

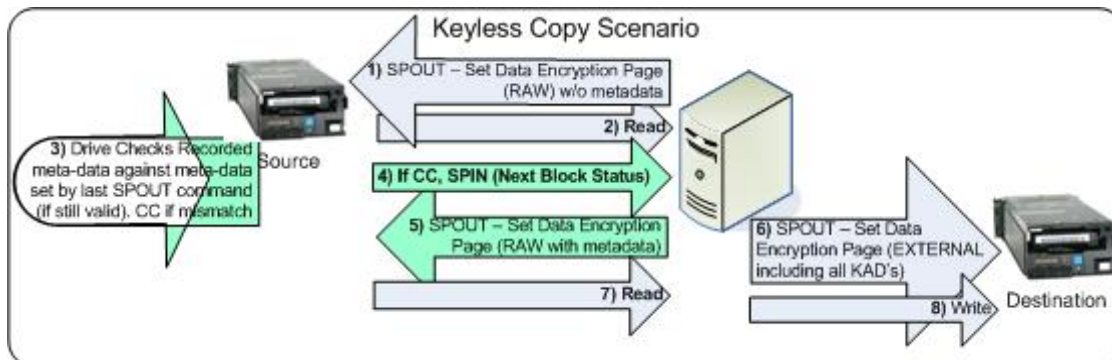
## 1. Revisions

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.

## 2. Introduction

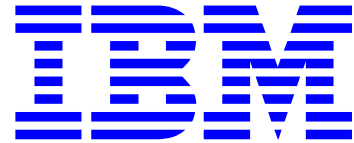
During the SSC working group meeting in November, Paul Entzel expressed some significant concerns about the direction this keyless copy proposal was heading. He presented 06-502r0 as an alternative approach. I agreed to work with Paul offline and see if we could come to an agreement on a simpler method 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 accommodating 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.

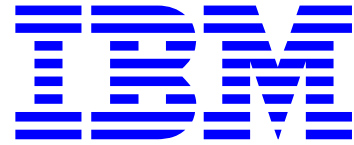
To: INCITS Technical Committee T10  
From: Kevin Butt  
Date: March 2, 2007 1:57 pm  
Document: T10/06-462r3 — SSC-3: Keyless Copy



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?

To: INCITS Technical Committee T10  
From: Kevin Butt  
Date: March 2, 2007 1:57 pm  
Document: T10/06-462r3 — SSC-3: Keyless Copy



