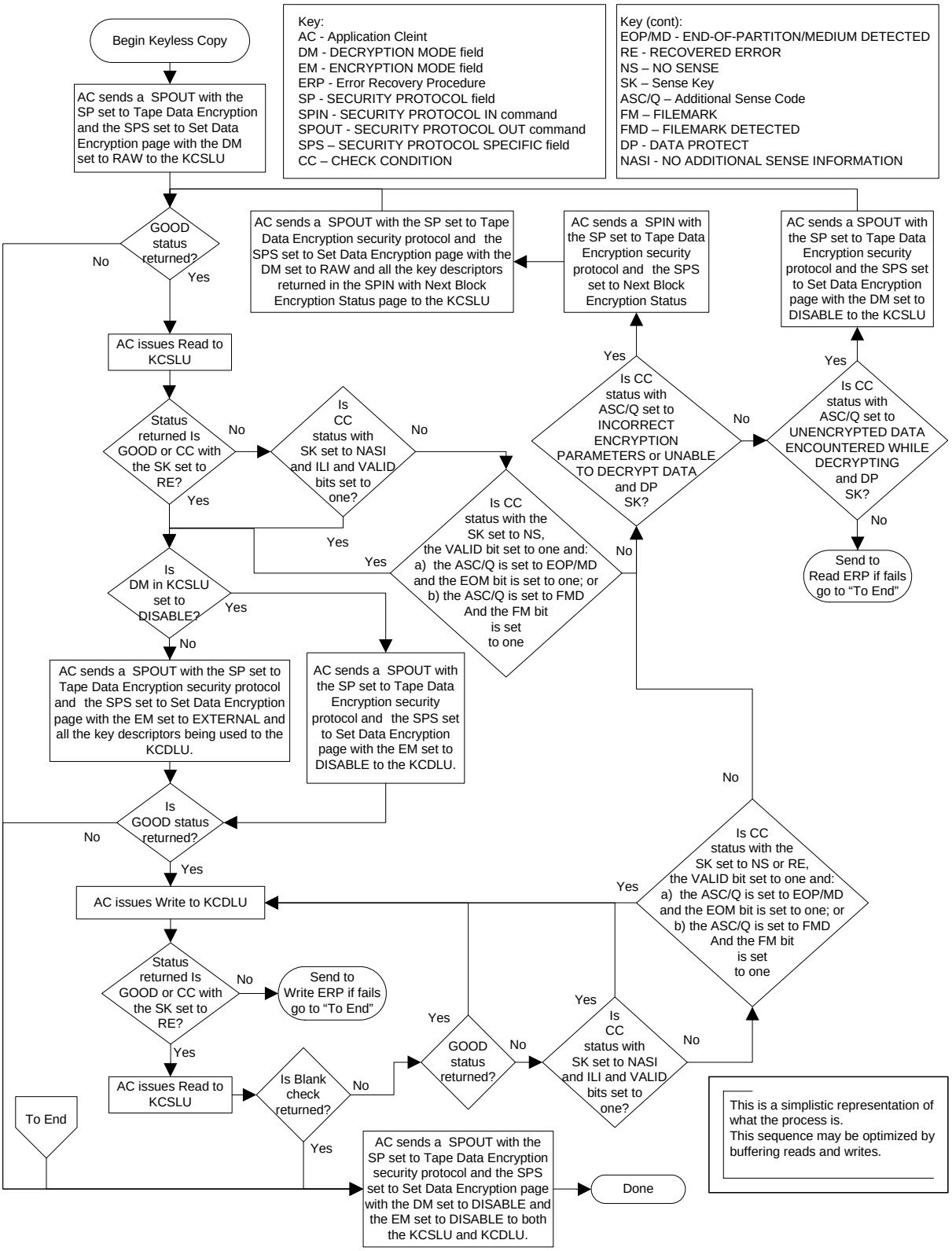


FIGURE 1. Example of a keyless copy operation

~~The key-associated data descriptors, if any, that are required for use when the ENCRYPTION MODE is set to EXTERNAL, shall also be required for use when the DECRYPTION MODE is set to RAW.~~

~~All algorithms that permit keyless copy shall require that all of the key-associated descriptors that are required to be set in the data encryption parameters when the encryption mode is set to EXTERNAL are also required to be set when performing a read operation while the decryption mode is set to RAW.~~

It shall not be considered an error if a Set Data Encryption page has the DECRYPTION MODE field is set to RAW and ~~all~~ any ~~the required key-associated data descriptors~~ of the key-associated data descriptors required by the algorithm specified by the value in the ALGORTIHM INDEX field are not present.

