To: INCITS Technical Committee T10
From: Gideon Avida, Decru
Date: June 22, 2006
Document: T10/06-207r2
Subject: SSC-3: Add Encrypted Write Command

1 Revision History

Revision 0 (06-207r0): Posted to the T10 web site on April 20, 2006.

Revision 1 (06-207r1): Posted to the T10 web site on June 22, 2006

- Added WRITE ENCRYPTED (32) (3.1)
- Added bits in 8.5.3.2 table Y2 to define whether set of data encryption parameters apply to WRITE and/or WRITE ENCRYPTED. (3.3)

Revision 2 (06-207r2): Posted to the T10 web site on August 23, 2006.

- Incorporate feedback received in the Colorado Springs SSC-3 meeting:
  - Added KEY SCOPE to the WRITE ENCRYPTED parameters.
  - Cleaned section 3.3.
- 06-172r1 was incorporated into ssc3r03

2 Introduction

Proposal T10/06-172r1, SSC-3: Add commands to control data encryption (was 05-446, now in SSC-3) does not attempt to change the existing write commands to support data encryption. While the proposal does try to assure that once encryption is setup, the application server will get notified in case the encryption configuration changes, there are some cases where the application server might not get notified (e.g. the device server is behind a protocol bridge, implementation errors in the device server/OS/driver/application...) The only way to guarantee that the data will get either get encrypted or an error will be returned, is to mark the write operation for encryption. There is strong opposition to any changes to the current write commands from the ISV's because they usually don't have control over the write CDB. The other option is to create new commands for encrypted write.

The proposed WRITE ENCRYPTED(16) and WRITE ENCRYPED (32) will associate the write command to the desired encryption configuration by including the KEY INSTANCE COUNTER in the CDB. This will simplify error checking on the device server.

3 Proposed Changes to SSC-3

3.1 Changes to explicit address command descriptions for sequential-access devices clause (5)

In table 14 add the following command:

Command Name	Type	Opcode	Synchronization Operation Required	Command Type	Reference
WRITE ENCRYPTED(32)	O	XXh	No	W-E	5.X

Add the following sub-clause:

5.X WRITE ENCRYPTED (32) command

The WRITE(16) command (see table Y) requests that the device server write the logical block that is transferred from the application client to the logical object identifier and partition specified in the command descriptor block encrypted by the set of data encryption parameters established by a SECURITY PROTOCOL OUT command that sends a Set Data Encryption page (see 8.5.3.2).

Table Y — WRITE ENCRYPTED(32) command

Bit / Byte	7	6	5	4	3	2	1	0
0	OPERATION CODE (7Fh)							
1	CONTROL							
2	Reserved							
6								
7	ADDITIONAL CDB LENGTH (18h)							
8	(MSB)							
9	SERVICE ACTION (XXXXh)							(LSB)
10	Rsvd	KEY SCOPE			FCS	LCS	Rsvd	FIXED
11	PARTITION							
12	(MSB)							
19	LOGICAL OBJECT IDENTIFIER							(LSB)
20	(MSB)							
22	TRANSFER LENGTH							(LSB)
23	Reserved							
24	(MSB)							
27	KEY INSTANCE COUNTER							(LSB)
28	(MSB)							
31	Reserved							(LSB)

See the WRITE (16) command (see 5.6) for the definitions of the FCS bit, the LCS bit, the FIXED bit, the PARTITION field, the LOGICAL OBJECT IDENTIFIER field and the TRANSFER LENGTH field.

The KEY SCOPE field shall contain the value from the key scope in the saved data encryption parameters currently associated with the I_T nexus on which this command was received (see 4.2.19.7). If the KEY SCOPE does not match, the device server shall terminate the command with CHECK CONDITION status, with the sense key set to DATA PROTECT, and the additional sense code set to DATA ENCRYPTION PARAMETERS CHANGED BY ANOTHER I_T NEXUS.

KEY INSTANCE COUNTER is the same KEY INSTANCE COUNTER from the Data Encryption Status page (see 8.5.2.7). If the KEY INSTANCE COUNTER does not match, the device server shall terminate the command with CHECK CONDITION status, with the sense key set to DATA PROTECT, and the additional sense code set to DATA

ENCRYPTION KEY INSTANCE COUNTER HAS CHANGED. If encryption is not enabled, the device server shall terminate the command with CHECK CONDITION status, with the sense key set to DATA PROTECT, and the additional sense code set to DATA ENCRYPTION NOT ENABLED.

Editor's Note: DATA ENCRYPTION NOT ENABLED is a new ASC.

3.2 Changes to Implicit address command descriptions for sequential-access devices clause (6)

In table 21 add the following command:

Command Name	Type	Opcode	Synchronization Operation Required	Reference
WRITE ENCRYPTED(16)	O	XXh	No	6.X

Add the following sub-clause:

6.X WRITE ENCRYPTED(16) command

The WRITE ENCRYPTED command (see table W) requests that the device server write the logical block that is transferred from the application client to the current logical position encrypted by the set of data encryption parameters established by a SECURITY PROTOCOL OUT command that sends a Set Data Encryption page (see 8.5.3.2).

