To: INCITS Technical Committee T10

From: Kevin Butt, IBM

Date: March 2, 2006 4:42 pm

Document: T10/06-120r0

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 bve 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.

3. Proposal

3.1.x Control Information: Information stored in auxiliary memory, either MAM or on tape in non-user data area, reflecting medium usage related information related to how it is being used by application clients (e.g. encryption keys, passwords, directory information, EOD locations, cached data). (Information that reveals how the medium has been used)

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	UDSE	CASE	Reserved		FCS	LCS	IMMED	LONG
2	Reserved							

TABLE 14. ERASE(16) command

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

Table 15 specifies the erase processing indicated by the UDSE, CASE, and LONG bits.

TABLE 15. Specification of Erase(16) processing

UDSE	CASE	LONG	Description
0	0	0	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.
0	0	1	The device server shall erase or over-write with a format specific pattern the remaining medium beginning at the specified logical object identifier and partition. After the processing of this command the data is not recognized as valid user data using normal medium processing methods. 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 the processing of the erase is not specified by this standard.

TABLE 15. Specification of Erase(16) processing

UDSE	CASE	LONG	Description
0	1	0	The device server shall erase or over-write with a format specific pattern control information saved on the medium (e.g. tape, auxiliary memory) including but not necessarily limited to that which is related to security features (e.g encryption, passwords). 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 BOP as part of the erase operation. If the medium is not positioned at BOP, the command shall be rejected with CHECK CONDITION status. The sense key shall be set to ILLEGAL REQUEST and the additional sense code shall be set to POSITION PAST BEGINNING OF MEDIUM.
0	1	1	The device server shall erase or over-write with a format specific pattern the remaining medium beginning at the specified logical object identifier and partition. After the processing of this command the data is not recognized as valid user data using normal medium processing methods. The device server shall also erase or over-write with a format specific pattern control information saved on the medium (e.g. tape, auxiliary memory) including but not necessarily limited to that which is related to security features (e.g encryption, passwords). 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 BOP as part of the erase operation. If the medium is not positioned at BOP, the command shall be rejected with CHECK CONDITION status. The sense key shall be set to ILLEGAL REQUEST and the additional sense code shall be set to POSITION PAST BEGINNING OF MEDIUM. 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 the processing of the erase is not specified by this standard.
1	0	0	The device server shall erase or over-write with a format specific pattern encryption key data and passwords. After processing of the erase no normal means (i.e., standard code method to read beyond EOD) should be possible, but there may be some magnetic residue on left on medium. 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 the processing of the erase is not specified by this standard.

TABLE 15. Specification of Erase(16) processing

UDSE	CASE	LONG	Description
1	0	1	The device server shall erase or over-write with a format specific pattern the remaining medium beginning at the specified logical object identifier and partition. The device server shall guarantee that there are no data fragments of user data left on the medium in the current partition from the point of erasure to EOP. This shall be done in a manner that prevents any future data recovery actions from being successful. 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 the processing of the erase is not specified by this standard.

TABLE 15. Specification of Erase(16) processing

UDSE	CASE	LONG	Description
1	1	0	The device server shall erase or over-write with a format specific pattern encryption key data and passwords. After processing of the erase no normal means (i.e., standard code method to read beyond EOD) should be possible, but there may be some magnetic residue on left on medium. The device server shall also erase or over-write with a format specific pattern control information saved on the medium (e.g. tape, auxiliary memory) including but not necessarily limited to that which is related to security features (e.g encryption, passwords). 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 BOP as part of the erase operation. If the medium is not positioned at BOP, the command shall be rejected with CHECK CONDITION status. The sense key shall be set to ILLEGAL REQUEST and the additional sense code shall be set to POSITION PAST BEGINNING OF MEDIUM. 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 the processing of the erase is not specified by this standard.
1	1	1	The device server shall erase or over-write with a format specific pattern the user data on the medium beginning at BOP of the specified partition. The device server shall guarantee that there are no data fragments of user data left on the medium in the specified partition from the point of erasure to EOP. This shall be done in a manner that prevents any future data recovery actions from being successful. 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 BOP as part of the erase operation. The device server shall also erase or over-write with a format specific pattern control information saved on the medium (e.g. tape, auxiliary memory) including but not necessarily limited to that which is related to security features (e.g encryption, passwords). If the medium is not positioned at BOP, the command shall be rejected with CHECK CONDITION status. The sense key shall be set to ILLEGAL REQUEST and the additional sense code shall be set to POSITION PAST BEGINNING OF MEDIUM. 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 the processing of the erase is not specified by this standard.

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 values in Table 15 ~~of the LONG bit, see below~~. However, for all values in Table 15 ~~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 UDSE set to one or CASE set to one. It should also be noted that when using UDSE set to one and LONG set to one, the duration of the processing may be very long (i.e. may be longer than just LONG 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.~~

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 (see4.2.8).

