SD Memory Card Specifications

Part 3
SECURITY SPECIFICATION

Version 1.0

February 2000

SD Group

Matsushita Electric Industrial Co., Ltd. (MEI)

SanDisk Corporation

Toshiba Corporation

This page is intentionally left blank

Conditions for publication

Publisher and Copyright Holder

SD Group(MEI, SanDisk, Toshiba)

Confidentiality

This document shall be treated as confidential under the Non Disclosure Agreement which has been signed by the obtainer. Reproduction in whole or in part is prohibited without prior written permission of SD Group.

Exemption

None will be liable for any damages from use of this document.

This page is intentionally left blank

Part 3 SECURITY SPECIFICATION

This page is intentionally left blank

1.General

1.1 Scope

The main objectives of the Security specifications of SD Memory Card are:

- To protect the copyrighted data recorded on the SD Memory Card from unauthorized use (for reproduction and duplication).
- To give independent protection for different pieces of copyrighted data of different applications (electronic music distribution EMD, electronic books, etc.).

This document and *"Content Protection for Recordable Media Specification SD Memory Card Book"*, that is developed by 4C Entity, LLC(IBM,Intel,MEI,Toshiba), contain the information on the functions required of the SD Memory Card to achieve the above objectives.

This document especially contains the security specification that is depending on the implementation of the SD Memory Card, more concretely,

(A) Data Element (SD-Card Specific)
Media Identifier

(B) Security Command set of SD Memory Card

(C) Random Number Generation on SD Memory Card

(D) File system (volume structure) of Protected Area on SD Memory Card

The following technologies are offered by *Content Protection for Recordable Media Specification SD Memory Card: Book:*

- Content and key encryption algorithm (C2 encryption),
- Revocation scheme of the unauthorized accessing device (Media Key Block),
- Authentication and Key Exchange mechanism (AKE) between SD Memory Card and the accessing devices.
- Data Structure on SD Memory Card
- File System (directory and file format) of Protected Area on SD Memory Card
- Content Encryption Format

etc.

1.2 References

4C Entity, LLC, *[Content Protection for Recordable Media Specification SD Memory Card Book, available soon.]*

SD Group, SD Memory Card Specifications Part1: Physical Layer Specifications

SD Group, SD Memory Card Specifications Part2: File System Specifications

2.Data Element

This Section describes the SD Memory Card specific 'data element'.

SD Memory Card non-specific data element is described in *Content Protection for Recordable Media Specification SD Memory Card Book*.

2.1 Media Identifier

SD Memory Card shall contain a 64-bit Media Identifier (ID_{media}), a part of which is unique by each SD Memory Card.

The Media Identifier logical format is shown in Table 2-1. As shown in Table 2-1, the least significant 56-bit(Byte"1" to Byte"7") of the Media Identifier is a SD Memory Card Specific part.

In Table2-1,

- The 4C Entity, LLC assigns each SD Memory Card Manufacturer a unique 1-byte value as the Manufacture ID field. (The detail is defined in *Content Protection for Recordable Media Specification SD Memory Card Book*)
- The SD Group assigns each SD Memory Card Manufacturer a unique 2-byte value as the OEM/Application ID value
- Each SD Memory Card Manufacturer assigns a unique 5-byte value as the Serial Number, which consists of 1-byte Product Revision (PRV) value, and 4-byte Product serial number (PSN) value.

Table 2.1: Media Identifier for SD Memory Card

Bit / Byte	7	6	5	4	3	2	1	0
0	Manufacturer ID (MID:1byte) assigned by 4C Entity, LLC							
1	OEM/Application ID(OID:2byte) assigned by SD Group							
2								
3	Product Revision(PRV:1byte)							
4	Product serial number(PSN:4byte)							
5								
6								
7								

3. Security Command set for copyright protection

3.1 Security Command List

In order to support a new set of commands that will be 'behind' the MULTIMEDIACARD standard, the new commands will be an Application Specific given commands and shall be preceded with CMD55 (APP_CMD). First describes the new set of commands. Note that all the commands do not use RCA (Relative Card Address). Therefor those commands shall be used after the card was selected (in '*tran_state*'). Note that the SD Memory CARD supports only a fix block size of 512 Bytes per block (Sector Size). The Sector Size is able to change by Set_Block_Size command, though it is not executable except for 512 Bytes Sector size because of restriction of ATA.