~~The KCLU is not required to validate that all required key-associated data descriptors to be used while decrypting in RAW mode are present when the DECRYPTION MODE field is set to RAW in the Set Data Encryption page. This allows an application client to use the same algorithm when performing a keyless copy operation regardless of a KCLUs requirements on key-associated data descriptors.~~

If the encryption algorithm in use by the KCSLU requires key-associated data ~~descriptors~~ to be ~~used while decrypting in RAW mode~~ included in the Set Data Encryption page when the ENCRYPTION MODE field is set to EXTERNAL, then an attempt to read or verify an encrypted block while the decryption mode is set to RAW shall cause the KCSLU to compare ~~those key-associated data descriptors~~ all key-associated data associated with each encrypted block that is read or verified to the corresponding key-associated data ~~descripors~~ that are part of ~~its~~ the current encryption parameters. Key-associated data ~~descriptors~~ required to be compared by the decryption algorithm that do not match or are not present shall cause the KCSLU 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 KCSLU shall establish the logical position at the BOP side of the block.

Editors Note: INCORRECT ENCRYPTION PARAMETERS in a new additional sense code. This should have an ASC of 74h.
When this proposal is passed this needs to be requested from the SPC-4 editor.

If a KCDLU receives a SECURITY PROTOCOL OUT command with a Set Data Encryption page with ~~encryption mode~~ the ENCRYPTION MODE field set to EXTERNAL, and any of the key associated data descriptors required ~~for a supported encryption algorithm~~ by the data encryption algorithm specified by the ALGORITHM INDEX field are not present or are ~~incorrect~~ not supported, then the KCDLU 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.

4.2.20.7 Data encryption parameters

A device server that supports data encryption shall have the ability to save the following information as a set of data encryption parameters when a Set Data Encryption page is processed:

a) for SCSI transport protocols where SCSI initiator device port names are required, the SCSI initiator device port name; otherwise, the SCSI initiator device port identifier;

b) indication of the SCSI target port through which the data encryption parameters were established;

c) key scope;

d) encryption mode;

e) decryption mode;

f) key;

g) supplemental decryption keys where supported;

h) algorithm index;

i) key instance counter;

j) CKOD;

k) CKORL;

l) CKORP;

m) U-KAD;

n) A-KAD; ~~and~~

o) nonce; and

p) M-KAD.

A device server may have limited resources for storage of sets of data encryption parameters (i.e., it may not have enough resources to store a unique set of data encryption parameters for every I_T nexus that it is capable of managing). A device server may release a previously established set of data encryption parameters when a Set Data Encryption page is processed and there are no unused resources available. The method of choosing which set of data encryption parameters to release is vendor specific. If the device server does release a previously established set of data encryption parameters to free the resource, it shall establish a unit attention condition for every affected I_T nexus (see 4.2.20.5) that has its registered for encryption unit attentions state set to one (see 4.2.20.6). A device server is not required to have separate resources to store data encryption parameters for every scope that is supported.

A device server shall support an encryption key scope value of ALL I_T NEXUS and shall have resources to save one set of data encryption parameters with this scope.

If the device server supports an encryption key scope value of LOCAL, it shall have resources to save one or more sets of data encryption parameters with this scope.

The data encryption parameters that shall be used for an I_T nexus shall be established by the following order of precedence:

a) if the data encryption scope for the I_T nexus is set to LOCAL or ALL I_T NEXUS (see 4.2.20.6), the data encryption parameters set by the last Set Data Encryption page from that I_T nexus; or

b) if the data encryption scope for the I_T nexus is set to PUBLIC:

   1) the data encryption parameters that have been saved by the device server with a key scope of ALL I_T NEXUS if any data encryption parameters have been saved with this key scope; or

   2) the default data encryption parameters.

4.2.20.13 Metadata 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~~ the key and every logical block encrypted with that key. This data ~~shall be~~ is contained in an M-KAD ~~field~~ descriptor.

8.5.2.7 Data Encryption Status page

.
.
.

An unauthenticated key-associated data descriptor (see 8.5.4.3) shall be included if an unauthenticated key-associated data descriptor was included when the key was established in the device server. The AUTHENTICATED field is reserved. The KEY DESCRIPTOR field shall contain the U-KAD value associated with the key.

An authenticated key-associated data descriptor (see 8.5.4.4) shall be included if an authenticated key-associated data descriptor was included when the key was established in the device server. The AUTHENTICATED field is reserved. The KEY DESCRIPTOR field shall contain the A-KAD value associated with the key.

A nonce value descriptor (see 8.5.4.5) shall be included if a nonce value descriptor was included when the key was established in the device server. The AUTHENTICATED field is reserved. The KEY DESCRIPTOR field shall contain the nonce value associated with the key. A nonce value descriptor may be included if no nonce value descriptor was included when the key was established in the device server. In this case, the KEY DESCRIPTOR field shall be set to the nonce value established by the device server for use with the selected key.

