

SD Specifications

Part 3

Security Specification

Version 3.00

June 12, 2009

SD Group

Panasonic Corporation
SanDisk Corporation
Toshiba Corporation

SD Card Association

CONFIDENTIAL

Revision History

Date	Version	Changes compared to previous issue
March 22, 2000	1.0	Base Version
April 15, 2001	1.01	- The Supplementary Note (May 2000) for "SD Memory Card Specifications Part 3 Security Specification Version 1.0 (March 2000)" was incorporated into the spec. - MKB Supplementary Notes 1 (May 2000) for "SD Memory Card Specifications Part 3 Security Specification Version 1.0 (March 2000)" was incorporated into the spec. - Typing error fixes and some clarification notes
June 7, 2006	2.00	- The Supplementary Note (April 2001) for "SD Memory Card Specifications Part 3 Security Specification Version 1.01 (April 2001)" was incorporated into the spec. - Description for High Capacity SD Memory Card, which is defined in both "SD Specifications Part 1 Physical Layer Specification Version 2.00 (December 2005)" and "SD Specifications Part2 File System Specification Version 2.00 (December 2005)", was added.
June 12, 2009	3.00	- The Supplementary Notes (March 2008) for "SD Memory Card Specification Part 3 Security Specification Version 2.00 (June 2006)" was incorporated into the spec. - Bit 502-509 in SD Status is reserved for security function, and description on bit assignments within that field is added as chapter 3. - Description for Extended Capacity SD Memory Card, which is defined in both "SD Specifications Part 1 Physical Layer Specification Version 3.00" and "SD Specifications Part2 File System Specification Version 3.00", is added. - Clarification on CPRM implementation. - Typing error fixes and cosmetic changes

To the extent this proposed specification, which is being submitted for review under the IP Policy, implements, incorporates by reference or refers to any portion of versions 1.0 or 1.01 of the SD Specifications (including Parts 1 through 4), adoption of the proposed specification shall require Members utilizing the adopted specification to obtain the appropriate licenses from the SD-3C, LLC, as required for the utilization of those portion(s) of versions 1.0 or 1.01 of the SD Specifications.
For example, implementation of the SD Specifications in a host device under versions 1.0 or 1.01 and under the adopted specification requires the execution of a SD Host Ancillary License Agreement with the SD-3C, LLC; and implementation of the SD Specifications under versions 1.0 or 1.01 and under the proposed specification in a SD Card containing any memory storage capability (other than for storage of executable code for a controller or microprocessor within the SD Card) requires the execution of a SD Memory Card License Agreement with the SD-3C, LLC.

Conditions for publication

Publisher:
SD Card Association
2400 Camino Ramon, Suite 375
San Ramon, CA 94583 USA
Telephone: +1 (925) 275-6615,
Fax: +1 (925) 886-4870
E-mail: office@sdcard.org

Conventions Used in This Document

Naming Conventions

- Some terms are capitalized to distinguish their definition from their common English meaning. Words not capitalized have their common English meaning.

Numbers and Number Bases

- Hexadecimal numbers are written with a lower case "h" suffix, e.g., FFFFh and 80h.
- Binary numbers are written with a lower case "b" suffix (e.g., 10b).
- Binary numbers larger than four digits are written with a space dividing each group of four digits, as in 1000 0101 0010b.
- All other numbers are decimal.

Key Words

- May: Indicates flexibility of choice with no implied recommendation or requirement.
- Shall: Indicates a mandatory requirement. Designers shall implement such mandatory requirements to ensure interchangeability and to claim conformance with the specification.
- Should: Indicates a strong recommendation but not a mandatory requirement. Designers should give strong consideration to such recommendations, but there is still a choice in implementation.

Application Notes

Some sections of this document provide guidance to the host implementers as follows:

Application Note: This is an example of an application note.

Table of Contents

Table of Figures

Table of Tables

1. General

1.1. Scope

The main objectives of the Security specification of SD Memory Card are:
- To protect the copyrighted content data recorded on the SD Memory Card from unauthorized use (for reproduction and duplication).
- To give independent protection for different pieces of data of different applications (audio, video, picture, document, PIM, etc.).

To achieve the above objectives, this version of the Security specification supports the following security function.
- Content Protection technology specified in *"Content Protection for Recordable Media (CPRM) Specification SD Memory Card Book"*, which is developed by 4C Entity, LLC (IBM, Intel, Panasonic and Toshiba).

This document especially contains the security specification that is dependent on the implementation of the SD Memory Card.

For the detailed schemes and protocols of CPRM, see each specification book referred in 1.2.