## 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).

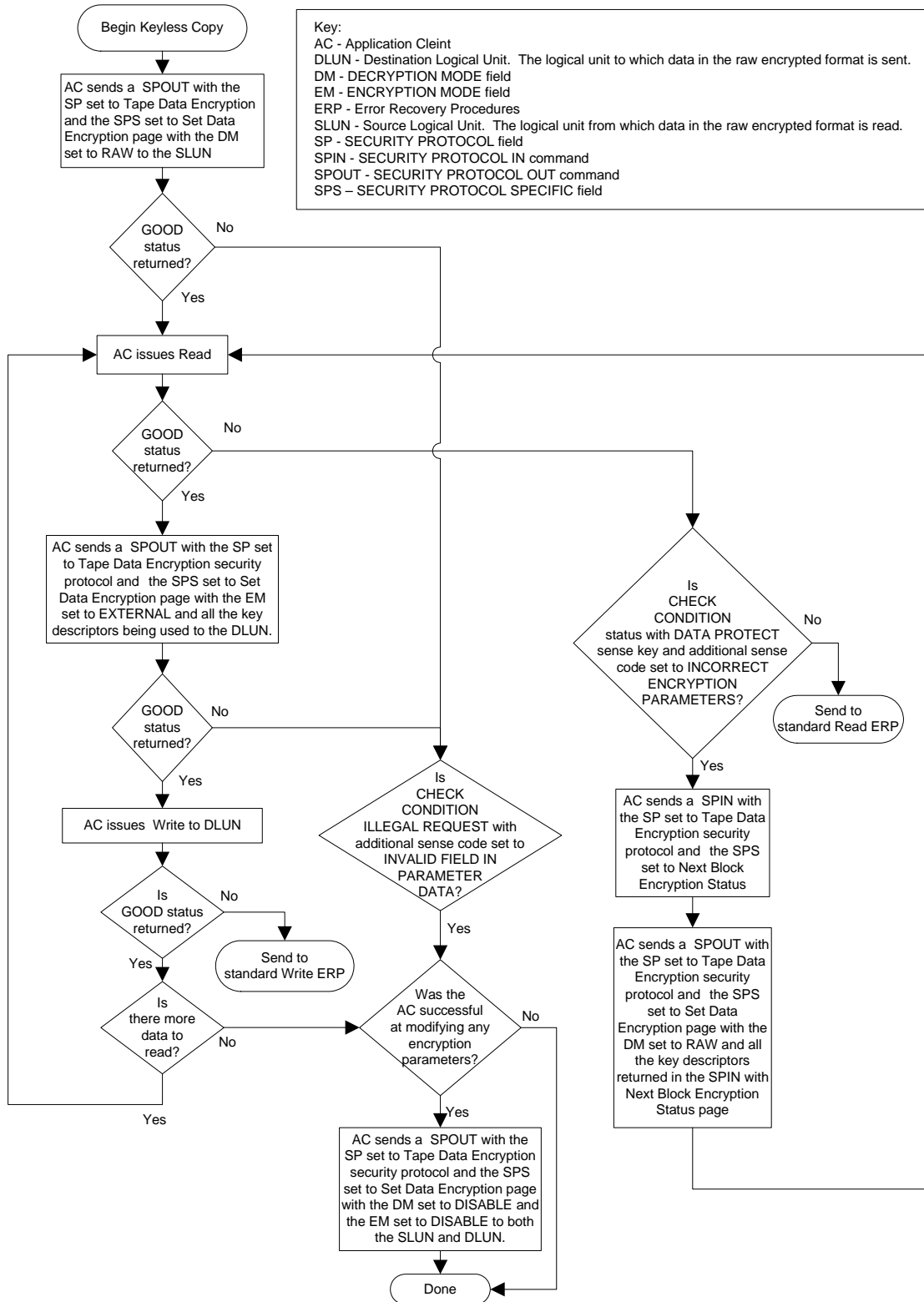
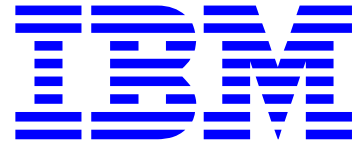
### **4.2.20.4 Keyless copy of encrypted data**

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 source logical unit controls configuration and data flows related to the volume from which the encrypted data is copied.

A keyless copy destination logical unit controls configuration and data flows related to the volume to which the encrypted data is being copied.

To accomplish an application client would set the KCSLUN decryption mode to RAW and the KCDLUN encryption mode to EXTERNAL. It would then read one or more logical objects from the KCSLUN while writing those logical objects to the KCDLUN. During this process if the KCSLUN detects an event that would require modification to the KCDLUN it returns a check condition to the application client to notify it that some action is required. An example of this is shown in the informative flowchart in figure xx.

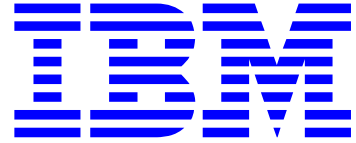


To: INCITS Technical Committee T10

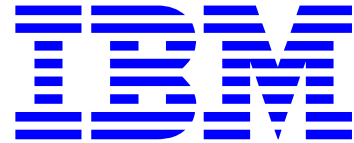
From: Kevin Butt

Date: March 2, 2007 1:57 pm

Document: T10/06-462r3 — SSC-3: Keyless Copy



To: INCITS Technical Committee T10  
From: Kevin Butt  
Date: March 2, 2007 1:57 pm  
Document: T10/06-462r3 — SSC-3: Keyless Copy



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.