Table 3.1 Security Command List

CMD INDEX	Type	Argument	Resp	Abbriviation	Command Description
ACMD43	Adtc	[31:24]UNIT_COUNT: [23:16] MKB_ID: [15:0]UNIT_OFFSET:	R1	GET_MKB	Reads Media Key Block from the System Area of SD Memory Card. -'UNIT_COUNT' specifies the Number of units to read. (here, a unit=512 byte (fixed)) - 'MKB_ID' specifies the application unique number. - 'UNIT_OFFSET' specifies the start address(offset) to read.
ACMD44	Adtc	[31:0] stuff bits	R1	GET_MID	Reads Media ID from the System Area of SD Memory Card.
ACMD45	Adtc	[31:0] stuff bits	R1	SET_CER_RN1	AKE Command: Writes random number RN1 as challenge1 in AKE process. (See Note(1)(2))
ACMD46	Adtc	[31:0] stuff bits	R1	GET_CER_RN2	AKE Command: Reads random number RN2 as challenge2 in AKE process. (See Note (1))
ACMD47	Adtc	[31:0] stuff bits	R1	SET_CER_RES2	AKE Command: Writes RES2 as response2 to RN2 in AKE process. (See Note (1))
ACMD48	Adtc	[31:0] stuff bits	R1	GET_CER_RES1	AKE Command: Reads RES1 as response1 to RN1 in AKE process. (See Note (1))

ACMD18	Adtc	[31:0] stuff bits	R1	SECURE_READ_MULTI_BLOCK	Protected Area Access Command: Reads continuously transfer data blocks from Protected Area of SD Memory Card. The (essential) argument of this command as shown below is transferred securely in AKE command(ACMD45) (See Note (2)). - [31:24] 'Unit_Count' specifies the number of blocks to transfer. Block Size is fixed 512bytes. -[23] 'Reserve'.(This value shall be set to '0' for the future extension.) - [22:0] 'UNIT_Address' specifies the start address to read. ([ ] shows bit position of the (essential) argument)

ACMD25	Adtc	[31:0] stuff bits	R1	SECURE_WRITE_MULT_BLOCK	Protected Area Access Command: Writes continuously transfer data blocks to Protected Area of SD Memory Card. (See Note (4)) The (essential) argument of this command as shown below is transferred securely in AKE command(ACMD45) (See Note (2)). - [31:24] 'Unit_Count' specifies the number of blocks to transfer. Block Size is fixed 512bytes. -[23] Mode specifies the following: - Mode=0: This mode shall be used to write a data which should be shared by all applications, such as FAT associated data (e.g. Master boot record, Partition table, FAT directory entry,). -Mode= 1: This mode shall be used to write a data which should be protected from other application such as content associated data(e.g. Title Key, CCI). - [22:0] 'UNIT_Address' specifies the start address to write. ([ ] shows bit position of the (essential) argument)

ACMD38	Ac	[31:0] stuff bits	R1b	SECURE_ERASE	Protected Area Access Command: Erase a specified region of the Protected Area of SD Memory Card. (See Note(4).) The (essential) argument of this command as shown below is transferred securely In AKE command(ACMD45) (See Note (2)). - [31:24] 'Unit_Count' specifies the number of blocks to transfer. Block Size is fixed 512bytes. - [23:0] 'UNIT_Address' specifies the start address to erase. ([ ] shows bit position of the (essential) argument)