Table W — WRITE ENCRYPTED(16) command

Bit / Byte	7	6	5	4	3	2	1	0
0	OPERATION CODE (XXh)							
1	Rsvd	KEY SCOPE			Reserved			FIXED
2	Reserved							
3	Reserved							
4	(MSB)	KEY INSTANCE COUNTER						
7								(LSB)
8	(MSB)	Reserved						
11								(LSB)
12	(MSB)	TRANSFER LENGTH						
14								(LSB)
15	CONTROL							

The FIXED bit specifies whether fixed-block transfers or variable-block transfers are to be used. See the READ BLOCK LIMITS command (see 7.4) for additional information about fixed-block transfers and variable-block transfers.

The KEY SCOPE field shall contain the value from the key scope in the saved data encryption parameters currently associated with the I_T nexus on which this command was received (see 4.2.19.7). If the KEY SCOPE does not match, the device server shall terminate the command with CHECK CONDITION status, with the sense key set to DATA PROTECT, and the additional sense code set to DATA ENCRYPTION PARAMETERS CHANGED BY ANOTHER I_T NEXUS.

KEY INSTANCE COUNTER is the same KEY INSTANCE COUNTER from the Data Encryption Status page (see 8.5.2.7). If the KEY INSTANCE COUNTER does not match, the device server shall terminate the command with CHECK CONDITION status, with the sense key set to DATA PROTECT, and the additional sense code set to DATA ENCRYPTION KEY INSTANCE COUNTER HAS CHANGED. If encryption is not enabled, the device server shall terminate the command with CHECK CONDITION status, with the sense key set to DATA PROTECT, and the additional sense code set to DATA ENCRYPTION NOT ENABLED.

Editor's Note: DATA ENCRYPTION NOT ENABLED is a new ASC.

If the FIXED bit is one, the TRANSFER LENGTH value specifies the number of fixed-length blocks to be transferred, using the current block length reported in the mode parameter block descriptor (see 8.3). If the FIXED bit is zero, a single logical block is transferred with TRANSFER LENGTH specifying the logical block length in bytes.

If TRANSFER LENGTH is zero, no data shall be transferred and the current position shall not be changed. This condition shall not be considered an error.

A WRITE ENCRYPTED(16) command may be buffered or unbuffered, as specified by the BUFFERED MODE field of the mode parameter header (see 8.3). When operating in unbuffered mode (see 3.1.71), the device server shall not return GOOD status until all logical block(s) are successfully written to the medium. When operating in buffered mode (see 3.1.8), the device server may return GOOD status as soon as all logical block(s) are successfully transferred to the logical unit's object buffer.

NOTE i For compatibility with devices implemented prior to this version of this International Standard, a WRITE FILEMARKS command with the IMMED bit set to zero should be issued when completing a buffered write operation to perform a synchronize operation (see 4.2.8).

If the device server enables a WRITE ENCRYPTED(16) command while positioned between EW and EOP, or encounters EW during the processing of a WRITE ENCRYPTED(16) command, an attempt to finish writing any data may be made as determined by the current settings of the REW and SEW bits in the Device Configuration mode page (see 8.3.3). The command shall terminate with CHECK CONDITION status and the additional sense code shall be set to END-OF-PARTITION/MEDIUM DETECTED. If all data that is to be written is successfully transferred to the medium, the sense key shall be set to NO SENSE or RECOVERED ERROR, as appropriate. If the device server is unable to transfer any data, buffered or unbuffered, when early-warning is encountered, the sense key shall be set to VOLUME OVERFLOW. If the SEW bit is set to zero, the EOM bit shall be set to one in the sense data. If the SEW bit is set to one, the EOM and VALID bits shall be set to one in the sense data.

The INFORMATION field shall be set as follows:

a. if the FIXED bit is set to one, the INFORMATION field shall be set to the requested transfer length minus the actual number of logical blocks transferred to the device server; or
b. if the FIXED bit is set to zero, the INFORMATION field shall be set to the requested transfer length.

The device server should perform a synchronize operation (see 4.2.8) after the first early-warning indication has been returned to the application client (see 4.2.3).

NOTE j For some application clients it is important to recognize an error if end-of-partition is encountered during the processing of a WRITE ENCRYPTED(16) command, without regard for whether all data that is to be written is successfully transferred to the medium. The VOLUME OVERFLOW sense key may always validly be returned if end-of-partition is encountered while writing, and such usage is recommended. Reporting the MEDIUM ERROR sense key may cause confusion as to

whether there was really defective medium encountered during the processing of the last WRITE ENCRYPTED(16) command.

If a WRITE ENCRYPTED(16) command is terminated early, an incomplete logical block (i.e., a logical block not completely transferred to the device server from the initiator) shall be discarded. The incomplete logical block may be accessible prior to new data being written to the media. The device server shall be logically positioned after the last logical block that was successfully transferred.

3.3 Changes to Parameters for sequential-access devices

In 8.5.3.2 (**Set Data Encryption page**), extend the LOCK bit to be a two bits field (bits 0 and 1) and add the following table where LOCK is described:

Table x – LOCK field values

LOCK	Description
00b	Unlocked. The set of data encryption parameters apply to WRITE and WRITE ENCRYPTED COMMANDS.
01b	Locked (see 4.2.19.9). The set of data encryption parameters apply to WRITE and WRITE ENCRYPTED COMMANDS.
10b	The set of data encryption parameters established at the completion of the processing of the command applies only to data written with WRITE ENCRYPTED (16) and WRITE ENCRYPTED (32). Data sent with WRITE (6) and WRITE (16) is written in the clear.
11b	The set of data encryption parameters apply only to WRITE ENCRYPTED COMMANDS. WRITE commands will error.