To: INCITS Technical Committee T10

From: Kevin Butt, IBM

Date: May 10, 2006 3:19 pm

Document: T10/06-120r3

Subject: SSC-3: Secure Data Erase

1. Revisions

2. Introduction

There is a desire to have an additional mode in the Erase function that guarantees the data on medium is unrecoverable after successful completion. This is sometimes called shredding or Secure Data Erase. This proposal attempts to define this functionality and add the mode to the Erase commands. Additionally the data that is desired to be completely destroyed may include Control area information that exists in MAM or a special control area on medium that is not user data. This will be covered in as a separate setting.

I have included the complete text for the Erase commands for reference. Additions/changes are in this font which is blue.

2.1 Revision 1

Modifications are in this font.

TABLE 1. Use cases of Erase processing

UDSE	CASE	LONG	Description
0	0	0	SSC-2 short erase.
0	0	1	SSC-2 long erase
0	1	0	Remove history of how medium was used and perform SSC-2 short erase.
0	1	1	Remove history of how medium was used and perform SSC-2 long erase.
1	0	0	Remove security information and perform SSC-2 short erase.
1	0	1	Remove security information and perform new security erase that guarantees data cannot be recovered from the point of erasure.
1	1	0	Remove security information and history of how medium was used and perform SSC-2 short erase.
1	1	1	Remove security information, history of how medium was used, and perform new security erase that guarantees data cannot be recovered for the entire partition.

2.2 Revision 2

Incorporated some of the changes and suggestions from Paul Entzel. Changed location of UDSE and CASE bits in CDB's. Split the concept of the type of erase to perform (i.e. normal or security) into its own field and the areas to erase into their own fields. Added METHOD field and renamed UDSE and CASE to VCM and SMD.

2.3 Revision 3

Incorporated changes in SSC-3 Working Group on 09 May 2006. This version is the version created from revision 2 that was passed as modified in the working group meeting.

3. Proposal

3.1.x Vendor-specific Control Meta-data: Vendor-specific information stored on the volume outside the user data area(s) that is used to control or specify how the volume is being used by application clients (e.g. directory information, partition information, EOD locations, copies of data stored in vendor-specific manner, volume serial number information, number of blocks on media, etc).

3.1.y Security Meta-Data: Data used by security methods to enable user data to be returned in the form it existed prior to the application of the security methods (e.g. Data encryption parameters, passwords, wrapped keys). This data may be for vendor-specific security methods.

5.2 ERASE(16) command

The ERASE(16) command (see table 14) causes part or all of the medium to be erased beginning at the logical object identifier and partition specified in the command descriptor block. Prior to performing the erase operation, the device server shall perform a synchronize operation (see 4.2.8).

TABLE 14. ERASE(16) command

	7	6	5	4	3	2	1	0
0	OPERATION CODE (93h)							
1	Reserved				FCS	LCS	IMMED	LONG
2	Reserved		METHOD		Reserved		SMD	VCM
3	PARTITION							

TABLE 14. ERASE(16) command

	7	6	5	4	3	2	1	0
4	(MSB)							
5								
6								
7								
8				LOGICAL OBJECT IDENTIFIER				
9								
10								
11								(LSB)
12	Reserved							
13	Reserved							
14	Reserved							
15	CONTROL							

A first command in sequence (FCS) bit of one specifies this command is the first command in a tagged write sequence. An FCS bit of zero specifies this command is not the first command in a tagged write sequence.

A last command in sequence (LCS) bit of one specifies this command is the last command in a tagged write sequence. An LCS bit of zero specifies this command is not the last command in a tagged write sequence.

An immediate (IMMED) bit of zero specifies the device server shall not return status until the erase operation has completed. Interpretation of an IMMED bit of one depends on the value of the LONG bit, see below. However, for all values of the LONG bit, if CHECK CONDITION status is returned for an ERASE(16) command with an IMMED bit of one, the erase operation shall not be performed.

Note: Application clients should use an IMMED bit set to zero to guarantee the operation has completed successfully when using the METHOD field set to 10b. When using the METHOD field set to 10b, the duration of the processing may be extended (i.e. may be longer than just the LONG bit set to one).

A LONG bit of one specifies all remaining medium shall be erased beginning at the specified logical object identifier and partition shall be erased or over-written with a format specific pattern. If the format on the medium specifies a recorded indication of EOD (see 3.1.16), the erase operation shall establish an EOD indication at the specified location as part of the erase operation. If the IMMED bit is one, the device server shall return status as soon as all buffered logical objects have been written to the medium and the command descriptor block of the ERASE(16) command has been validated. The logical position following an ERASE(16) command with a LONG bit of one is not specified by this standard.

NOTE 7 Some logical units may reject an ERASE(16) command if the logical object identifier is not zero.

A LONG bit of zero specifies the device server shall perform the action specified by the short erase mode field in the Device Configuration Extension mode page (see 8.3.8) at the logical object identifier and partition specified in the command. The logical position following a ERASE(16) command with a LONG bit of zero shall be at the specified logical object identifier and partition. If the IMMED bit is one, the device server shall return status as soon as the command descriptor block has been validated.

