To: INCITS T10 Committee

From: Paul Entzel, Quantum

Date: 20 January 2005

Document: T10/04-373r2

Subject: SSC-3 model sub clause for WORM

1 Revision History

Revision 0:
Posted to the T10 web site on 5 November 2004.

Revision 1:
Updated based on discussion at the November T10 meeting (see 04-390) and the 3 December 2004 conference call (see 05-006). Posted to the T10 web site on 9 December 2004.

Revision 2:
Updated again based on discussion at the January 2005 T10 meeting (see 04-048). Posted to the T10 web site on 20 January 2005.

2 General

The concepts of archive tape and WORM mode have started creeping into SSC-3 without a good definition of these terms. This proposal adds definitions for the terms to the model section in SSC-3.

3 Proposed change

3.1 Definitions Clause

Add the following definition:

3.1.25 Format Label A vendor specific series of logical objects that contain information used to identify the volume or data set.

3.2 Model clause

Add the following sub clause to the model section of SSC-3:

4.2.19 Archive tape and WORM mode

4.2.19.1 WORM overview

An SSC-3 device may optionally support a Write Once, Read Many (WORM) mode of operations. This mode of operation places additional restrictions on the processing of commands by the device server.

4.2.19.2 Archive tape

An archive tape is identified by a format defined method (e.g, the Medium Type attribute in the MAM data returning a Write Once Medium type value).

4.2.19.2 WORM mode

A device server that supports WORM mode and detects an archive tape is mounted shall enter WORM mode. While in WORM mode, WRITE, WRITE FILEMARKS, ERASE, FORMAT MEDIUM, SET CAPACITY, and MODE SELECT commands that alter the partitioning or format are subject to the restrictions applied to archive tape by the device server (see 8.3.4).

If a device server operating in WORM mode detects that one of these additional restrictions would be violated by a command being processed, the device server shall terminate the command with CHECK CONDITION status, the Sense Key shall be set to DATA PROTECT, and the additional sense code shall be set to WORM MEDIUM – OVERWRITE ATTEMPTED. If a write protection is in effect for the device server or medium (see 4.2.12), it shall take precedence over the WORM violation.

If a device server operating in WORM mode is unable to determine if medium position is such that one of these additional restrictions would be violated by a command being processed, the device server shall terminate the command with CHECK CONDITION, the Sense Key shall be set to DATA PROTECT, and the additional sense code shall be set to WORM MEDIUM – OVERWRITE ATTEMPTED. If a write protection is in effect for the device server or medium (see 4.2.12), it shall take precedence over the WORM violation.

If a device server that does not support WORM mode detects that archive tape is mounted, it shall treat the medium as write protected. Any command that attempts to alter the medium shall be terminated with CHECK CONDITION status, the Sense Key shall be set to DATA PROTECT, and the additional sense code shall be set to CANNOT WRITE MEDIUM – INCOMPATIBLE FORMAT.

3.3 Add references

In section 4.2.16.4, add a reference:

"…it shall set that flag to one when an application client attempts to overwrite or erase user data on an archive tape (see 4.2.19).

In 8.4.2, replace the sentence:

“The definition of write once capability and WORM mode operation is TBD.”

With:

“See 4.2.19.2 for a definition of WORM mode”.

3.4 Add new mode page to section 8.3

Add to table 58 a new line:

15h Medium Configuration mode page

Add a new subclause to describe this new mode page:

8.3.4 Medium Configuration mode page

The Medium Configuration mode page (see table X) specifies any special considerations the device server shall use when processing commands with the medium.

Table X – Medium Configuration mode page

Bit Byte	7	6	5	4	3	2	1	0
0	PS	SPF(0)	PAGE CODE (1Dh)					
1	PAGE LENGTH (1Eh)							
2	Reserved							WORMM
3	Reserved							
4	WORM MODE LABEL RESTRICTIONS							
5	WORM MODE FILEMARK RESTRICTIONS							
6 - 31	Reserved							

The WORMM bit shall be set to one when the device server is operating in WORM mode (see 4.2.19.2). The WORMM bit shall be set to zero when the device server is not operating in WORM mode. If a MODE SELECT command is processed that attempts to change the setting of the WORMM bit, the device server shall return a CHECK CONDITION status, with the sense key set to ILLEGAL REQUEST, and the addition sense code set to INVALID FIELD IN PARAMETER LIST.

The WORM MODE LABEL RESTRICTIONS field specifies the restrictions against overwriting format labels when operating in WORM mode (see table Y). A series of filemarks with no interleaved logical blocks immediately preceding

EOD is treated as filemark sequence and controlled by the WORM MODE FILEMARKS RESTRICTIONS field.

Table Y – WORM MODE LABEL RESTRICTIONS field values

WORM MODE LABEL RESTRICTIONS	Description
00h	The device server shall not allow any logical blocks to be overwritten.
01h	The device server shall allow some types of format labels to be overwritten.
02h	The device server shall allow all format labels to be overwritten.
03h - FFh	Reserved.

The WORM MODE FILEMARKS RESTRICTIONS field specifies the restrictions against overwriting a series of filemarks immediately preceding EOD when operating in WORM mode (see table Z). This field controls only the overwriting of a series of filemarks with no interleaved logical blocks immediately preceding EOD.

Table Z – WORM MODE FILEMARKS RESTRICTIONS field values

WORM MODE FILEMARKS RESTRICTIONS	Description
00h – 01h	Reserved
02h	The device server shall allow any number of filemarks immediately preceding EOD to be overwritten except the filemark closest to BOP.
03h	The device server shall allow any number of filemarks immediately preceding EOD to be overwritten.
04h - FFh	Reserved.