Content Protection for Recordable Media Specification

SD Memory Card Book Common Part

Intel Corporation

International Business Machines Corporation

Panasonic Corporation

Toshiba Corporation

Revision 0.97

December 15, 2010

This page is intentionally left blank.

Preface

Notice

THIS DOCUMENT IS PROVIDED "AS IS" WITH NO WARRANTIES WHATSOEVER, INCLUDING ANY WARRANTY OF MERCHANTABILITY, NONINFRINGEMENT, FITNESS FOR ANY PARTICULAR PURPOSE, OR ANY WARRANTY OTHERWISE ARISING OUT OF ANY PROPOSAL, SPECIFICATION OR SAMPLE. IBM, Intel, Panasonic, and Toshiba disclaim all liability, including liability for infringement of any proprietary rights, relating to use of information in this specification. No license, express or implied, by estoppel or otherwise, to any intellectual property rights are granted herein.

This document is an intermediate draft and is subject to change without notice. Adopters and other users of this specification are cautioned that products based on it may not be interoperable with the final version or subsequent versions thereof.

Intellectual Property

Implementation of this specification requires a license from the 4C Entity, LLC. Note that use of the AES-based technology also requires execution of an addendum to the 4C license agreement.

Contact Information

Please address inquiries, feedback, and licensing requests to the 4C Entity, LLC:

- Licensing inquiries and requests should be addressed to 4C-Services@4Centity.com.
- Feedback on this specification should be addressed to 4C-Services@4Centity.com.

The URL for the 4C Entity, LLC web site is http://www.4Centity.com.

This page is intentionally left blank.

Table of Contents

Notice ..... **iii**

Intellectual Property ..... **iii**

Contact Information ..... **iii**

CHAPTER 1. INTRODUCTION **1**

1.1 Purpose and Scope **1**

1.2 Document Organization **1**

1.3 References **1**

1.4 Future Directions **2**

1.5 Notation **2**

CHAPTER 2. ABBREVIATIONS AND ACRONYMS **3**

CHAPTER 3. COMMON CPRM ELEMENTS FOR THE SD MEMORY CARD **5**

3.1 Introduction **5**

3.2 Device Requirements **5**

3.3 CPRM Components **5**
3.3.1 System Area 6
3.3.1.1 Media Identifier 6
3.3.1.2 Media Key Block (MKB) 7
3.3.2 Hidden Area 7
3.3.2.1 Media Unique Key 7
3.3.3 Protected Area 8
3.3.3.1 Encrypted Title Key, CCI (Copy Control Information) and UR (Usage Rules) 8
3.3.4 User Data Area 8
3.3.4.1 Encrypted content 8
3.3.4.2 MKB Extension 8

3.4 Content Encryption and Decryption Protocol **8**
3.4.1 Authentication and Key Exchange (AKE) 10
3.4.1.1 Random Number Generation 12

3.5 Accessing the Protected Area **12**
3.5.1 Secure Write Process to the Protected Area 13
3.5.2 Secure Read Process from the Protected Area 14
3.5.3 Secure Title Key Delete Process 15

3.6 Content Encryption and Decryption Format 16
3.6.1 General Principle 16

3.7 File System of the Protected Area 17
3.7.1 Directory and file configuration in the Protected Area 17

3.8 Process 17

3.9 MKB Extensions on SD Memory Card 18

3.10 Updateable MKB 18
3.10.1 Detailed procedure of the dynamic MKB update scheme 18
3.10.2 Redundancy Check Code (RCC) 22

3.11 Additional ID Binding 24
3.11.1 Device Requirements and Features 24
3.11.2 CPRM Components 24
3.11.3 Content Encryption and Decryption Protocol for Additional ID Binding 25

3.12 Enhanced Version of CPRM (AES-CPRM) 27

List of Figures

Figure 3-1 – SD Memory Card 6
Figure 3-2 – Calculation of Media Unique Key 7
Figure 3-3 – Content Encryption and Decryption on SD Memory Card 9
Figure 3-4 – Details of Authentication and Key Exchange (AKE) on SD Memory Card 11
Figure 3-5 – Protocol Flow of “Secure Write Process” to the Protected Area 13
Figure 3-6 – Protocol Flow of “Secure Read Process” from the Protected Area 14
Figure 3-7 – Protocol Flow of “Secure Title Key Delete Process” to the Protected Area 15
Figure 3-8 – Directory and File Configuration 17
Figure 3-9 – Dynamic Update MKB Scheme (Step1) 20
Figure 3-10 – Dynamic Update MKB Scheme (Step2) 21
Figure 3-11 – Dynamic Update MKB Scheme (Step3) 21
Figure 3-12 – RCC (Redundancy Check Code) Generation Scheme 22
Figure 3-13 – RCC Check Scheme 23
Figure 3-14 – Content Encryption and Decryption on additional ID Binding 25
Figure 3-15 – AES-CPRM Content Encryption and Decryption 28

This page is intentionally left blank.

List of Tables

Table 3-1 – Media Identifier Format for SD Memory Card 6

This page is intentionally left blank.

Chapter 1. Introduction

1.1 Purpose and Scope

The *Content Protection for Recordable Media Specification* (CPRM) defines a robust and renewable method for protecting content stored on a number of physical media types. The specification is organized into several "books." The *Introduction and Common Cryptographic Elements* book provides a brief overview of CPRM, and defines cryptographic procedures that are common among its different uses. The *SD Memory Card Book* specifies additional details for using CPRM technology to protect content stored on the SD Memory Card, and on other implementations of protected storage with an interface and security system equivalent to that of the SD Memory Card. Note that such other implementations must not provide any external interface to the memory other than one that adheres to the protocols described in this specification.