A M-KAD descriptor shall be included if the metadata key-associated data descriptor was included when the data encryption parameters were established. The KEY DESCRIPTOR field shall contain the M-KAD value associated with the key

8.5.2.8 Next Block Encryption Status page

.
.
.

An unauthenticated key-associated data descriptor (see 8.5.4.3) shall be included if any unauthenticated key-associated data is associated with the next logical block. The AUTHENTICATED field shall be set to 1. 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) shall be included if any authenticated key-associated data is associated with the next logical block. The AUTHENTICATED field shall indicate the status of the authentication done by the device server (see table 118). The KEY DESCRIPTOR field shall contain the A-KAD value associated with the encrypted block.

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 AUTHENTICATED field shall indicate the status of the authen-

tication done by the device server (see table 118). The KEY DESCRIPTOR field shall contain the nonce value associated with the encrypted block.

A M-KAD descriptor (see 8.5.4.4) shall be included if any M-KAD is associated with the next logical block and the decryption mode is set to RAW in the saved data encryption parameters currently associated with the I_T nexus on which this command was received. The KEY DESCRIPTOR field shall contain the M-KAD value associated with the encrypted block.

8.5.3.2 Set Data Encryption page.

.
.
.

If the ENCRYPTION MODE field is set to ENCRYPT the device server shall save the key-associated descriptors in the KEY-ASSOCIATED DATA DESCRIPTORS LIST field and associate them with every logical block that is encrypted with this key by the device server.

If the ENCRYPTION MODE field is set to EXTERNAL the device server shall save the key-associated descriptors in the KEY-ASSOCIATED DATA DESCRIPTORS LIST field and associate them with every logical block that is ~~encrypted with this key written by the device server~~ written using the data encryption parameters established by this command.

If more than one key-associated data descriptor is specified in the Set Data Encryption page, they shall be in increasing numeric order of the value in the DESCRIPTOR TYPE field.

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:

a) key-associated descriptors are included in the KEY-ASSOCIATED DATA DESCRIPTORS LIST field;

b) DECRYPTION MODE field is not set to RAW; and

c) the ENCRYPTION MODE field is not set to:

   A) EXTERNAL, or

   B) ENCRYPT.

~~If the ENCRYPTION MODE field is not set to EXTERNAL or ENCRYPT and the DECRYPTION MODE field is not set to RAW and key-associated descriptors are included in the KEY-ASSOCIATED DATA DESCRIPTORS LIST field, 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.~~

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 M-KAD descriptor (see 8.5.4.6) may be included if the DECRYPTION MODE field is set to RAW and the encryption algorithm requires any ~~metadata key-associated data~~ M-KAD to be associated with encrypted logical blocks read when the DECRYPTION MODE is set to RAW. ~~If a metadata key-associated data descriptor is included and the ENCRYPTION MODE is not set to EXTERNAL or the DECRYPTION MODE is not set to RAW or the device server does not support metadata key-associated data for an DECRYPTION MODE field set to RAW, 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. It shall not be considered an error if a metadata key-associated data descriptor (see 8.5.4.6) is not included and the DECRYPTION MODE field is set to RAW and the encryption algorithm requires any metadata key-associated data to be associated with encrypted logical blocks read when the DECRYPTION MODE is set to RAW.~~

A M-KAD descriptor (see 8.5.4.6) shall be included if the ENCRYPTION MODE field is set to EXTERNAL and the encryption algorithm requires any ~~metadata key-associated data~~ M-KAD to be associated with logical blocks written when the ENCRYPTION MODE is set to EXTERNAL. ~~If a metadata key-associated data descriptor is included and the ENCRYPTION MODE is not set to EXTERNAL or the DECRYPTION MODE is not set to RAW or the ENCRYPTION MODE is set to EXTERNAL and the encryption algorithm or the device server does not support metadata key-associated data for an ENCRYPTION MODE field set to EXTERNAL, 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.~~

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 an M-KAD is included and:

a) the ENCRYPTION MODE field is not set to EXTERNAL and the DECRYPTION MODE field is not set to RAW; or,

b) the encryption algorithm specified by the ALGORITHM INDEX field does not support M-KAD.

~~If the encryption algorithm or the device server requires a metadata key-associated data descriptor and a metadata key-associated 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. 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	M-KAD	8.5.4.6
04-BFh	Reserved	
C0h-FFh	Vendor specific	

8.5.4.6 M-KAD key descriptor

The AUTHENTICATED field in a M-KAD descriptor shall be set to 2h.

The KEY DESCRIPTOR field of a M-KAD descriptor contains data required by the ~~format~~ encryption algorithm for a keyless copy operation (see Section 4.2.20.4).