1.2. References

[1] 4C Entity, LLC, Content Protection for Recordable Media Specification SD Memory Card Book.
[2] SD-3C, LLC, SD Specifications Part1: Physical Layer Specification
[3] SD-3C, LLC, SD Specifications Part2: File System Specification

(Notes)
- SD-3C, LLC is a limited liability company established by Panasonic Corporation, SanDisk Corporation and Toshiba Corporation.
SD-3C, LLC licenses companies that wish to manufacture and/or sell SD Memory Cards, including but not limited to flash memory, ROM, OTP, RAM, and SDIO Combo Cards.

- 4C Entity, LLC is a limited liability company established by Intel Corporation, International Business Machines Corporation, Panasonic Corporation and Toshiba Corporation.

2. Security Specification for CPRM

This chapter describes the SD Security Specification for CPRM.

2.1. Data Element

This Section describes the SD Memory Card specific Data Element for CPRM.
SD Memory Card non-specific CPRM Data Element is described in *Content Protection for Recordable Media Specification SD Memory Card Book*.

2.1.1. Media Identifier

SD Memory Card that supports CPRM shall contain a 64-bit Media Identifier unique to 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 an SD Memory Card Specific part.

In Table 2-1,

- The 4C Entity, LLC or its designated agent assigns each SD Memory Card Manufacturer a unique 1-byte value as the Manufacturer ID field. (The detail is defined in Content Protection for Recordable Media Specification SD Memory Card Book)
- The SD-3C, LLC 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 SerialNumber, 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-3C, LLC							
2								
3	Product Revision (PRV: 1byte)							
4	Product serial number (PSN: 4byte)							
5								
6								
7								

2.2. Security Command set

2.2.1. Security Command List

In order to support these Security Commands that are 'behind' the MultiMediaCard standard, Security Commands will be Application Specific command and shall be preceded with APP_CMD (CMD55).
Note that all the Security Commands do not use RCA (Relative Card Address). Therefore those commands shall be used after the card was selected (in '*tran_state*').

The block size of the Security Commands is of fixed length regardless of the block size for User Area which is set by CMD16.

- ACMD44, ACMD45, ACMD46, ACMD47 and ACMD48 are 8 bytes.
- ACMD43, ACMD18, ACMD25, ACMD38 and ACMD26 are 512 bytes

When the block size is set less than 512 bytes, upper command's (ACMD43, ACMD18, ACMD25, ACMD38 and ACMD26) block size may be influenced by its value. Host shall not set block sizes other than 512 bytes before Security Command execution.

Note that if the card is locked, none of the Security Commands can be used and the card returns no response.
Definition of 'stuff bit' in Table 2-2 is the same as SD Specifications Part1: Physical Layer Specification.
Abbreviations in 'Resp' column are the same as SD Specifications Part1: Physical Layer Specification.

Table 2-2 : Security Command List

CMD INDEX	Type	Argument	Resp	Abbreviation	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's unique number. - 'Unit_Offset' specifies the start address(offset) to read. (See Note (12)(13))
ACMD44	adtc	[31:0] stuff bits	R1	GET_MID	Reads Media ID from the System Area of SD Memory Card. (See Note (12))
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)(15))

CMD INDEX	Type	Argument	Resp	Abbreviation	Command Description
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. (See Note (7)(13)(16)) 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] 'Reserved'.(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)

CMD INDEX	Type	Argument	Resp	Abbreviation	Command Description
ACMD25	adtc	[31:0] stuff bits	R1	SECURE_WRITE_MULTI_BLOCK	Protected Area Access Command: Writes continuously transfer data blocks to Protected Area of SD Memory Card. (See Note (4)(7)(16)) 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, File Allocation Table and Root Directory). - 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)

CMD INDEX	Type	Argument	Resp	Abbreviation	Command Description
ACMD38	ac	[31:0] stuff bits	R1b	SECURE_ERASE	Protected Area Access Command: Erases a specified region of the Protected Area of SD Memory Card. (See Note (4)(7)) 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 erase. Block Size is fixed 512bytes. - [23:0] 'Unit_Address' specifies the start address to erase. ([ ] shows bit position of the (essential) argument)

CMD INDEX	Type	Argument	Resp	Abbreviation	Command Description
ACMD49	ac	[31:0] stuff bits	R1b	CHANGE_SECURE_AREA	Protected Area Access Command: Changes size of the Protected Area. (See Note (3)(9)(14)(15)(18)) 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 Specifications Part1: Physical Specification). 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)

CMD INDEX	Type	Argument	Resp	Abbreviation	Command Description
ACMD26	adtc	[31:0] stuff bits	R1	SECURE_WRITE_MKB	System Area Access Command: Overwrite the existing Media Key Block (MKB) on the System Area of SD Memory Card with new MKB. This command is used in “dynamic update MKB scheme”. (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)

Notes:

(1) AKE Commands (ACMD45-48) are always executed in conjunction with one of the “Protected Area Access Commands” (ACMD18, ACMD25, ACMD26, ACMD38, and 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 Table 2-2). 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 (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 Memory Card.) and the following process shall be executed automatically by SD Memory Card itself:
- 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 SECURE_ERASE (ACMD38) before SECURE_WRITE_MULTI_BLOCK (ACMD25) for high-speed purpose. In this case, AKE commands shall be done before each Protected Area Access command (ACMD38, ACMD25) is executed.