The *SD Memory Card Book* consists of the following parts, under the general title *CPRM Specification SD Memory Card Book:*

- *Common Part,*
- *SD-Application Specific Parts (e.g. SD-Audio, SD-Video, SD-Binding, SD-SD)*

This document is the *Common Part* of the *SD Memory Card Book,* and describes aspects of CPRM that are common to each SD-Application. Other *SD-Application Specific Parts* of the *SD Memory Card Book* describe additional details specific to each SD-Application.

The use of this specification and access to the intellectual property and cryptographic materials required to implement it will be the subject of a license. A license authority referred to as the 4C Entity, LLC is responsible for establishing and administering the content protection system based in part on this specification.

1.2 Document Organization

This specification is organized as follows:

- Chapter 1 provides an introduction.
- Chapter 2 lists abbreviations and acronyms used in this document.
- Chapter 3 describes the common CPRM protection mechanisms that are used to protect each SD-Application's content stored on SD Memory Card media.

1.3 References

This specification shall be used in conjunction with the following publications. When the publications are superceded by an approved revision, the revision shall apply.

4C Entity, LLC, *CPRM License Agreement*

4C Entity, LLC, *CPRM Specification: Introduction and Common Cryptographic Elements, Revision 1.1*

4C Entity, LLC, *Content Protection System Architecture White Paper, Revision 0.81*

SD Group, *SD Memory Card Specifications, Part 3: Security Specification, Version 1.01*

1.4 Future Directions

This document describes aspects of CPRM that are common to each existing SD application. In future revisions, additional common CPRM elements may also be described.

1.5 Notation

Except where specifically noted otherwise, this document uses the same notations and conventions for numerical values, operations, and bit/byte ordering as described in the *Introduction and Common Cryptographic Elements* book of this specification.

Chapter 2. Abbreviations and Acronyms

The following abbreviations and acronyms are used in this document:

AES	Advanced Encryption Standard
AKE	Authentication and Key Exchange
C-CBC	Converted Cipher Block Chaining
C2	Cryptomeria Cipher
CBC	Cipher Block Chaining
CCI	Copy Control Information
CPRM	Content Protection for Recordable Media
CTR	Counter
ECB	Electronic Codebook
FAT	File Allocation Table
ID	Identifier
LLC	Limited Liability Company
lsb	Least Significant Bit
MKB	Media Key Block
PC	Personal Computer
RCC	Redundancy Check Code
UR	Usage Rules
XOR	Exclusive-OR

This page is intentionally left blank.

Chapter 3. Common CPRM Elements for the SD Memory Card

3.1 Introduction

This chapter specifies details for using elements of CPRM technology that are common to the protection of each SD Application content stored on SD Memory Card media. The formats for each SD Application and the SD Memory Card are licensable from the SD Association and SD Group respectively, which also publishes specifications describing them in detail (see the corresponding references in Section 1.3). This chapter assumes that the reader is familiar with these formats, as defined in their corresponding specifications.

It is anticipated that CPRM technology may also be applied to other SD formats under future extensions to this specification, as authorized by the 4C Entity, LLC.

3.2 Device Requirements

Each CPRM compliant device (e.g. recording, playback, viewing, source, and destination device) for the SD Memory Card must follow the protocols for accessing devices described in this specification.

In addition, each device is given a set of 16 secret Device Keys, denoted K_{d_1},K_{d_2},…,K_{d_16}. There are different sets for each application group defined by the SD Association. The actual keys are provided by the 4C Entity, LLC, and are used for processing the MKB to calculate the Media Key (K_m), as described in the *Introduction and Common Cryptographic Elements* book of this specification. However, *f(c, r)* (the function that is XORed with the Media Key) is simply the constant 0 – that is, the function is effectively not used. Key sets may be either unique per device, or used commonly by multiple devices. The CPRM License Agreement describes the details and requirements associated with these two alternatives. A device shall treat its Device Keys as Highly Confidential, and their associated Row values as confidential, as defined in the CPRM License Agreement.

3.3 CPRM Components

This section describes the logical location and format of the CPRM components, when stored on the "SD Memory Card." Figure 3-1 depicts the logical locations of CPRM Components on the "SD Memory Card." These logical locations are used, unless explicitly noted otherwise in an application specific part of *CPRM SD Memory Card Book.*

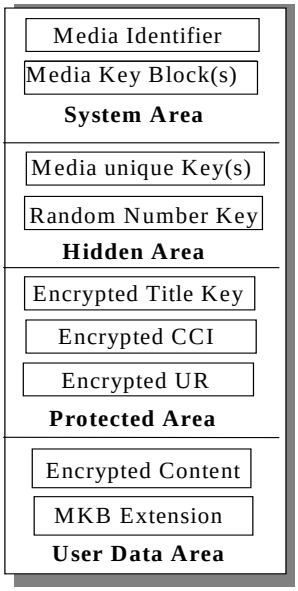

Figure 3-1 – SD Memory Card

- A Media Identifier (ID_{media}) and sixteen Media Key Blocks are pre-recorded in the System Area.
- Sixteen Media Unique Keys and Random Number Key are pre-recorded in the Hidden Area.
- Encrypted Title Keys, Encrypted CCI (Copy Control Information) and Encrypted UR (Usage Rules) are recorded in the Protected Area.
- Encrypted Content and MKB Extension are recorded in the User Data Area

3.3.1 System Area

Each CPRM Compliant SD Memory Card shall contain a System Area, which is a write-protected area that is accessible from outside the SD Memory Card. The System Area contains the Media Identifier (ID_{media}) and the Media Key Blocks (MKBs).