ACMD49	Ac	[31:0] stuff bits	R1b	CHANGE_SECURE_AREA	Protected Area Access Command: Change size of the Protected Area. See Note(3). The value of Unit_address [23:0] (discribed bellow) is given in units of MULT*BLOCK_LEN/512-1. Error occurs in the case that the Protected Area size (in Bytes) is set to a value other than multiplies of MULT*BLOCK_LEN. Note that the minimum User Data Area size is MULT*BLOCK_LEN. In that case Unit_address[23:0]=MULT*BLOCK_LEN/512-1. (About MULT*BLOCK_LEN, see chapter5.3 of SD-Card Specifications Part1: Physical Specifications). The (essential) argument of this command as shown below is transferred securely In AKE command(ACMD45) (see Note(2)). - [23:0]'UNIT_Address' The Protected Area follows the User Data Area in such a way that the first unit address (unit=512 byte) of the Protected Area follows the last unit address of the User Data Area and the highest unit address of the Protected Area is the highest unit address of the memory area. Under those conditions, [23:0]'UNIT_Address' is an address, in units of 512byte, of the end of the User Data Area. - [31:24] stuff bits ([ ] shows bit position of the (essential) argument)

ACMD26	Adtc	[31:0] stuff bits	R1	SECURE_WRITE_MKB	Protected Area Access Command: Overwrite the exist Media Key Block(MKB) on the System Area of SD Memory Card with new MKB.(See Note(4)) The (essential) argument of this command as shown below is transferred securely in AKE command (ACMD45) (see Note(2)). -[31:24] 'Unit_Count' specifies the total number of units to be transferred (up to max of 128K bytes). Unit Size is fixed 512bytes. -[23:16] 'MKB_ID' -[15:0] reserved. (This value shall be set to '0' for the future extension.) ([ ] shows bit position of the (essential) argument)

Note:

(1) AKE Commands (ACMD45-48) are always executed in conjunction with either of "Protected Area Access Command" (ACMD18,ACMD25, ACMD26,ACMD38,ACMD49).

(2) In AKE command (ACMD45), challenge1 (random number RN1) is generated by encrypting an (essential) argument of the following "Protected Area Access Command" (shown in Table3.1). SD Memory Card gets the (essential) argument of the following "Protected Area Access Command" by decrypting received challenge1. Regarding the generation method of challenge1, please see 3.2.1 of *Content Protection for Recordable Media Specification SD Memory Card Book*.

(3) Change_Secure_Area command(ACMD49) is restricted to execute as follows:

-The use of this command in end-user application is prohibited.

-The use of this command is allowed only in special authorized applications or devices.
(e.g. manufacturer specific application which is used to make a custom SD-card.)

and the following process shall be executed:

- If the new Protected Area is larger than the former Protected Area, the region of the new Protected Area shall be erased.
- If the new Protected Area is smaller than the former Protected Area, the region of the former Protected Area shall be erased.

(4) It is possible to send ACMD38 (SECURE_ERASE) before

ACMD25(SECURE_WRITE_MULTI_BLOCK) or ACMD26(SECURE_WRITE_MKB) for high-speed purpose.In this case, AKE commands must be done before each secured command (ACMD38, ACMD25, ACMD26) is executed.

(5) The card will send "OUT_OF_RANGE" when the MKB_ID number is bigger than the amount of MKBs saved in the card.

(6) The host shall send the stop transmission command described in the SD-Card Specification Part1 in case that there was an error while Read or Write operation.

(7)In Protected Area Access Command(ACMD18,ACMD25,ACMD38), UNIT_Address starts at "0"(It is not "the top address of User Data Area +1"). And if data accessing is out_of_range, the operation (write,read or erase) will be performed up to the 'end' of range and then indicates 'out_of_range'.

(8) Write Protect Group, Permanent Write Protection and Temp Write Protection(see chapter4.3.5 of SD-Card Specifications Part1:Physical Specifications) do not affect operations on Protected area.

(9) CHANGE_SECURE_AREA command will set WP_VIOLATON flag in Card Status (and change of protected area will not be performed) in case that the card is Permanent Write Protected, Temp Write Protected or if the requested secure area fall into Write Protected Group area.
In case that there is Write Protected area but the new requested Protected Area does not fall into the Write Protected Area then there will not be an error and the new Protected Area shell be defined.