(5) The card shall send “OUT_OF_RANGE” error 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 Specifications Part1: Physical Layer Specification, in case that there was an error while Read or Write operation.

(7) In Protected Area Access Commands (ACMD18, ACMD25, ACMD38), Unit_Address starts at “0”. And if data being accessed 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 Temporary Write Protection (see section 4.3.6 and 4.11 of SD Specifications Part1: Physical Layer Specification) do not affect operations on Protected Area.

(9) CHANGE_SECURE_AREA (ACMD49) will set “WP_VIOLATON” error flag in Card Status (and this command will not be performed), in case that the card is Permanent Write Protected, Temporary Write Protected or if the requested Protected 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 shall be defined.

(10) 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 (ACMD26) begins 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.

To simplify the calculation of RCC, further '0 padding' fields are added in the unit data. Those '0 padding' data have no meaning to RCC value. And it is allowed to send extended units after the last unit (that contains the RCC). In this case the content of the extended units shall be all “0”.

Here, in “Size of MKB” field, byte length of MKB shall be stored by big-endian as well as *Content Protection for Recordable Media Specification Introduction and Common Cryptographic Elements* (which means that byte 0 is a most significant byte).

Following is SECURE_WRITE_MKB (ACMD26) data format and a drawing of explanation of the 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. (M is MKB size in units of 512 bytes) ***
N Bytes MKB data
(M * 512 - N) Bytes '0 padding' (*1)
((M * 512 - N) Bytes should be less than 512 bytes.)
*** (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”.

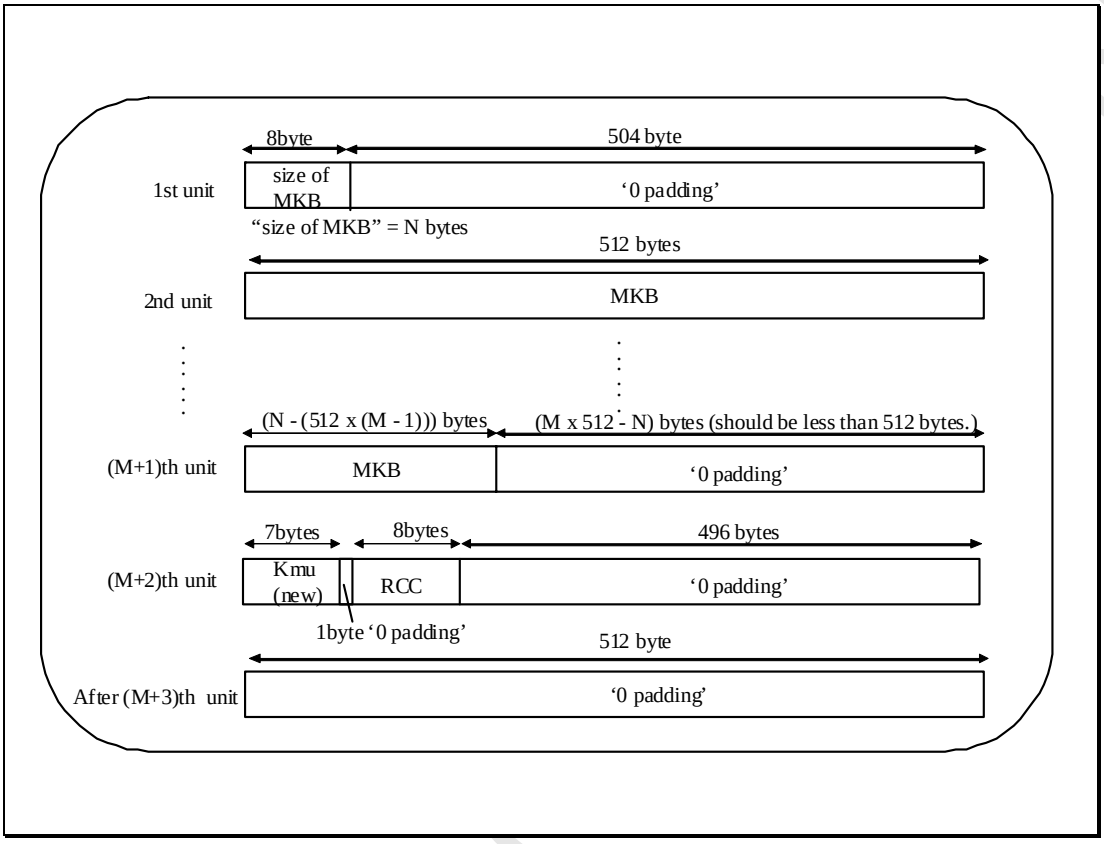


Figure 2-1 : SECURE_WRITE_MKB data format

(11) About 'Unit_Count' in the Security Read/Write/Erase, GET_MKB (ACMD43) and SECURE_WRITE_MKB (ACMD26), 'Unit_Count'=0 means 256 units.