If the encryption algorithm in use by the keyless copy source logical unit requires key-associated data descriptors to be used while decrypting in RAW mode, an attempt to read or verify an encrypted block while the decryption mode is set to RAW shall cause the keyless copy source logical unit to compare those key-associated data descriptors to the corresponding key-associated data descriptors that are part of its current encryption parameters. Key-associated data descriptors required to be compared by the decryption algorithm that do not match shall cause the keyless copy source logical unit 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 keyless copy source logical unit 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.**

---

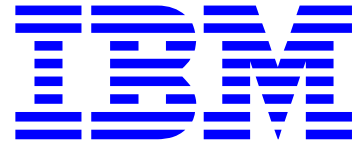
If a device server receives a SECURITY PROTOCOL OUT command with a SET DATA ENCRYPTION page with encryption mode set to EXTERNAL, and the key associated data descriptors required for a supported encryption algorithm are not present or are incorrect, then the device server shall terminate the command with CHECK CONDITION, with the sense key set to ILLEGAL REQUEST, and the additional sense code set to INVALID FIELD IN PARAMETER LIST.

#### **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;

To: INCITS Technical Committee T10  
From: Kevin Butt  
Date: March 2, 2007 1:57 pm  
Document: T10/06-462r3 — SSC-3: Keyless Copy



- 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:

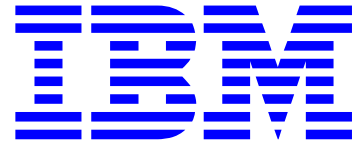
- a) if the data encryption scope for the I\_T nexus is set to LOCAL or ALL I\_T NEXUS (see 4.2.20.6), the data encryption parameters set by the last Set Data Encryption page from that I\_T nexus; or
- b) if the data encryption scope for the I\_T nexus is set to PUBLIC:
  - 1) the data encryption parameters 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 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.](#)

To: INCITS Technical Committee T10  
From: Kevin Butt  
Date: March 2, 2007 1:57 pm  
Document: T10/06-462r3 — SSC-3: Keyless Copy



### 8.5.3.2 *Set Data Encryption page.*

.  
. .  
.

#### **Add for EXTERNAL mode into 8.5.3:**

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 by the device server.

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.

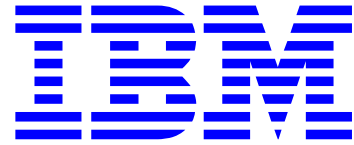
If the ENCRYPTION MODE field is not set to EXTERNAL or ENCRYPT and key-associated descriptors are included in the KEY-ASSOCIATED DATA DESCRIPTORS LIST field, the device server shall terminate the command with CHECK CONDITION, with the sense key set to ILLEGAL REQUEST, and the additional sense code set 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.





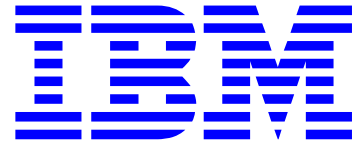
A metadata key-associated data descriptor (see 8.5.4.6) may be included if the DECRYPTION MODE field is set to RAW and the encryption algorithm requires any metadata key-associated data to be associated with encrypted logical blocks read when the DECRYPTION MODE is set to RAW. If a metadata key-associated 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 metadata key-associated data 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 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. 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 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
<u>03h</u>	<u>Meta-data key-associated data</u>	<u>8.5.4.6</u>
<u>04-BFh</u>	Reserved	
C0h-FFh	Vendor specific	

To: INCITS Technical Committee T10  
From: Kevin Butt  
Date: March 2, 2007 1:57 pm  
Document: T10/06-462r3 — SSC-3: Keyless Copy



**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 0h.

The KEY DESCRIPTOR field of a meta-data key-associated data descriptor contains data required by the format for a keyless copy operation (see Section 4.2.20.4).