3.3.1.1 Media Identifier

Each CPRM Compliant SD Memory Card shall contain a 64-bit Media Identifier (ID_{media}), which is placed in the System Area by the SD Memory Card manufacturer. The Media Identifier logical format is shown in Table 3-1.

Table 3-1 – Media Identifier Format for SD Memory Card

Bit / Byte	7	6	5	4	3	2	1	0
0	Manufacturer ID							
1	(Data defined in *SD Memory Card Specifications –Part3 Security specification*)							
2								
3								
4								
5								
6								
7								

The 4C Entity, LLC assigns each licensee a unique 1-byte value as the Manufacturer ID field. Each licensee assigns the last 7-byte Data uniquely based on the *SD Memory Card Specifications -Part3 Security specification.*

3.3.1.2 Media Key Block (MKB)

Each CPRM Compliant SD Memory Card shall contain 16 distinct Media Key Blocks (MKBs) in order to support multiple applications. Each MKB is provided by the 4C Entity, LLC and is pre-recorded in the System Area by the SD Memory Card manufacturer. Each MKB shall have a maximum size of 65,536 bytes. Each MKB has at most 16 columns. A given column can have at most 500 rows.

3.3.2 Hidden Area

Each CPRM Compliant SD Memory Card contains a Hidden Area, which is a write-protected area that is accessible only to the SD Memory Card itself and contains the sixteen Media Unique Keys. The Hidden Area may also contain a Random Number Key, which is used in the random number generation process.

3.3.2.1 Media Unique Key

Each CPRM Compliant SD Memory Card shall contain 16 distinct Media Unique Keys (K_{mu}) corresponding to the 16 distinct Media Key Blocks. Each K_{mu} is 56-bit value and is pre-computed by the manufacturer based on each Media Key and the Media ID using the C2-Oneway function. Here, each Media Key is assigned by the 4C Entity, LLC, and is unique for each application group defined by the SD Association. Figure 3-2 shows the procedure of the Media Unique Key calculation. As shown in Figure 3-2, each Media Unique Key (K_{mu}) is calculated as

$$K_{mu}=[C2\_G\ (\text{Media Key, Media ID})]_{lsb\_56}.$$

The C2 One-way Function (C2_G) is described in the *Introduction and Common Cryptographic Elements* book of this specification.

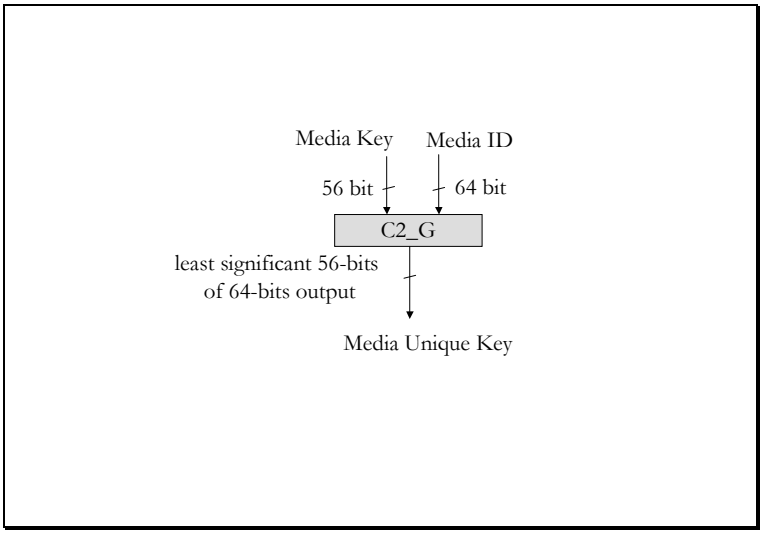

Figure 3-2 – Calculation of Media Unique Key

3.3.3 Protected Area

Each CPRM Compliant SD Memory Card shall contain a Protected Area, which is a read/write area that is accessible only after successful explicit mutual authentication. The Protected Area contains the Encrypted Title Keys and may also contain the Encrypted CCI (Copy Control Information), and/or Encrypted UR (Usage Rules).

3.3.3.1 Encrypted Title Key, CCI (Copy Control Information) and UR (Usage Rules)

In the SD Memory Card, each piece of content to be protected shall be encrypted by a unique Title Key.

Some SD applications define CCI (Copy Control Information). When CCI is defied, the Title Key and CCI of the content are concatenated and encrypted together by a Media Unique key, which is unique for each SD Memory Card. The Encrypted Title Keys and CCI are stored as a file in the Protected Area.

Other SD applications also define UR (Usage Rules). When UR is defied, the encryption of UR is defined by each application specific part of the *CPRM SD Memory Card Book.*

The file system of the Protected Area and the detailed format of the Encrypted Title Keys, CCI and/or UR are specific for each application, and are described in each application specific part of the *CPRM SD Memory Card Book.*

3.3.4 User Data Area

The SD Memory Card shall contain a User Data Area, which is a user-accessible read/write area that is used to store Encrypted content. User Data Area may also contain other user data. When the SD Memory Card is connected to a PC, the user data area typically looks like a normal disk.

3.3.4.1 Encrypted content

In the SD Memory Card, each piece of content to be protected shall be encrypted with a unique Title Key, and stored as an encrypted file in the User Data Area. The file system of the User Data Area is typically a FAT12, FAT16, FAT32 or exFAT file system. The directory structure and file names of the encrypted content are defined in each application specific part of the *CPRM SD Memory Card Book.*

3.3.4.2 MKB Extension

The User Data Area may also contain an MKB Extension file. Regarding the MKB Extension file, refer to section 3.9.