(12) After GO_IDLE_STATE (CMD0), GET_MKB (ACMD43) and GET_MID (ACMD44) are required before the next authentication process.

(13) Wait time after GET_MKB (ACMD43) / SECURE_READ_MULTI_BLOCK (ACMD18):
Those commands implement read operation with Stop Transmission by the card. Since there is no Busy indication for Reading, the following procedures shall be done by the host before continuing next command:
In SD mode: Confirm 'tran_state' or Wait 100us
In SPI mode: Wait 100us

(14) The host's time out after CHANGE_SECURE_AREA (ACMD49) shall consider the associated Erase operation (described in Note (3)), one block Read operation and two times Sector Write operation.

(15) After AKE sequence, the host is required to confirm AKE result by using SD_STATUS (ACMD13). (Especially in SPI mode, AKE_SEQ_ERROR error does not appear.) After CHANGE_SECURE_AREA (ACMD49) execution, confirm user area size by reading CSD register and confirm Protected Area size by reading SD status. And initialize user and Protected Area.

(16) The Secure Write Mode and MKB_ID :
The host can't read the right data that was written by SECURE_WRITE_MULTI_BLOCK (ACMD25) with another MKB ID and Mode=1. In this case the data from the card is all '0' or '1' data that is specified as a DATA_STAT_AFTER_ERASE in SCR register.

(17) The ACMD46 (GET_CER_RN2) is a special READ command and timeout value of this command is same as that of WRITE one. This command's timeout value is possible to define as 250ms maximum.

(18) The ACMD49 (CHANGE_SECURE_AREA) is not supported in either High Capacity SD Memory Card (capacity is over 2GB) or Extended Capacity SD Memory Card (capacity is over 32GB). In this case, reception of ACMD49 indicates ILLEGAL_COMMAND in the Card Status.

2.2.2. Usage of Security Command

Regarding the usage of Security Command, please refer to the chapter 3.4 of Content Protection for Recordable Media Specification SD Memory Card Book Common Part.

2.2.3. SD Memory Card State Diagram on Authentication for CPRM

Figure 2-2 shows the SD Memory Card State Diagram on Authentication for CPRM.