(10) CHANGE_SECURE_AREA command will set LOCK_UNLOCK_FAILED flag in Card Status (and change of protected area will not be performed) in case that the card is LOCKED (with Password). It is always the responsibility of the host to verify successful operation by sending SEND_STATUS (CMD13) command.

(11) As shown in the chapter 3.9.2 of Content Protection for Recordable Media Specification SD Memory Card Book, the data field of Secure_Write_MKB is begun with "Size of MKB" field, followed by "MKB" field , 0 or 4 bytes “0 padding” field, "Kmu" field, 1byte "0 padding" field and "RCC" field.
And to simplify the calculation of RCC, further “0 padding” fields are added in the unit data. Those “0 padding” data has no meaning to RCC value.
Here, in "Size of MKB" field, byte length of MKB shall be stored by big-endian as well as CPRM (which means that byte 0 is a most significant byte).
SECURE_WRITE_MKB data format.

*** 1st unit of 512 bytes contains the following data ***

8 Bytes	Size of MKB (N bytes)
504 Bytes	'0 padding' (*1)

*** A succession of M units of 512 bytes each.(where M is MKB size in units of 512 bytes) ***

N Bytes	MKB data
M * 512 - N Bytes	'0 padding' (*1)

*** (M+2)th unit of 512 bytes data ***

7 Bytes	Kmu
1 Byte	'0 Padding'
8 Bytes	RCC
512 - 16 = 496 Bytes	'0 Padding' (*1)

*** After (M+3)th units are '0 padding' data ***

*1) To simplify the calculation of RCC remaining data in the unit should be "0".

(12) About 'Unit_Count' in the Security R/W/E, GET_MKB and SECURE_WRITE_MKB.

'Unit_Count=0' means 256 units.

3.2 Usage of Security command

Regarding the usage of Security command, please refer to the chapter 3.3 of *Content Protection for Recordable Media Specification SD Memory Card Book*.

3.3 SD Memory Card State Diagram on Authentication

Figure 3.1 shows the SD Memory Card State Diagram on Authentication.

