ENDL
TEXAS

Date: 17 January 2001
To: T10 Technical Committee
From: Ralph O. Weber
Subject: CDB Structure Rewrite

Several SPC-2 letter ballot comments suggest non-substantive rewriting the subclauses in clause 4 that describe the general structure of a CDB (see 00-017r0 for letter ballot results and 00-267 for letter ballot comments resolution). A few comments require additions or changes to the existing text. So that the effects of the rewrite can be reviewed and discussed as a whole product, this proposal contains the complete rewrite.

Text created in response to letter ballot comments is blue and the comment number precedes the text in cyan surrounded by square brackets. Text generated by the editor as part of the restructuring is in red. Text that is unchanged from SPC-2 revision 18 is black. Text found in SPC-2 revision 18 that is proposed to be removed has a strike through. Text found in SPC-2 revision 18 that is proposed to be removed because it has been moved is in green with a strike through.

Revision 1 of this document reflects the decision of the September, 2000 CAP working group (minutes in 00-307) to make the ENCRYPTION IDENTIFICATION field Reserved in the variable length CDB and the requested wording to specify the case where the number of variable length CDB bytes delivered by the protocol doesn't match the additional length value in the CDB itself.

Revision 2 of this document corrects an oversight in revision 1 wherein text relating to encrypted CDBs was not marked for removal.

Revision 3 includes changes from recently accepted comments IBM 34) [5.34], IBM 35) [5.35], Seagate 18) [8.18], and Seagate 20) [8.20] (see 00-267r5.pdf). As of this writing all comments in 00-267r5 have a proposed resolution and no other comments are known to have a possibility of changing this proposal.

Revision 4 includes minor editorial changes requested by the January CAP working group.

4.3 The Command Descriptor Block (CDB)

4.3.1 CDB usage and structure

A command is communicated by sending a command descriptor block [5.26](CDB) to the device server. For several commands, the [5.26]CDB~~command descriptor block~~ is accompanied by a list of parameters in the Data-Out Buffer. See the specific commands for detailed information.

~~Except for the variable length CDB (see 4.3.3), the command descriptor block shall have an operation code as its first byte and a control byte as its last byte.~~ The fixed length CDB formats are described in 4.3.2. The variable length CDB formats are described in 4.3.3. The CDB fields that are common to most commands are described in 4.3.4. The [7.14]fields~~field uses~~ shown in 4.3.2 and 4.3.3~~tables 1, 2, 3, and 4~~ and described in 4.3.4 are used consistently by most commands. However, the actual usage of any field (except OPERATION CODE and CONTROL) is described in the [5.30]subclause defining that command.

~~The general structure of the operation code and control byte are defined in SAM-2.~~ If a device server receives a CDB containing an operation code that is invalid or not supported, it shall return CHECK CONDITION status with

18484 Preston Road, Suite 102#178, Dallas, TX 75252214-912-1373 972-596-2775 Fx ENDL_TX@computer.org

the sense key set to ILLEGAL REQUEST and an additional sense code of INVALID COMMAND OPERATION CODE.

For all commands, if there is an invalid parameter in the [5.26]CDB~~command descriptor block~~, then the device server shall terminate the command without altering the medium.

4.3.2 The fixed length CDB formats

All fixed length CDBs shall have an OPERATION CODE field as their first byte and a CONTROL byte as their last byte. Table 1 shows the typical format of a 6-byte CDB. Table 2 shows the typical format of a 10-byte CDB. Table 3 shows the typical format of a 12-byte CDB. Table 4 shows the typical format of a 16-byte CDB. [5.33]Table 5 shows the format of a 16-byte CDB for commands that provide for a long LBA.

Table 1 — Typical CDB for 6-byte commands

Bit / Byte	7	6	5	4	3	2	1	0
0	OPERATION CODE							
1	Reserved			(MSB)				
2	LOGICAL BLOCK ADDRESS (if required)							
3								(LSB)
4	TRANSFER LENGTH (if required) PARAMETER LIST LENGTH (if required) ALLOCATION LENGTH (if required)							
5	CONTROL							

Table 2 — Typical CDB for 10-byte commands

Bit / Byte	7	6	5	4	3	2	1	0
0	OPERATION CODE							
1	Reserved			SERVICE ACTION (if required)				
2	(MSB)	LOGICAL BLOCK ADDRESS (if required)						
3								
4								
5								(LSB)
6	Reserved							
7	(MSB)	TRANSFER LENGTH (if required) PARAMETER LIST LENGTH (if required) ALLOCATION LENGTH (if required)						
8								(LSB)
9	CONTROL							

~~The following field descriptions apply to tables 1, 2, 3, and 4. The OPERATION CODE field contains the code value identifying the operation being requested by the CDB. SAM-2 defines the general structure of the operation code value. This standard specifies the operation code values used by the commands defined herein. The contents of the CONTROL field are defined in SAM-2. The uses of the other fields defined in the typical CDB formats are described in 4.3.4.2 through 4.3.4.6.~~