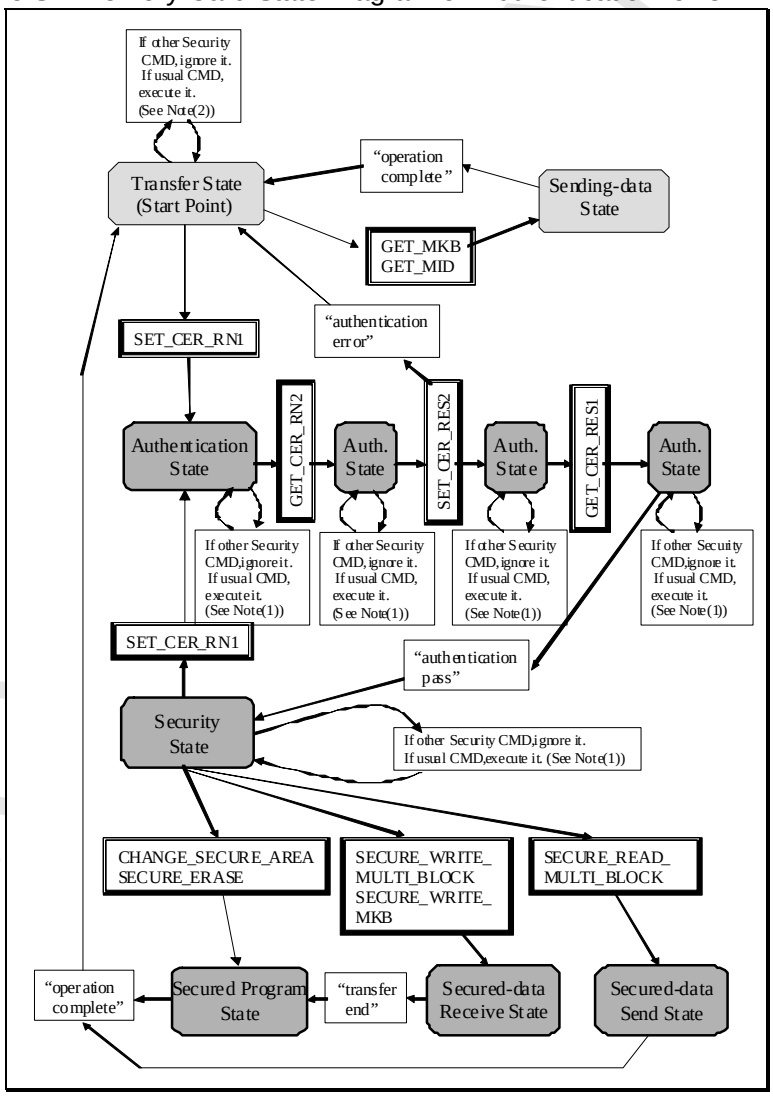


Figure 2-2 : State Diagram for CPRM

2.2.4. Summarization of Error Responses

Table 2-3 summarizes the error responses while executing each Security Command specified in 2.2.1. The error Type, Value and Clear condition are described in SD Specifications Part1: Physical Layer Specification.

Table 2-3 : Error responses List

CMD index	Abbreviation	Error	Description
ACMD18	SECURE_READ_MULTI_BLOCK	OUT_OF_RANGE	Address over.
		CARD_ECC_FAILED	Card internal ECC is applied and it fails to correct the data.
		ERROR	A general or an unknown error occurred during the operation.
ACMD25	SECURE_WRITE_MULTI_BLOCK	OUT_OF_RANGE	Address over.
		ERROR	A general or an unknown error occurred during the operation.
ACMD26	SECURE_ WRITE_MKB	OUT_OF_RANGE	Address over.
		ERROR	A general or an unknown error occurred during the operation.
ACMD38	SECURE_ ERASE	OUT_OF_RANGE	Address over.
		ERROR	A general or an unknown error occurred during the operation.
ACMD43	GET_MKB	OUT_OF_RANGE	MKB_ID over / Unit_Count over / Unit_Offset over
		CARD_ECC_FAILED	Card internal ECC is applied and it fails to correct the data.
		ERROR	Issued in secured mode. A general or an unknown error occurred during the operation.
ACMD44	GET_MID	CARD_ECC_FAILED	Card internal ECC is applied and it fails to correct the data.
		ERROR	A general or an unknown error occurred during the operation.
ACMD45	SET_CER_RN1	-	There is no error.
ACMD46	GET_CER_RN2	ERROR	In case of unsuccessful save of the Random number in the Flash.
ACMD47	SET_CER_RES2	-	There is no error.
ACMD48	GET_CER_RES1	AKE_SEQ_ERROR	Error in the sequence of authentication process (SD mode only) In SPI mode, AKE_SEQ_ERROR error is not appeared. So the host shall make sure whether AKE process is completed or not by using ACMD13
ACMD49	CHANGE_SECURE_AREA	OUT_OF_RANGE	Address over.
		WP_VIOLATION	In case that the card is Permanent Write Protected, Temp Write Protected or if requested Protected Area fall into Write Protected Group area.
		ERROR	A general or an unknown error occurred during the operation.
		ILLEGAL_COMMAND	In case that the card capacity is over 2GB, this command is not supported.

2.3. Random Number Generation (RNG)

2.3.1. Random Number Generation

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.

2.3.1.1. Seed Generation

The 64-bit seed v_t is kept secret in RAM. More concretely, it shall be difficult 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}). Figure 2-3 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.

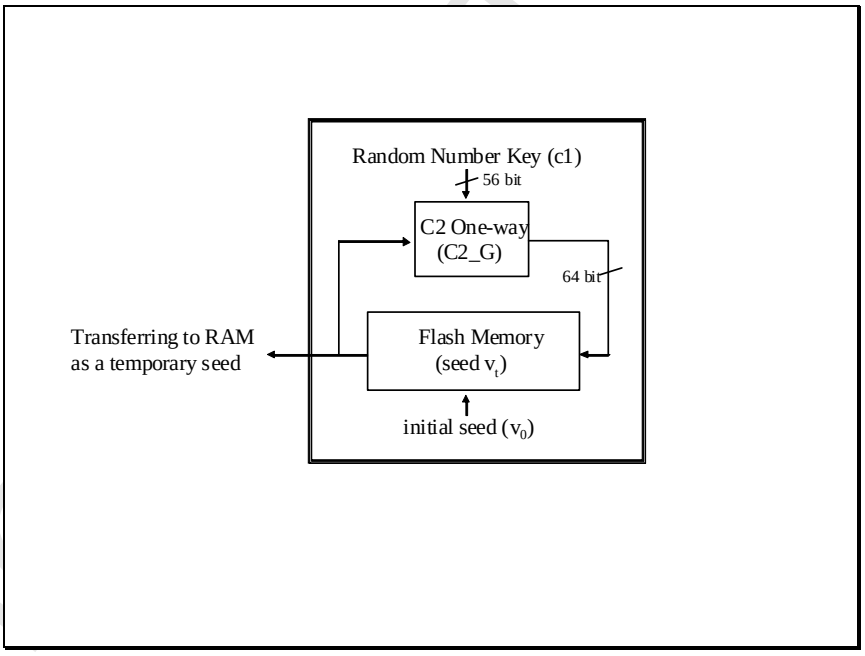


Figure 2-3 : Seed Generation

2.3.1.2. 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. Figure 2-4 : Random Number Generation shows the procedure of random number generation.