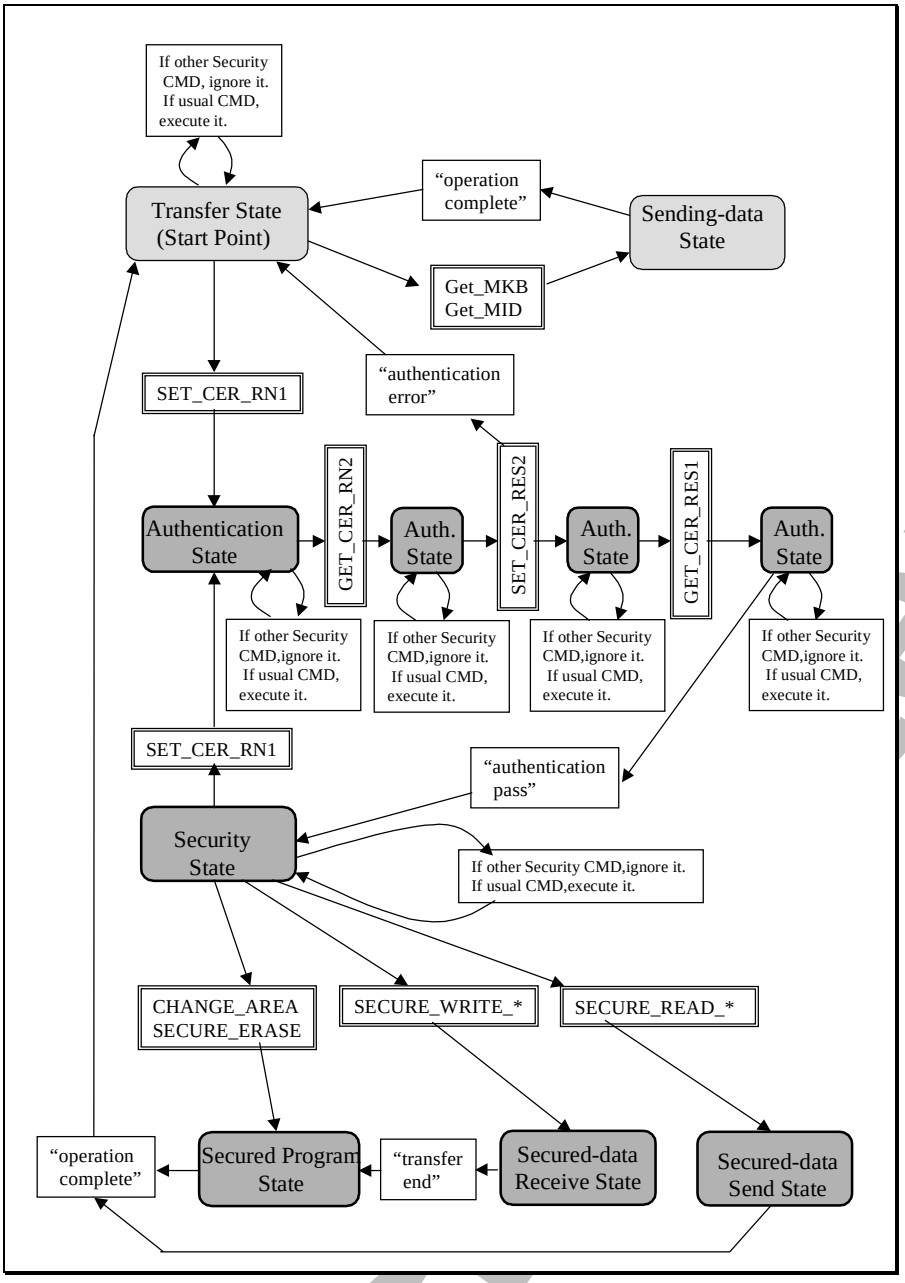


Figure 3.1 State Diagram

4. Random Number Generation(RNG)

In AKE process, SD Memory Card and the accessing device can use the following random number generation scheme. In this scheme, each licensee assigns two 56-bit random numbers as Random Number Key (RNK) pair (c_1, c_2) and pre-stores (c_1, c_2) on Hidden Area of SD Memory Card.

(1) Seed Generation

The 64-bit seed v_t is kept secret in RAM. More concretely, it shall be diffcult to access the seed v_t from outside of SD Memory Card.

The Media Unique Key (56-bit) is used for 56-bit(lsb) of the initial seed v_0 and 8-bit "0" is concatenated as the 8-bit(msb) of the initial seed v_0 when the Card is manufactured. Before shipment, the circuit of RNG freely runs. This makes temporary seed different from K_{mu}.

When the first AKE process is executed after the power of SD Memory Card is turned ON, the seed v_t stored in flash memory is transferred as a temporary seed to RAM. After that, the 64-bit seed (v_t) and 56-bit RNK (c_1) are input to C2 One-way function(C2_G), and 64-bit output (v_{t+1}) of C2_G is stored in flash memory as a next seed (v_{t+1}). Fig. 4.1 shows the procedure of seed generation.

Seed generation is executed only when the first AKE process is executed after the power of SD Memory Card is turned ON.