The METHOD field specifies the erase method that shall be used to erase data. Table 15 defines the METHOD values. If the LONG bit is set to zero, the METHOD field only applies to data outside the user data area(s).

TABLE 15. METHOD definition

Value	Description
00b	Vendor-Specific
01b	The device server shall erase or over-write the volume with a format specific pattern. Upon successful processing of the command the volume may contain fragments of data specified for erasure. The data specified for erasure shall not be recognizable as valid user data using normal volume processing methods.
10b	The device server shall erase or over-write the volume with a format specific pattern(s). Upon successful processing of the command the volume shall not contain fragments of data specified for erasure.
11b	Reserved

NOTE: The METHOD field set to a value of 10b is intended to support data shredding (e.g. Sanitization as specified in DoD 5220.22-M<Editors Note: Include normative reference>).

A Security Meta-Data (SMD) bit set to one specifies that the device server shall alter the Security Meta-Data stored on the volume with the method specified by the METHOD field.

A SMD bit set to zero specifies that the device server handling of the Security Meta-Data stored on the volume is vendor-specific.

A Vendor-specific Control Meta-data (VCM) bit set to one specifies that the device server shall alter the Vendor-specific Control Meta-data stored on the volume with the method specified by the METHOD field.

A VCM bit set to zero specifies that the device server handling of the Vendor-specific Control Meta-data stored on the volume is vendor-specific.

If the logical unit encounters early-warning during an ERASE(16) command, and any buffered logical objects remain to be written, the device server action shall be as defined for the early-

warning condition of the WRITE(16) command (see 5.6). If the LONG bit is zero, the erase operation shall terminate with CHECK CONDITION status and the sense data shall be set as defined for the WRITE(16) command. Any count of pending buffered erases shall not be reported as part of the value returned in the INFORMATION field or in the READ POSITION response data.

The PARTITION and LOGICAL OBJECT IDENTIFIER fields specify the position at which the ERASE(16) command shall start. If the current position does not match the specified LOGICAL OBJECT IDENTIFIER and PARTITION fields, the device server shall perform a locate operation to the specified logical object identifier and partition prior to performing the erase operation. If the locate operation fails, the device server shall return CHECK CONDITION status and the additional sense code shall be set to LOCATE OPERATION FAILURE. The logical position is undefined following a locate operation failure with a LONG bit of zero.

6.2 ERASE(6) command

The ERASE(6) command (see table 21) causes part or all of the medium to be erased beginning at the current position. Prior to performing the erase operation, the device server shall perform a synchronize operation (see 4.2.8).

TABLE 21. ERASE(6) command

	7	6	5	4	3	2	1	0
0	OPERATION CODE (19h)							
1	Reserved						IMMED	LONG
2	Reserved		METHOD		Reserved		SMD	VCM
3	Reserved							
4	Reserved							
5	CONTROL							

An immediate (IMMED) bit of zero specifies the device server shall not return status until the erase operation has completed. Interpretation of an IMMED bit of one depends on the values of the LONG bit, see below. However, for all values of the LONG bit, if CHECK CONDITION status is returned for an ERASE(6) command with an IMMED bit of one, the erase operation shall not be performed.

Note: Application clients should use an IMMED bit set to zero to guarantee the operation has completed successfully when using the METHOD field set to 10b. When using the METHOD field set to 10b, the duration of the processing may be extended (i.e. may be longer than just the LONG bit set to one).

A LONG bit of one specifies all remaining medium in the current partition beginning at the current logical position shall be erased using the method indicated by the METHOD field (see Table 15). If the format on the medium specifies a recorded indication of EOD (see 3.1.16), the erase operation shall establish an EOD indication at the current logical position as part of the erase operation. If the IMMED bit is one, the device server shall return status as soon as all buffered

logical objects have been written to the medium and the command descriptor block of the ERASE(6) command has been validated. The logical position following an ERASE(6) command with a LONG bit of one is not specified by this standard.

NOTE 17 Some logical units may reject an ERASE(6) command if the logical unit is not at beginning-of-partition.

A LONG bit of zero specifies the device server shall perform the action specified by the SHORT ERASE MODE field in the Device Configuration Extension mode page (see 8.3.8) at the current logical position. If the IMMED bit is one, the device server shall return status as soon as the command descriptor block has been validated.

If the logical unit encounters early-warning during an ERASE(6) command, and any buffered logical objects remain to be written, the device server action shall be as defined for the early-warning condition of the WRITE(6) command (see 6.8). If the LONG bit is zero, the erase operation shall terminate with CHECK CONDITION status and set the sense data as defined for the WRITE(6) command. Any count of pending buffered erases shall not be reported as part of the value returned in the INFORMATION field or in the READ POSITION response data.

The METHOD field, Security Meta-Data (SMD) bit, and the Vendor-specific Control Meta-data (VCM) bit are defined in 5.2.