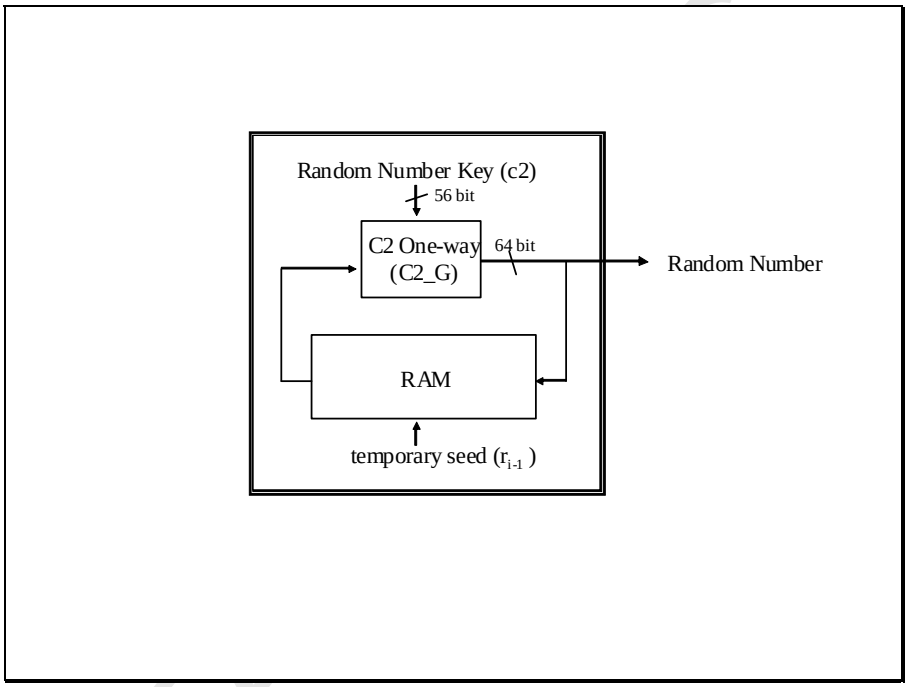


Figure 2-4 : Random Number Generation

3. Bit Assignment for Security Proprietary Field

From Bit 502 to Bit 509 in SD Status is reserved for security functions. Table 3-1 shows a bit assignment for that field. The same abbreviations for 'type' and 'clear condition' are used as SD Specifications Part1: Physical Layer Specification.

Table 3-1 : Bit Assignment for Security Proprietary Field in SD Status

Bit	Identifier	Type	Value	Description	Clear Condition
509	SECURED_MODE	SR	'0'= Not in the mode '1'= In Secured Mode	Card is in Secured Mode of operation.	A
508	Reserved for future use (shall be set to 0)				
507					
506					
505					
504	Reserved				
503	Reserved				
502	Reserved				