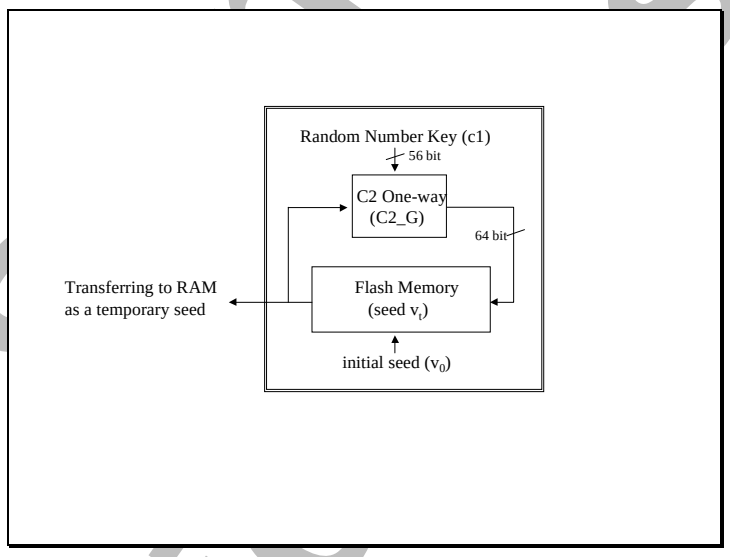


Figure 4.1 Seed Generation

(2) Random Number Generation:

When the first AKE process is executed after the power of SD Memory Card is turned ON, RAM receives the seed from flash memory as a temporary seed (r_{i-1}). After that, the 64-bit temporary seed (r_{i-1}) and 56-bit RNK (c_2) are input to C2 One-way function(C2_G), and 64-bit output (r_i) of C2_G is used as a 64-bit random number and stored in RAM as a next temporary seed(r_i).

Next, Random Number Generation is executed using new temporary seed (r_i). This process is executed repeatedly until the power of SD Memory Card is turned OFF. Fig. 4.2 shows the procedure of random number generation.

