To: INCITS T10 Committee

From: Paul Entzel, Quantum

Date: 30 March 2007

Document: T10/07-016r2

Subject: SSC-3 Additional controls for keyless copy

1 Revision History

Revision 0:
Initial revision posted to the T10 web site on 2 January 2007.

Revision 1:
Make CEEM code value 00b “vendor specific” and move the description from 00b to code value 01b.

Revision 2:
Updates based on feedback from the March 13 SSC-3 working group meeting:

1. Convert the “raw decryption mode enable” encryption parameter to “raw decryption mode disabled”.
2. Convert the RDME_C bit in the algorithm descriptor to a 3-bit field call RDMC_C. Include capabilities and default settings in the codes for this field.
3. Change the RDME bit in the Data Encryption Status page to RDMD and reworked its definition.
4. Change the RDMES bit in the Next Block Encryption Status page to RDMDS.
5. Change the RDME bit in the Set Data Encryption page to a 2-bit field called RDMC and defined new definitions to it that should make it compatible with more technologies.

2 Reference

T10/SSC-3 revision 3b
T10/06-0462r1, SSC3, Keyless Copy of Encrypted Data [Butt]

3 General

Concerns about a perceived security hole introduced by the keyless copy feature has caused at least one tape format to add some control over the feature. In particular:

1. A flag for encrypted blocks indicating the block is prohibited from raw decryption mode read operations that also prevents keyless copy operations.
2. A flag recorded with each block that indicates if the block was recorded while the encryption mode was set to EXTERNAL.

This proposal adds text to the model section describing how these flags shall be handled by a device server that supports a format that includes these KAD features. It also adds fields to several pages to coordinate the use of these features between the application client and the device server.

4 Changes to SSC-3

4.1 Add the following to the lettered list in 4.2.20.7

m) raw decryption mode disable, where supported;
n) check external encryption mode, where supported;

4.2 Add the following text to the Keyless Copy model clause (see 06-046)

Some encryption algorithms provide a mechanism to record with encrypted blocks the encryption mode setting when the encrypted block was written. The device server reports if an encryption algorithm supports this mechanism by way of the EAREM bit in the algorithm descriptor (see 8.5.2.4). If the encryption algorithm provides this capability, the device server may support a feature to check during read and verify operations if the block was written with the encryption mode set to EXTERNAL. The CEEM field in the Set Data Encryption page (See 8.5.3.2) provides the means to control the process of checking the encryption mode used when an encrypted block was written to tape.

If the decryption mode is set to DECRYPT or MIXED and the check external encryption mode data encryption parameter (see 4.2.20.7) is set to 10b:

1. the device server shall verify that each encrypted block that is processed for read and verify commands was written with the encryption mode set to ENCRYPT; and
2. if an attempt is made to read or verify an encrypted block that was written with the encryption mode set to EXTERNAL, the device server shall terminate the command with CHECK CONDITION status, with the sense key set to DATA PROTECT and the additional sense key set to ENCRYPTION MODE MISMATCH ON READ.

Editor's note: ENCRYPTION MODE MISMATCH ON READ is a new ASC.

If the decryption mode is set to DECRYPT or MIXED and the check external encryption mode data encryption parameter is set to 11b:

1. the device server shall verify that each encrypted block that is processed for read and verify commands was written with the encryption mode set to EXTERNAL; and
2. if an attempt is made to read or verify an encrypted block that was written with the encryption mode set to ENCRYPT, then the device server shall terminate the command with CHECK CONDITION status, with the sense key set to DATA PROTECT and the additional sense key set to ENCRYPTION MODE MISMATCH ON READ.

The check external encryption mode data encryption parameter shall not affect space or locate operations. The check external encryption mode data encryption parameter shall not affect read or verify operations on filemarks and unencrypted blocks.

Some encryption algorithms provide a mechanism to record with encrypted blocks an indication that they are disabled for raw decryption mode operations. The device server reports if an encryption algorithm supports this mechanism by way of the RDMC_C field in the algorithm descriptor (see 8.5.2.4). If the decryption mode is set to RAW and the encryption algorithm supports this feature, then:

1. the device server shall check the format specific indication that disables raw decryption mode operations for each encrypted block that is processed for read and verify commands; and
2. if an attempt is made to read or verify an encrypted block that was disabled for raw decryption mode operations, then the device server shall terminate the command with CHECK CONDITION status, with the sense key set to DATA PROTECT and the additional sense key set to ENCRYPTED BLOCK NOT RAW READ ENABLED.

Editor's note: ENCRYPTED BLOCK NOT RAW READ ENABLED is a new ASC.

4.3 Changes to 8.5.2.4

In the Algorithm Descriptor table (table 99), add 2 new bits:

Byte 5, bit 0: EAREM
Byte 5, bit 1-3: RDMC_C

Add the following text to describe these bits:

The raw decryption mode control capabilities (RDMC_C) field indicates the capabilities the encryption algorithm provides to the application client to control read operations that access encrypted blocks while the decryption mode is set to RAW. Table A defines the values for the RDMC_C field.