3.4 Content Encryption and Decryption Protocol

Figure 3-3 illustrates a basic process for content encryption and decryption on the "SD Memory Card." This figure shows the case where CCI is defined. In the case where UR (Usage Rules) is defined, a similar process for content encryption and decryption is applicable, and the details are described in each application specific part of the *CPRM SD Memory Card Book.*

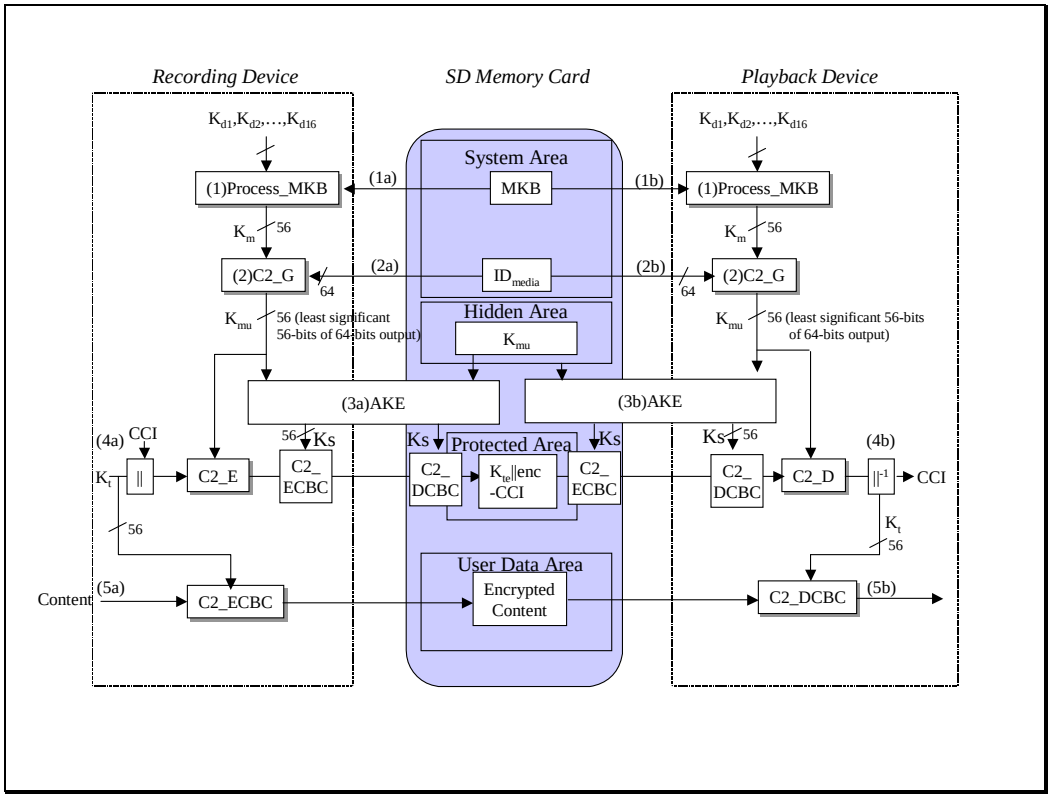

Figure 3-3 – Content Encryption and Decryption on SD Memory Card

The SD Memory Card and the accessing device (Recording Device / Playback Device) authenticate each other, and encrypt or decrypt content as follows:

- (1) The accessing device executes Process_MKB

  (1a, 1b) Calculate Media Key from MKB using Device Keys. (see chapter 3 in the *Introduction and Common Cryptographic Elements* book of this specification)

- (2) The accessing device executes the C2_G process

  (2a, 2b) Calculate Media Unique Key (K_{mu}) from Media Key (K_m) and Media Identifier (ID_{media}). (see chapter 3 in the *Introduction and Common Cryptographic Elements* book of this specification)

- (3) AKE process

  (3a, 3b) If the AKE process succeeds, the Session Key (K_s), which is randomly generated in each AKE Process, is shared between the accessing device (Recording Device/Playback Device) and SD Memory Card. (The detail of AKE Process is shown in 3.4.1)

-(4a) Encrypt Title Key and CCI process.

  When the content is encrypted, a Title Key is picked at random. The Recording Device concatenates the Title Key (K_t) and CCI (Copy Control Information) and then encrypts them together using the Media Unique Key (K_{mu}) with C2_E (the C2 cipher algorithm in ECB mode) described in the *Introduction and Common Cryptographic Elements* book of this specification. Then, the Encrypted Title Key and CCI are further encrypted by the Session Key (K_s), which is shared at step (3a), using the C2_ECBC (C2 cipher algorithm in C-CBC mode) described in the *Introduction and Common Cryptographic Elements* book of this specification. The doubly-encrypted Encrypted Title Key and CCI are sent to the SD Memory Card. In the SD Memory Card, they are decrypted by the Session Key (K_s), which is shared at step (3a), using the C2_DCBC, and those results (Encrypted Title Key and CCI) are stored in the Protected Area.

-(4b) Decrypt Encrypted Title Key and CCI process.

The Encrypted Title Key (K_t) and CCI are encrypted by the SD Memory Card using the Session Key (K_s), which is shared at step (3b), using the C2_ECBC (C2 cipher algorithm in C-CBC mode) described in the *Introduction and Common Cryptographic Elements* book of this specification. The doubly-encrypted Encrypted Title Key and CCI are sent to the Playback Device. Then, in the Playback Device, they are decrypted by the Session Key (K_s), which is shared at step (3b), using the C2_DCBC, and those results (Encrypted Title Key and CCI) are decrypted using the Media Unique Key (K_{mu}) with C2_D (the C2 cipher algorithm in ECB mode) described in the *Introduction and Common Cryptographic Elements* book of this specification.