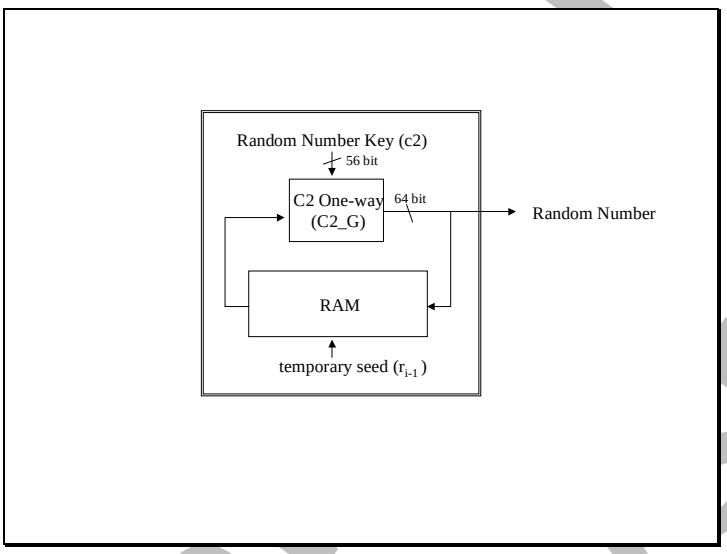


Figure 4.2 Random Number Generation

5. File System

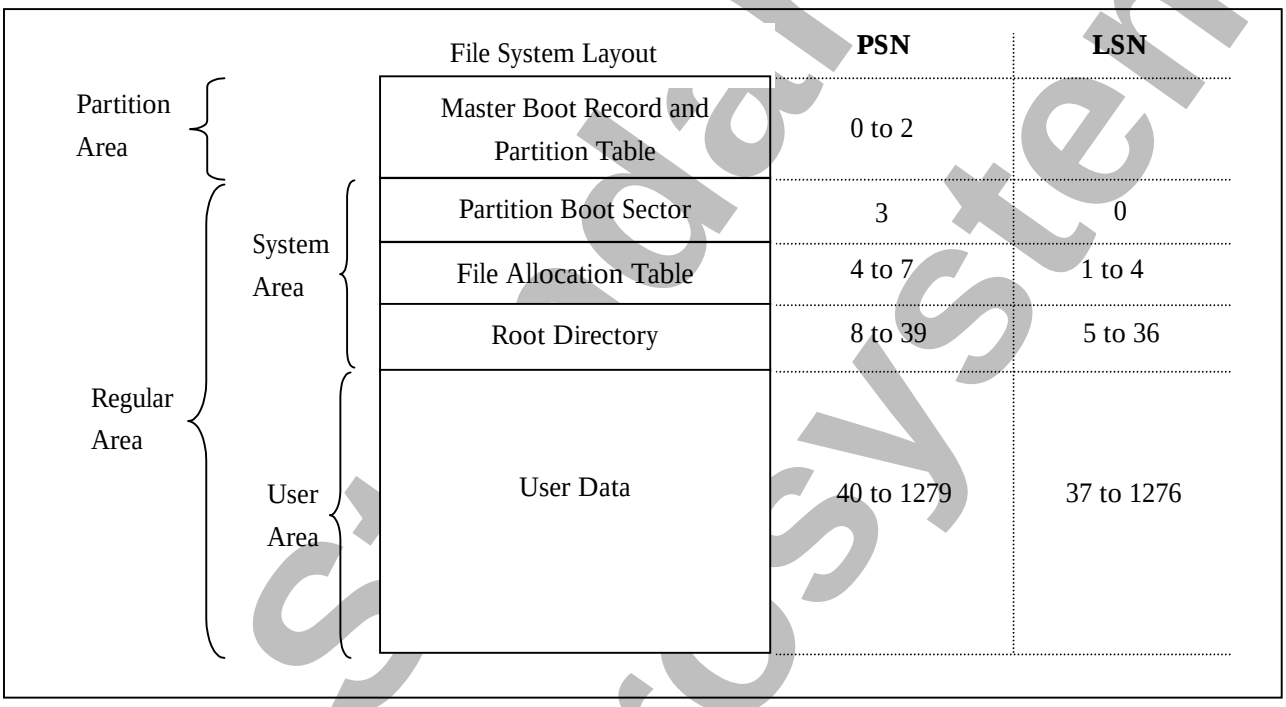
5.1 General

This section defines volume structure regarding Protected Area in SD Memory Card. As well as User Data Area, File System in Protected Area uses ISO/IEC 9293-compliant FAT file system. Furthermore, following is a major point that File System in Protected Area differs from one in User Data Area (defined in SD-Card Specifications Part2: File System Specifications):

- Cluster size of Protected Are is not necessarily a multiple of SD Memory Card erase block size.
- Since it does not require high-speed write for Protected Area, the starting address of User Data is not necessarily located on the boundary of SD Memory Card erase block.

Figure 5.1 shows the example of volume structure for Protected Area.

◊ **Figure 5.1 : Example of Volume Structure for Protected Area**



PSN : Physical Sector Number

LSN : Logical Sector Number

5.2 Master Boot Record and Partition Table

See SD Memory Card Specifications Part2: File System Specifications as reference since this Master Boot Record and Partition Table are defined in the same way as Master Boot Record and Partition Table in Data Area.

5.3 Partition Boot Sector

Since each field in Partition Boot Sector is almost the same as the one in Partition Boot Sector of Data Area, see SD-Card Specifications Part2: File System Specifications as reference. Fields that differ from the ones described in Specifications above mentioned are explained as follows:

(BP13) Sectors per Cluster

This field shall specify the number of sectors per cluster. It shall be recorded the following number: 1, 2, 4, 8, 16, 32 or 64.

5.4 File Allocation Table

See SD-Card Specifications Part2: File System Specifications as reference since this File Allocation Table is defined in the same way as File Allocation Table in User Data Area.

5.5 Root Directory

See SD-Card Specifications Part2: File System Specifications as reference since this Root Directory is defined in the same way as Root Directory in User Data Area.

5.6 User Data

The minimum read/write access size is defined in the units of Sector.

Annex

A Test command Requirement

Each SD Memory card manufacturer can individually define the new test command for setting up and testing or analyzing the devices in SD card. But such defined new test command must comply the following security requirement. CMD60,61,62,63 is reserved for manufacturer for test purpose.

Requirement:

(1) cannot read nor update the data stored in a Hidden Area

(2) cannot update the data stored in a System Area

(3) cannot read nor update the data stored in a Protected Area without successful authentication.