TABLE 21. ERASE(6) command

	7	6	5	4	3	2	1	0
0	OPERATION CODE (19h)							
1	UDSE	CASE	Reserved				IMMED	LONG
2	Reserved							
3	Reserved							
4	Reserved							
5	CONTROL							

Table 22 specifies the erase processing indicated by the UDSE, CASE, and LONG bits.

TABLE 22. Specification of Erase(16) processing

UDSE	CASE	LONG	Description
0	0	0	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 in the current 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 in the current partition. If the IMMED bit is one, the device server shall return status as soon as the command descriptor block has been validated.
0	0	1	The device server shall erase or over-write with a format specific pattern the remaining medium beginning at the specified logical object identifier in the current partition. After the processing of this command the data is not recognized as valid user data using normal medium processing methods. 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 the processing of the erase is not specified by this standard.

TABLE 22. Specification of Erase(16) processing

UDSE	CASE	LONG	Description
0	1	0	The device server shall erase or over-write with a format specific pattern control information saved on the medium (e.g. tape, auxiliary memory) including but not necessarily limited to that which is related to security features (e.g encryption, passwords). 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 BOP as part of the erase operation. If the medium is not positioned at BOP, the command shall be rejected with CHECK CONDITION status. The sense key shall be set to ILLEGAL REQUEST and the additional sense code shall be set to POSITION PAST BEGINNING OF MEDIUM. 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 the processing of the erase is not specified by this standard.
0	1	1	The device server shall erase or over-write with a format specific pattern the remaining medium beginning at the specified logical object identifier in the current partition. After the processing of this command the data is not recognized as valid user data using normal medium processing methods. The device server shall also erase or over-write with a format specific pattern control information saved on the medium (e.g. tape, auxiliary memory) including but not necessarily limited to that which is related to security features (e.g encryption, passwords). 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 BOP as part of the erase operation. If the medium is not positioned at BOP, the command shall be rejected with CHECK CONDITION status. The sense key shall be set to ILLEGAL REQUEST and the additional sense code shall be set to POSITION PAST BEGINNING OF MEDIUM. 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 the processing of the erase is not specified by this standard.
1	0	0	The device server shall erase or over-write with a format specific pattern encryption key data and passwords. After processing of the erase no normal means (i.e., standard code method to read beyond EOD) should be possible, but there may be some magnetic residue on left on medium. 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 the processing of the erase is not specified by this standard.

TABLE 22. Specification of Erase(16) processing

UDSE	CASE	LONG	Description
1	0	1	The device server shall erase or over-write with a format specific pattern the remaining medium beginning at the specified logical object identifier in the current partition. The device server shall guarantee that there are no data fragments of user data left on the medium in the current partition from the point of erasure to EOP. This shall be done in a manner that prevents any future data recovery actions from being successful. 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 the processing of the erase is not specified by this standard.

TABLE 22. Specification of Erase(16) processing

UDSE	CASE	LONG	Description
1	1	0	The device server shall erase or over-write with a format specific pattern encryption key data and passwords. After processing of the erase no normal means (i.e., standard code method to read beyond EOD) should be possible, but there may be some magnetic residue on left on medium. The device server shall also erase or over-write with a format specific pattern control information saved on the medium (e.g. tape, auxiliary memory) including but not necessarily limited to that which is related to security features (e.g encryption, passwords). 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 BOP as part of the erase operation. If the medium is not positioned at BOP, the command shall be rejected with CHECK CONDITION status. The sense key shall be set to ILLEGAL REQUEST and the additional sense code shall be set to POSITION PAST BEGINNING OF MEDIUM. 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 the processing of the erase is not specified by this standard.
1	1	1	The device server shall erase or over-write with a format specific pattern the user data on the medium beginning at BOP of the current partition. The device server shall guarantee that there are no data fragments of user data left on the medium in the specified partition from the point of erasure to EOP. This shall be done in a manner that prevents any future data recovery actions from being successful. 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 BOP as part of the erase operation. The device server shall also erase or over-write with a format specific pattern control information saved on the medium (e.g. tape, auxiliary memory) including but not necessarily limited to that which is related to security features (e.g encryption, passwords). If the medium is not positioned at BOP, the command shall be rejected with CHECK CONDITION status. The sense key shall be set to ILLEGAL REQUEST and the additional sense code shall be set to POSITION PAST BEGINNING OF MEDIUM. 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 the processing of the erase is not specified by this standard.

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 in Table 22 ~~of the LONG bit, see below~~. However, for all values in Table 22 ~~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 UDSE set to one or CASE set to one. It should also be noted that when using UDSE set to one and LONG set to one, the duration of the processing may be very long (i.e. may be longer than just LONG 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 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 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.