-(5a) Encrypt content process

The Recording Device shall protect each piece of content by encrypting it using the Title Key (K_t) with C2_ECBC (C2 cipher algorithm in C-CBC mode) described in the *Introduction and Common Cryptographic Elements* book of this specification. Note that if the content delivered to the Recording Device is already encrypted in this way, the Recording Device does not perform this encryption step. It then sends it to the SD Memory Card, and stores it in the User Data Area.

-(5b) Decrypt encrypted content process

The Playback Device uses the Title Key (K_t) decrypted at step (4b) to decrypt the encrypted content using C2_DCBC (C2 cipher algorithm in C-CBC mode) described in the *Introduction and Common Cryptographic Elements* book of this specification.

3.4.1 Authentication and Key Exchange (AKE)

The SD Memory Card supports explicit mutual authentication with an accessing device (Recording Device or Playback Device) for protection against save-restore attacks and man-in-the-middle attacks.

When a device accesses data stored in the Protected Area, an SD Memory Card and the accessing device authenticate each other by a challenge-response protocol. When this authentication is successful, they share a secure common session key. This protocol is called Authentication and Key Exchange (AKE). The session key is used for encrypting and decrypting the protected data on the bus between accessing device and SD Memory Card. As shown in Figure 3-4, the AKE protocol also protects the argument field (32 bits) of the security commands, which are used to access the Protected Area as described in chapter 3 of *SD Memory Card Specifications -Part3 Security specification*.

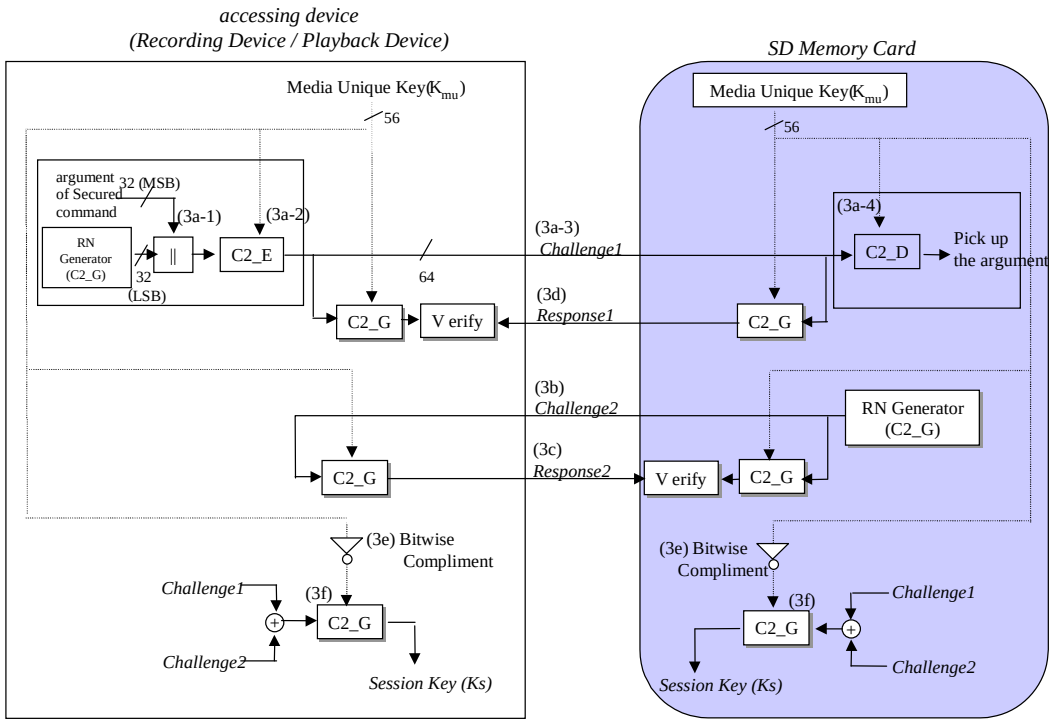

Figure 3-4 – Details of Authentication and Key Exchange (AKE) on SD Memory Card

The AKE procedure is the following:

(3a-1) In the accessing device (Recording Device / Playback Device), the argument of security command (32 bits), which is described in chapter 3 of the *SD Memory Card Specifications – Part3 Security Specification*, is concatenated with a random number (32 bits),

(3a-2) The result (64 bits) is encrypted by K_{mu} (Media Unique Key) using C2_E, and

(3a-3) The accessing device sends the cipher-text (64 bits) as Challenge1 to SD Memory Card.

(3a-4) In the SD Memory Card, the received data is decrypted by K_{mu} using C2_D. The decrypted argument is remembered securely and is used in the subsequent security command.

(3b) SD Memory Card sends a Challenge2 (64 bit random value) to the accessing device.

(3c) The accessing device calculates Response2 = C2_G (K_{mu}, Challenge2) and returns it to the SD Memory Card. The SD Memory Card calculates Vresponse2 =C2_G (K_{mu}, Challenge2), and checks if Vresponse2 == Response2. If they match, then go to (3d). Otherwise, abort this process.

(3d) SD Memory Card calculates Response1 = C2_G (K_{mu}, Challenge1), and returns it to the accessing device. The accessing device calculates Vresponse1 = C2_G (K_{mu}, Challenge1), and checks if VResponse1 == Response1. If they match, then go to (3e). Otherwise, abort this process.

(3e) The bitwise complement of Media Unique Key, (~K_{mu}), is generated in both the SD Memory Card and the accessing device.