~~Only the OPERATION CODE and CONTROL fields have consistently defined meanings across all commands. The field uses shown in tables 1, 2, 3, and 4 are used consistently by most commands. However, the actual usage of any field (except OPERATION CODE and CONTROL) is described in the clause defining that command.~~

Table 3 — Typical CDB for 12-byte commands

Bit / Byte	7	6	5	4	3	2	1	0
0	OPERATION CODE							
1	Reserved			SERVICE ACTION (if required)				
2	(MSB)							
3								
4				LOGICAL BLOCK ADDRESS (if required)				
5								(LSB)
6	(MSB)							
7				TRANSFER LENGTH (if required)				
8				PARAMETER LIST LENGTH (if required) ALLOCATION LENGTH (if required)				
9								(LSB)
10	Reserved							
11	CONTROL							

Table 4 — Typical CDB for 16-byte commands

Bit / Byte	7	6	5	4	3	2	1	0
0	OPERATION CODE							
1	Reserved			SERVICE ACTION (if required)				
2	(MSB)							
3								
4				LOGICAL BLOCK ADDRESS (if required)				
5								(LSB)
6								
7				Additional CDB data (if required)				
8								
9								
10	(MSB)							
11				TRANSFER LENGTH (if required)				
12				PARAMETER LIST LENGTH (if required) ALLOCATION LENGTH (if required)				
13								(LSB)
14	Reserved							
15	CONTROL							

Table 5 — Typical CDB for long LBA 16-byte commands

Bit Byte	7	6	5	4	3	2	1	0
0	OPERATION CODE							
1	Reserved			[5.33]miscellaneous CDB information				
2	(MSB)							
3								
4								
5								
6				[5.33]LOGICAL BLOCK ADDRESS				
7								
8								
9								(LSB)
10	(MSB)							
11				TRANSFER LENGTH (if required)				
12				PARAMETER LIST LENGTH (if required) ALLOCATION LENGTH (if required)				
13								(LSB)
14	Reserved							
15	CONTROL							

4.3.3 The variable length CDB formats

Operation code 7Fh heads a variable length CDB. The CONTROL byte is the second byte in the variable length CDB (see table 6).

Table 6 — Typical variable length CDB

Bit / Byte	7	6	5	4	3	2	1	0
0	OPERATION CODE (7Fh)							
1	CONTROL							
2	Reserved							
3	Reserved							
4	Reserved							
5	~~ENCRYPTION IDENTIFICATION~~ Reserved							
6	Reserved							
7	ADDITIONAL CDB LENGTH (n-7)							
8	(MSB)			SERVICE ACTION				
9								(LSB)
10	Service action specific fields							
n								

~~The contents of the CONTROL field are defined in SAM-2.~~

~~NOTE 1 In all other CDB formats, the control byte is the last byte in the CDB.~~

[1.8]~~The ENCRYPTION IDENTIFICATION field indicates whether CDB bytes 8 through n and/or the data bytes are encrypted. The value also indicates which encryption key to use for decryption. A value of zero indicates no encryption. All other values are reserved.~~

The ADDITIONAL CDB LENGTH field indicates the number of additional CDB bytes. This value in the ADDITIONAL CDB LENGTH field shall be a multiple of 4. [10.21]If the number of CDB bytes delivered by the service delivery subsystem is not sufficient to contain the number of bytes specified by the ADDITIONAL CDB LENGTH field, the command shall be terminated with a CHECK CONDITION status. The sense key shall be set to ILLEGAL REQUEST and the additional sense code shall be set to INVALID FIELD IN CDB.

The SERVICE ACTION field indicates the action being requested by the application client. The SERVICE ACTION field is required in the variable length CDB formats and is described in 4.3.4.2. Each service action code description defines a number of service action specific fields that are needed for that service action.

[1.8]~~If the device server detects an error during decryption of encrypted CDB bytes, it shall return CHECK CONDITION status with an additional sense code of CDB DECRYPTION ERROR. If the device server detects an error during decryption of encrypted data bytes, it shall return CHECK CONDITION status with an additional sense code of DATA DECRYPTION ERROR.~~

[5.27]A 32-byte variable length CDB format is defined for long LBA operations (see table 7).

Table 7 — Typical variable length CDB for long LBA 32-byte commands

Bit Byte	7	6	5	4	3	2	1	0
0	OPERATION CODE (7Fh)							
1	CONTROL							
2	Reserved							
4								
5	~~ENCRYPTION IDENTIFICATION~~ Reserved							
6	Reserved							
7	ADDITIONAL CDB LENGTH (18h)							
8	(MSB)							
9	SERVICE ACTION							(LSB)
10	Reserved			DPO	FUA	Reserved		
11	Reserved							
12	(MSB)							
19	LOGICAL BLOCK ADDRESS							(LSB)
20	Additional CDB data							
27								
28	(MSB)							
31	TRANSFER LENGTH (if required) PARAMETER LIST LENGTH (if required) ALLOCATION LENGTH (if required)							(LSB)

4.3.4 Common CDB fields

4.3.4.1 Operation code

[7.13]The OPERATION CODE field contains the code value identifying the operation being requested by the CDB. SAM-2 defines the general structure of the operation code value. The OPERATION CODE field has a consistently defined meaning across all commands. This standard specifies the operation code values used by the commands defined herein.