B Sectors per Cluster and Boundary Unit Recommendation for Protected Area

The following table shows the recommendation for Sectors per Cluster and Boundary Unit of Protected Area.

◊ **Table B-1 Sectors per Cluster and Boundary Unit Recommendation (Protected Area)**

Protected Area size	Sectors per Cluster	Boundary Unit
~256KB	1	1
~1MB	2	2
~4MB	8	8
~1024MB	32	32
~2048MB	64	64

NOTE: The Table B-1 is not based on the Card Capacity.

Minimum Protected Area size and format parameters for Protected Area are shown in following table.

◊ **Table B-2 Minimum Protected Area size and format parameters**

Card Capacity	Min Protected Area size(sector)	Sectors per Cluster	an example(values depend on Protected Area size)				
			Clusters	FAT Sec	Hidden	FAT bits	User Data Offset
~4MB	160	1	124	1	1	12	36
~8MB	160	1	124	1	1	12	36
~16MB	320	1	284	1	1	12	36
~32MB	640	2	301	1	3	12	38
~64MB	1280	2	620	2	3	12	40
~128MB	2560	8	314	1	13	12	48
~256MB	5120	8	634	2	11	12	48
~512MB	10240	32	317	1	61	12	96
~1024MB	20480	32	637	2	59	12	96
~2048MB	40960	32	1277	4	55	12	96

However,

Card Capacity…SD Card Capacity.

Min Protected Area size…minimum number of sectors for Protected Area. This parameter is defined from the Card Capacity, using Table B-2.

Sectors per Cluster…number of sectors per cluster. This parameter is defined from the Protected Area size, using Table B-1.

Clusters…number of clusters in User Data. This parameter varies with the Protected Area size.

FAT Sec…number of sectors per FAT. This parameter varies with the Protected Area size.

Hidden…number of sectors existing before Partition Boot Sector. This parameter varies with the Protected Area size.

FAT bits…If the area is formatted with FAT12, FAT bits is 12. And If the area is formatted with FAT16, FAT bits is 16. This parameter varies with the Protected Area size.

User Data Offset…number of sectors existing before the starting sector of User Data.
Sectors per Cluster is defined from the Protected Area size. Clusters, FAT Sec, Hidden, FAT bits, and User Data Offset vary with the Protected Area size (Use the parameters in Table B-1 for calculation).

C Type of 16 MKBs on SD Memory Card

This annex shows the type of 16 MKBs pre-stored in the SD Memory Card. As shown in Table C-1, first eight MKBs (MKB "#0" to MKB "#7") are read-only and not updateable by the "dynamic MKB update scheme". Here, the "dynamic MKB update scheme" is described in Chapter 3.9 of *Content Protection for Recordable Media Specification SD Memory Card Book*. Next seven MKBs (MKB "#8" to MKB "#14") are updateable MKB by using the "dynamic MKB update scheme". A last MKB (MKB "#15") is a master MKB which is used in a special authorized accessing device (e.g., a Kiosk), which is allowed to execute the "dynamic MKB update scheme". MKB "#0" is used in SD-Audio application. MKB "#1" to MKB "#14" are reserved for other applications. Application which uses reserved MKB (MKB "#1" to MKB "#14") is added in the future.

◊ **Table C-1 Type of 16MKBs**

Number of MKB	Type	Application
MKB0	Read only	SD-Audio
MKB 1	Read only	Reserved
MKB 2	Read only	Reserved
MKB 3	Read only	Reserved
MKB 4	Read only	Reserved
MKB 5	Read only	Reserved
MKB 6	Read only	Reserved
MKB 7	Read only	Reserved
MKB 8	Updateable	Reserved
MKB 9	Updateable	Reserved
MKB 10	Updateable	Reserved
MKB 11	Updateable	Reserved
MKB 12	Updateable	Reserved
MKB 13	Updateable	Reserved
MKB 14	Updateable	Reserved
MKB 15	Master	Reserved