(3f) A Session Key (K_s) is calculated as

$$K_s = [C2\_G\ (\sim K_{mu}, \text{Challenge1} \oplus \text{Challenge2})]_{lsb\_56}$$

in both the SD Memory Card and the accessing device. The function C2_G is the C2 One-way Function described in the *Introduction and Common Cryptographic Elements* book of this specification. The Challenge and Response values are 64 bits long, and Session Key (K_s) is 56 bits long.

When this authentication process is successful, the data field of security command is encrypted using the session key (K_s) with C2_ECBC.

The SD Memory Card shall enforce the order of steps in the protocol, by ignoring any commands received out of order. The SD Memory Card shall abort the process after step (3c) if the accessing device's response is not correct.

3.4.1.1 Random Number Generation

The SD Memory Card uses a unique random number generator for the challenges in this protocol. Note that with this protocol, even if the challenges can be predicted, the Session Key cannot. Therefore, a random number generator used solely for this protocol does not need to produce an unpredictable sequence, like the generator specified in the *Introduction and Common Cryptographic Elements* book of this specification does. Its only requirements are: 1) the seed cannot be set from outside the card, and 2) the numbers come from a long sequence (approximately 2^{64}).

3.5 Accessing the Protected Area

In the case of the SD Memory Card, AKE is used to control access to the Protected Area.

Three operations are possible on the Protected Area:

- Write a protected data item (Encrypted Title Key, CCI and/or UR) (part of recording content)
- Read a protected data item (part of playback)
- Delete a protected data item (part of removing content).

Each time one of these operations is performed, a successful AKE must first take place. The resulting Session Key is used to encrypt the data field of the security command, which is described in chapter 3 of the *SD Memory Card Specifications – Part3 Security Specification*. The data field is encrypted with C2 in C-CBC mode, with continuous chaining. The argument field, while not encrypted, is protected against tampering, because it forms part of the challenge in the AKE protocol.

Note that the actual security commands used are block-oriented; they deal with units of 512-byte sectors. Thus, to write a small item, it might be necessary to first read the data block to make the small change. These straightforward details are omitted from this specification.

As explained in chapter 3 of *SD Memory Card Security Specifications – Part3 Security Specification*, sectors in the protected area may be written in either "mode 0" or "mode 1." Mode 0 sectors can be read by any application that can perform a successful AKE. Mode 1 sectors can only be read successfully by the same application that wrote them – or at least by one that uses the same MKB. In other words, when a mode 1 sector is written, the card records the MKB number used during the preceding AKE. If the sector is read using an AKE with a different MKB, an error occurs. File system metadata sectors shall be written in mode 0. File data sectors shall be written in mode 1.

Note: The boundary between the Protected Area and the User Area can be moved by a secure command. If this command extends the Protected Area, the SD Memory Card shall erase the new memory that is added to the Protected Area. If this command decreases the Protected Area, the SD Memory Card shall erase the new memory that is added to the User Area. The erase is performed before the boundary move is committed.

3.5.1 Secure Write Process to the Protected Area

Figure 3-5 shows the protocol flow for the accessing device writing an Encrypted Title Key to the Protected Area using an SD Memory Card command, which is described in chapter 3 of the *SD Memory Card Specifications – Part3 Security Specification*.

This figure shows the case where CCI is defined. In the case where UR (Usage Rules) is defined, in steps (4a) and (4c) of Figure 3-5, CCI should be replaced with UR, unless explicitly noted otherwise in an application specific part of *CPRM SD Memory Card Book.*

An accessing device (e.g. Recording, Playback Device) may securely remember the Media Unique Key value calculated during the first AKE, in order to avoid the "Calculate Media Unique Key Process (steps (1a)~(1d) and (2a)~(2d) of Figure 3-5) " in subsequent AKE procedures with the same SD Memory Card.