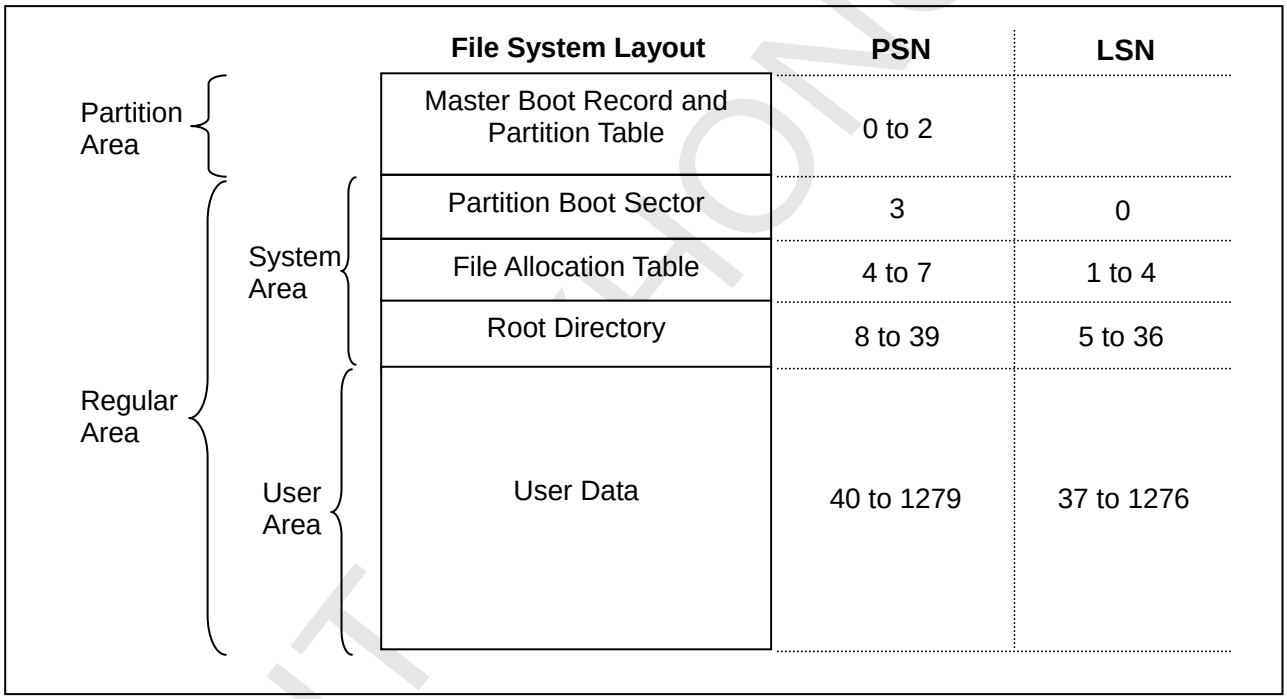
4. File System

4.1. General

This section defines volume structure regarding Protected Area in SD Memory Card. The File System in Protected Area shall use ISO/IEC 9293-compliant FAT file system (FAT12 / FAT16 file system) for all SD Memory Cards up to 2TB. This ISO/IEC 9293-compliant FAT file system is almost the same as the FAT12 / FAT16 file system defined in SD Specifications Part2: File System Specification. The major points of the differences between them are as follows:

- The recommended cluster size of Protected Area differs from the recommendation of User Data Area.
- The recommended boundary unit of Protected Area differs from the recommendation of User Data Area.

Figure 4-1 shows the example of volume structure for Protected Area.



PSN : Physical Sector Number

LSN : Logical Sector Number

Figure 4-1 : Example of Volume Structure for Protected Area

4.2. Master Boot Record and Partition Table

See SD Specifications Part2: File System Specification as reference since this Master Boot Record and Partition Table are defined in the same way as Master Boot Record and Partition Table of FAT12 / FAT16 file system in User Data Area.

4.3. Partition Boot Sector

Since each field in Partition Boot Sector is almost the same as the one in Partition Boot Sector of FAT12 / FAT16 file system in User Data Area, see SD Specifications Part2: File System Specification as reference. Fields that differ from the ones described in Specification above mentioned are explained as follows:

(BP13) Sectors per Cluster

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

4.4. File Allocation Table

See SD Specifications Part2: File System Specification as reference since this File Allocation Table is defined in the same way as File Allocation Table of FAT12 / FAT16 file system in User Data Area.

4.5. Root Directory

See SD Specifications Part2: File System Specification as reference since this Root Directory is defined in the same way as Root Directory of FAT12 / FAT16 file system in User Data Area.

4.6. User Data

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

5. Restrictions Depend on Card Type

5.1. Restrictions in ROM Card

Security function defined by the Part 3 Specification is optional for ROM Card. If the security is not supported, SD_SECURITY in SCR is set to 0 and all security commands are treated as illegal commands.

If the security is supported, SD_SECURITY in SCR is set to 2 for Standard Capacity and 3 for High Capacity. Table 5-1 shows security commands support in ROM card. Not supported commands are treated as illegal command.

It is important note that the random number seed shall be modified in different value by implementation.

Table 5-1 : Security Command Support in ROM Card

	ROM Card
ACMD43	Same as R/W card
ACMD44	Same as R/W card
ACMD45	Same as R/W card
ACMD46	Same as R/W card
ACMD47	Same as R/W card
ACMD48	Same as R/W card
ACMD18	Same as R/W card
ACMD25	Not Supported
ACMD38	Not Supported
ACMD49	Not Supported
AMCD26	Not Supported

Appendix A (Normative) : Reference

A.1 Reference

[1] Part 1 Physical Layer Specification Version 3.00
[2] Part 2 File System Specification Version 3.00
[3] 4C Entity, LLC, Content Protection for Recordable Media Specification SD Memory Card Book.

Appendix B (Normative) : Special Terms

B.1 Abbreviations

4C Entity, LLC	Limited liability company established by Intel Corporation, International Business Machines Corporation, Panasonic Corporation and Toshiba Corporation.
AKE	Authentication Key Exchange
CPRM	Content Protection for Recordable Media
LSN	Logical Sector Number
MKB	Media Key Block
PSN	Physical Sector Number
SD-3C, LLC	Limited liability company established by Panasonic Corporation, SanDisk Corporation and Toshiba Corporation.