Table A – RDMC_C field values

Code	Description
0h	No capabilities are specified.
1h	The encryption algorithm does not allow read operations in RAW decryption mode.
2h – 3h	Reserved
4h	The encryption algorithm disables read operations in RAW mode by default and allows the application client to control RAW reads via the RDMC field in the Set Data Encryption page (see 8.5.3.2).
5h	The encryption algorithm enables read operations in RAW mode by default and allows the application client to control RAW reads via the RDMC field in the Set Data Encryption page.
6h	The encryption algorithm disables read operations in RAW mode by default and does not allow the application client to control RAW reads via the RDMC field in the Set Data Encryption page.
7h	The encryption algorithm enables read operations in RAW mode by default and does not allow the application client to control RAW reads via the RDMC field in the Set Data Encryption page.

The encryption algorithm records encryption mode (EAREM) bit shall be set to one if the encryption mode is recorded with each encrypted block. The EAREM bit shall be set to zero if the encryption mode is not recorded with each encrypted block.

4.4 Changes to 8.5.2.7

In the Data Encryption Status page table (table 105), add 2 new field:

Byte 12, bit 0: RDMD
Byte 12, bits 1-2: CEEMS

Add the following text to describe these fields:

The raw decryption mode disabled (RDMD) bit shall be set to one if the device server is configured to mark each encrypted record as disabled for raw read operations based on the RDMC_C value and the raw decryption mode disable parameter in the saved data encryption parameters currently associated with the I_T nexus on which the command was received (see 4.2.20.7).

The check external encryption mode status (CEEMS) field shall contain the value from the check external encryption mode parameter in the saved data encryption parameters currently associated with the I_T nexus on which the command was received (see 4.2.20.7).

4.5 Changes to 8.5.2.8

In the Next Block Encryption Status page table (table 106), add 2 new bits:

Byte 14, bit 0: RDMDS
Byte 14, bit 1: EMES

Add the following text to describe these bits:

The raw decryption mode disabled status (RDMDS) bit shall be set to one if the device server supports raw decryption mode, the ENCRYPTION STATUS field is set to either 5h or 6h, and the next block is marked as disabled for raw decryption mode operations (see 4.2.20). The RDMDS bit shall be set to zero if the device server does not support raw decryption mode, the ENCRYPTION STATUS field is set to a value other than 5h or 6h, or the next block is not marked as disabled for raw decryption mode operations.

The encryption mode external status (EMES) bit shall be set to one if:

a) the ENCRYPTION STATUS field is set to either 5h or 6h;
b) the EAREM bit in the algorithm descriptor (see 8.5.2.4) for the algorithm specified by the ALGORITHM INDEX field is set to one; and
c) the next block is marked as having been written to the medium while the encryption mode was set to EXTERNAL.

The EMES bit shall be set to zero if:

a) the ENCRYPTION STATUS field is set to a value other than 5h or 6h;
b) the EAREM bit in the algorithm descriptor for the algorithm specified by the ALGORITHM INDEX field is set to zero; or
c) the next block is marked as having been written to the medium while the encryption mode was set to ENCRYPT.

4.6 Changes to 8.5.3.2

In the Set Data Encryption page table (table 110), add 2 new fields:

Byte 5, bit 4-5: RDMC
Byte 5, bit 6-7: CEEM

Add the following text to describe these fields:

The raw decryption mode control (RDMC) field specifies if the device server shall mark each encrypted block written to the medium as disabled for read operations in raw mode (i.e., read operations with the decryption mode set to RAW). The RDMC field shall be ignored if the ENCRYPTION MODE field is not set to ENCRYPT. Table Y describes the values for the RDMC field when the ENCRYPTION MODE field is set to ENCRYPT.

Table Y – RDMC field values

Code	Description
00b	The device server shall mark each encrypted block per the default setting for the algorithm (see table A).
01b	Reserved
10b	The device server shall mark each encrypted block written to the medium in a format specific manner as enabled for raw decryption mode operations.
11b	The device server shall mark each encrypted block written to the medium in a format specific manner as disabled for raw decryption mode operations.

The device server shall terminate the command with CHECK CONDITION status, with the sense key set to ILLEGAL REQUEST and the additional sense key set to INVALID FIELD IN PARAMETER DATA if:

a) the ENCRYPTION MODE field is set to ENCRYPT;
b) the RDMC field is set to 10b or 11b; and
c) the RDMC_C field in the algorithm descriptor for the encryption algorithm selected by the value in the ALGORITHM INDEX field is set to 1h, 6, or 7h.

Table X describes the values for the check external encryption mode (CEEM) field.

Table X – CEEM field values

Code	Description
00b	Vendor specific
01b	Do not check the encryption mode that was in use when the block was written to the medium.
10b	On read and verify commands, check the encryption mode that was in use when the block was written to the medium. Report an error if the block was written in EXTERNAL mode (see 4.2.20.?).
11b	On read and verify commands, check the encryption mode that was in use when the block was written to the medium. Report an error if the block was written in ENCRYPT mode (see 4.2.20.?).

The device server shall terminate the SECURITY PROTOCOL OUT command with CHECK CONDITION status, with the sense key set to ILLEGAL REQUEST, and the additional sense code set to INVALID FIELD IN PARAMETER DATA if the CEEM field is set to either 10b or 11b, and:

a) the decryption mode field is set to DISABLE; or
b) the EAREM bit in the algorithm descriptor (see 8.5.2.4) for the algorithm specified by the ALGORITHM INDEX field is set to zero.