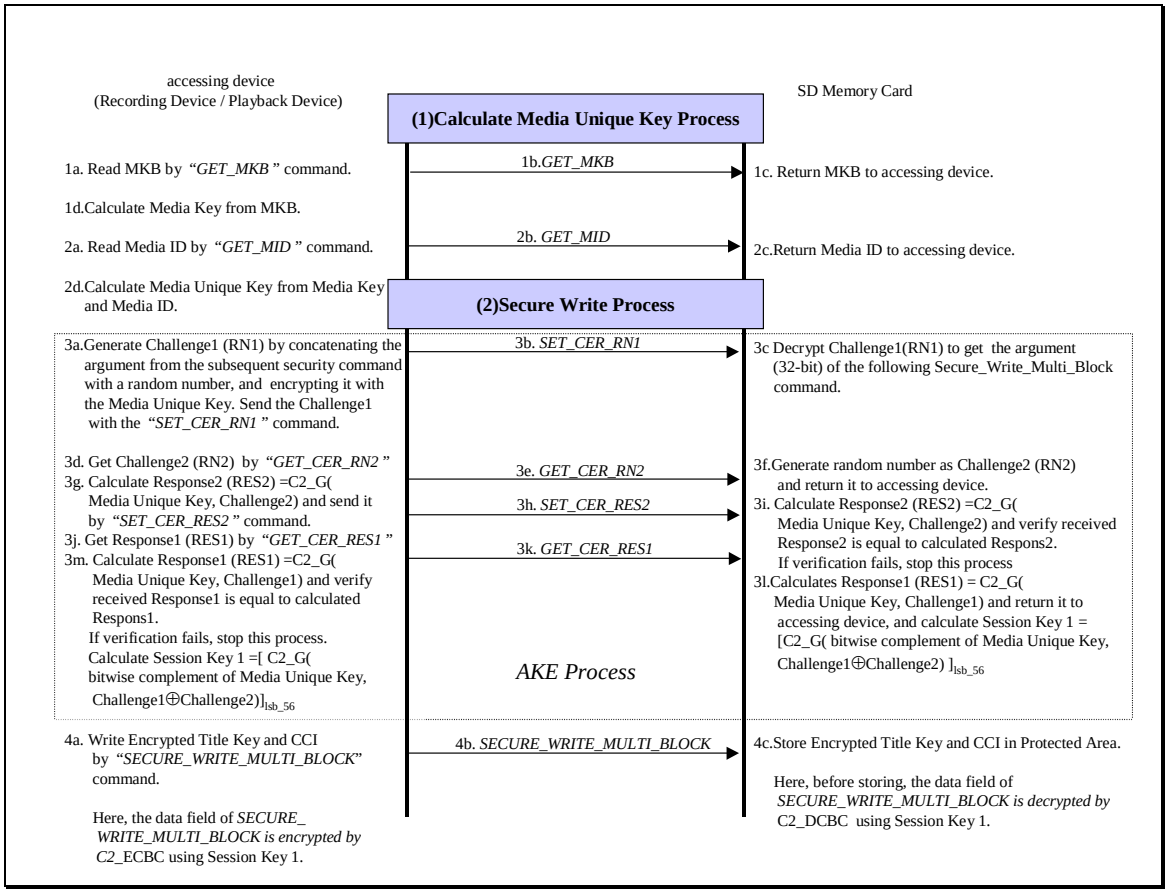

Figure 3-5 – Protocol Flow of "Secure Write Process" to the Protected Area

3.5.2 Secure Read Process from the Protected Area

Figure 3-6 shows the protocol flow for the accessing device reading an Encrypted Title Key from the Protected Area using SD Memory Card Command, which is described in chapter 3 of the *SD Memory Card Specifications – Part3 Security Specification*.

This figure shows the case where CCI is defined. In the case where UR (Usage Rules) is defined, in steps (6a), (6c), and (6d) of Figure 3-6, CCI is replaced with UR, unless explicitly noted otherwise in an application specific part of *CPRM SD Memory Card Book.*

In Figure 3-6, it is supposed that an accessing device securely holds the Media Unique Key value before the AKE process. If not, it is necessary to execute the "Calculate Media Unique Key Process (steps (1a)~(1d) and (2a)~(2d) of Figure 3-5)" before the AKE process.

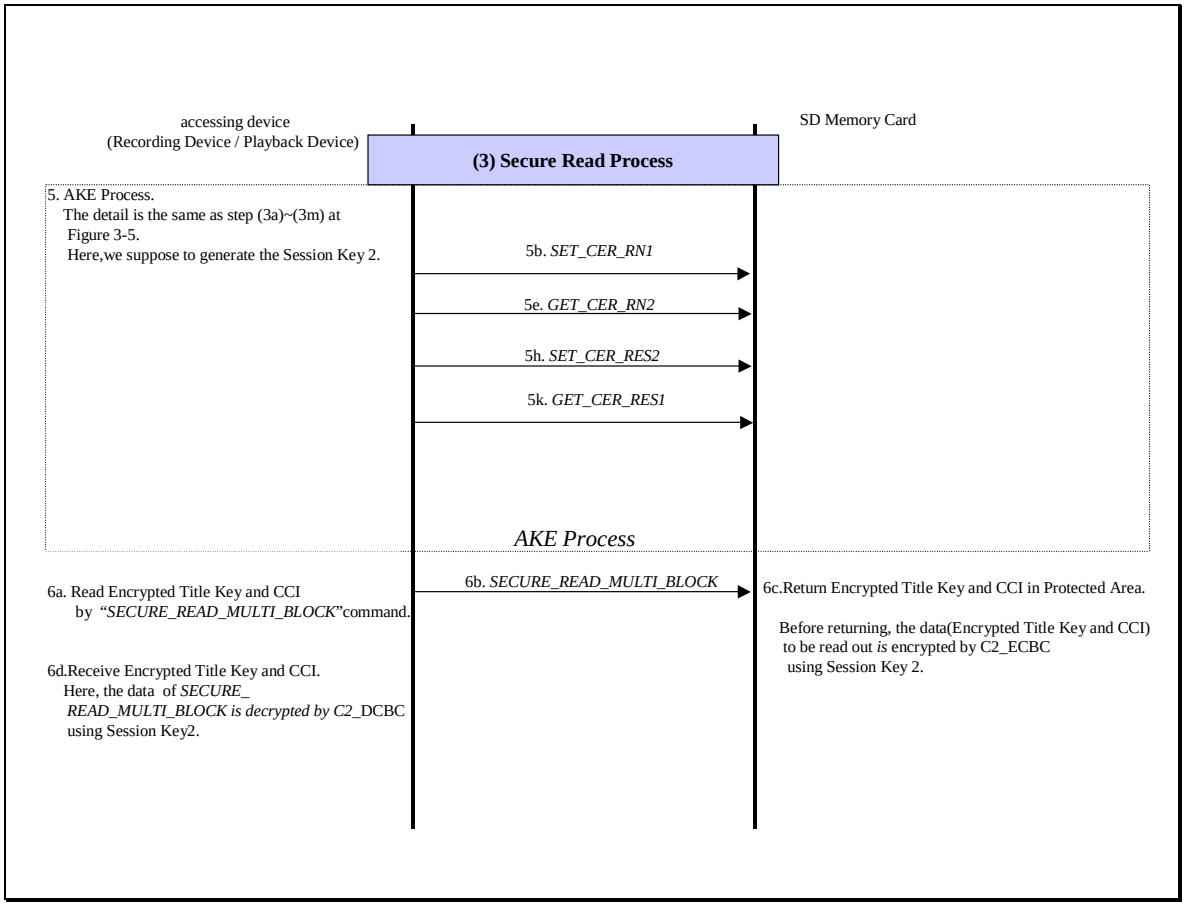

Figure 3-6 – Protocol Flow of "Secure Read Process" from the Protected Area

3.5.3 Secure Title Key Delete Process

An accessing device may delete an Encrypted Title Key from the Protected Area by linking together the write and read operations described above. First a write operation overwrites the Encrypted Title Key with a selected value, and then a read operation reads the value to confirm that the overwriting was successful. Figure 3-7 shows the protocol flow for the accessing device deleting an Encrypted Title Key in the Protected Area.