Appendix C : 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 an SD Memory Card. But such defined new test command shall comply with the following security requirement. CMD60, 61, 62, 63 are reserved for manufacturer for test purpose.

Requirement:

(1) Can neither read nor update the data stored in a Hidden Area
(2) Can not update the data stored in a System Area
(3) Can neither read nor update the data stored in Protected Areas without succeeding authentication.

Appendix D : Protected Area

D.1 Sectors per Cluster and Boundary Unit Recommendation for Protected Area

Table D- 1 shows the recommendation for Sectors per Cluster and Boundary Unit of Protected Area.

Table D- 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 D- 1 is not based on the Card Capacity.

D.2 Protected Area Size for the Standard Capacity Card

Minimum Protected Area size for the Standard Capacity SD Memory Card, whose capacity is 2GB or less, and an example of format parameters for Protected Area are shown in Table D- 2. The format parameters in this table are examples. They should be calculated with steps described in SD Specifications Part2: File System Specification.

Table D- 2 : Minimum Protected Area size and format parameters

Card Capacity	Min. Protected Area size(sector)	Sectors per Cluster	An example of format parameters (these values vary depending 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

Meanings of parameters used in Table D- 2 is described as follow:

Card Capacity: SD Memory Card Capacity.
Min. Protected Area size: minimum number of sectors for Protected Area. This parameter is defined from the Card Capacity, using Table D- 2.

Sectors per Cluster: number of sectors per cluster. This parameter is defined from the Protected Area size, using Table D- 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 D- 1 for calculation).

D.3 Protected Area Size for the High Capacity Card

The minimum Protected Area size is defined for the Standard Capacity SD Memory Card whose capacity is 2GB or less as described above. For the High Capacity SD memory Card whose capacity is over 2GB and up to 32GB, the Protected Area size is fixed. Other than that, there are no differences between the standard capacity card and the high capacity card.

Table D- 3 shows the Protected Area size and format parameters.

Table D- 3 : Protected Area size and format parameters for High Capacity Card

Card Capacity	Protected Area size (sector)	Sectors per Cluster	Format parameters				
			Clusters	FAT Sec	Hidden	FAT bits	User Data Offset
Over 2048MB ~4096MB	65536	32	2045	6	51	12	96
~8192MB	98304	32	3069	9	45	12	96
~16384MB	131072	32	4092	16	63	16	128
~32768MB	163840	32	5116	20	55	16	128

D.4 Protected Area Size for the Extended Capacity Card

For the Extended Capacity SD memory Card whose capacity is over 32GB and up to 2TB, the Protected Area size is fixed as shown in Table D- 4.

Table D- 4 : Protected Area size and format parameters for Extended Capacity Card

Card Capacity	Protected Area size (sector)	Sectors per Cluster	Format parameters				
			Clusters	FAT Sec	Hidden	FAT bits	User Data Offset
Over 32768MB ~ 2097152MB	262144	32	8187	32	63	16	160

Appendix E : MKB

E.1 Type of 16 MKBs for CPRM on SD Memory Card

This annex shows the type of 16 MKBs for CPRM which are pre-stored in the SD Memory Card. As shown in Table E- 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 “#8” is assigned for Audio related applications, including such as SD-Audio Extension, which is defined in SD Specifications- Part4: Audio Specification MOVE, MIGRATE AND PREVIEW EXTENSION (from 1.0 to 1.1) and *Content Protection for Recordable Media Specification SD Memory Card Book* Appendix A Move Extension and Appendix C Preview Extension. MKB “#9” is assigned for Visual related application, including such as SD-Video application. MKB “#10” is assigned for Document related applications, including such as SD-ePublish applications. MKB “#11” is assigned for SD-Binding applications. MKB “#1” to MKB “#7” and MKB “#13”, MKB “#14” are reserved for other applications. Applications that use reserved MKB (MKB “#1” to MKB “#7” and MKB “#13”, “#14”) will be assigned in the future.

MKB numbers may be shared with several applications within same types of content. The other applications may be assigned at MKB #8, #9, #10, #11 and #12 in the future.

Table E- 1 : Type of 16 CPRM MKBs

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	Audio related applications (such as SD-Audio Extension)
MKB 9	Updateable	Visual related applications (such as SD-Video)
MKB 10	Updateable	Document related applications (such as SD-ePublish)
MKB 11	Updateable	SD-Binding
MKB 12	Updateable	Separate Delivery
MKB 13	Updateable	Reserved
MKB 14	Updateable	Reserved
MKB 15	Master	For “dynamic MKB update scheme”

Appendix F : Implementation of CPRM

Implementation of CPRM is mandatory for every type of SD Memory Card except ROM and OTP card.