4.3.4.2 Service action

All [8.17]~~typical~~ CDB formats except the [8.17]~~typical~~ 6-byte format provide for a SERVICE ACTION field containing a coded value identifying a function to be performed under the more general command function specified in the OPERATION CODE field. While the SERVICE ACTION field is defined for [8.17]~~typical~~ CDB formats, it is used as described in this [5.30]sub clause only in those CDB formats that [5.31]~~explicitly~~ contain a SERVICE ACTION field. When the specific field SERVICE ACTION is not defined in a CDB format, the bits identified as the SERVICE ACTION field in a [8.17]~~typical~~ CDB [1.7]shall be used or reserved as specified by the particular CDB format~~may be used for other purposes~~.

4.3.4.3 Logical block address

The logical block [8.18]addresses on a logical unit ~~address on logical units~~ or within a [8.18]volume partition [8.18]~~on device volumes~~ shall begin with block zero and be contiguous up to the last logical block [8.18]of ~~on~~ that logical unit or within that partition.

A six-byte [5.26]CDB~~command descriptor block~~ contains a 21-bit LOGICAL BLOCK ADDRESS field. [5.33]The ten-byte~~,~~ and the twelve-byte ~~and the sixteen-byte~~ [5.26]CDBs~~command descriptor blocks~~ contain 32-bit LOGICAL BLOCK ADDRESS fields. [5.33]The sixteen-byte CDB has two formats one with a 32-bit LOGICAL BLOCK ADDRESS field (see table 4) and one with a 64-bit LOGICAL BLOCK ADDRESS field (see table 5). LOGICAL BLOCK ADDRESS fields in additional parameter data have their length specified for each occurrence. See the specific command descriptions.

4.3.4.4 Transfer length

The TRANSFER LENGTH field specifies the amount of data to be transferred, usually the number of blocks. [8.20]Some commands use transfer length to specify the requested number of bytes to be sent as defined in the command description. ~~For several commands the transfer length indicates the requested number of bytes to be sent as defined in the command description. For these commands the TRANSFER LENGTH field may be identified by a different name.~~ See the following descriptions and the individual command descriptions for further information.

Commands that use one byte for the TRANSFER LENGTH field allow up to 256 blocks of data to be transferred by one command. A TRANSFER LENGTH value of 1 to 255 indicates the number of blocks that shall be transferred. A value of zero [7.15]specifies that 256 blocks shall be transferred~~indicates 256 blocks~~.

In commands that use multiple bytes for the TRANSFER LENGTH field, a transfer length of zero indicates that no data transfer shall take place. A value of one or greater indicates the number of blocks that shall be transferred.

Refer to the specific command description for further information.

4.3.4.5 Parameter list length

The PARAMETER LIST LENGTH field is used to specify the number of bytes sent from the Data-Out Buffer. This field is typically used in [5.26]CDBs~~command descriptor blocks~~ for parameters that are sent to a device server (e.g., mode parameters, diagnostic parameters, log parameters~~,~~ [5.35]~~etc.~~). A parameter length of zero indicates that no data shall be transferred. This condition shall not be considered as an error.

4.3.4.6 Allocation length

The ALLOCATION LENGTH field specifies the maximum number of bytes that an application client has allocated for returned data. An allocation length of zero indicates that no data shall be transferred. This condition shall not be considered as an error. The device server shall terminate transfers to the Data-In Buffer when allocation length bytes have been transferred or when all available data have been transferred, whichever is less. The allocation length is used to limit the maximum amount of data (e.g., sense data, mode data, log data, diagnostic data~~,~~ [5.34]~~etc.~~) returned to an application client. If the information being transferred to the Data-In Buffer includes fields containing counts of the number of bytes in some or all of the data, the contents of these fields shall not be altered to reflect the truncation, if any, that results from an insufficient ALLOCATION LENGTH value, unless the standard that describes the Data-In Buffer format specifically states otherwise.

If the amount of information to be transferred exceeds the maximum value that may be specified in the ALLOCATION LENGTH field the device server shall transfer no data and return a CHECK CONDITION status; the sense key shall be set to ILLEGAL REQUEST and the additional sense code shall be set to INVALID FIELD IN CDB.

4.3.4.7 Control

[7.13]The contents of the CONTROL field are defined in SAM-2. The CONTROL field has a consistently defined meaning across all commands.