This figure shows the case where CCI is defined. In the case where UR (Usage Rules) is defined, in step (10c) of Figure 3-7, CCI is replaced with UR, unless explicitly noted otherwise in an application specific part of *CPRM SD Memory Card Book*.

In Figure 3-7, it is supposed that an accessing device securely holds the Media Unique Key value before the AKE process. If not, it is necessary to execute the "Calculate Media Unique Key Process (steps (1a)~(1d) and (2a)~(2d) of Figure 3-5)" before the AKE process.

Note: The SD Memory Card has a "Secure Erase" command. This command is a low-level writing command to improve performance of writes in the Protected Area. It is *not* a substitute for this Secure Title Key Delete process.

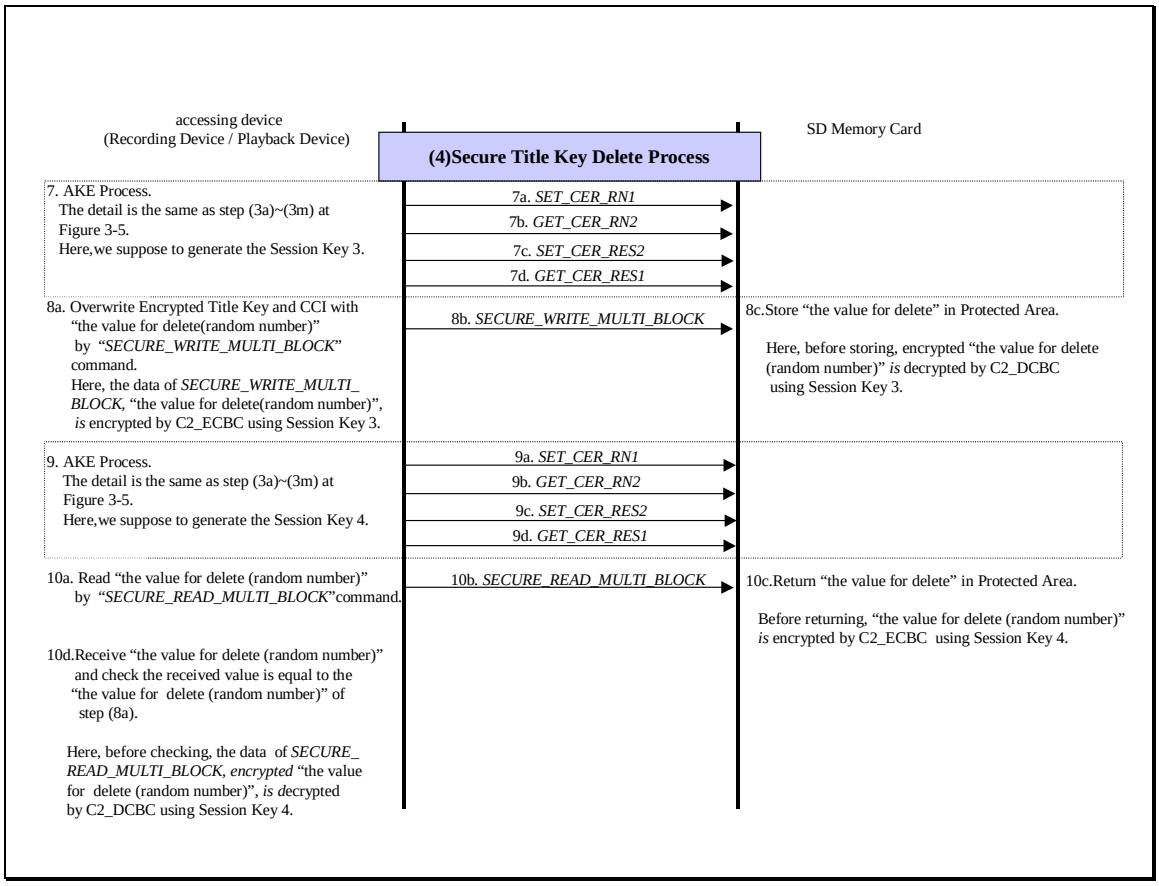

Figure 3-7 – Protocol Flow of "Secure Title Key Delete Process" to the Protected Area

Note: In step (8a) of Figure 3-7, the mode of *SECURE_WRITE_MULTI_BLOCK* shall be set "mode 1." Here, regarding the "mode" of *SECURE_WRITE_MULTI_BLOCK* command, refer to chapter 3 of the *SD Memory Card Specifications – Part3 Security Specification.*

If deletion of the Title Key is not verified, the accessing device must assume the deletion has not occurred. The actual Title Key usually resides within a single sector. As a side effect of updating that sector, file system metadata sectors might need to be written. If so, they should follow the same write/read-back protocol.

Some benefits that result from the use of SD Memory Card AKE are:

- Use of the Media Unique Key as part of the AKE protects against potential man-in-the-middle attacks on the Media ID and Media Key Block, since AKE will fail if either of those values is tampered with during transfer to the accessing devices.
- Use of a new Session Key to decrypt each Protected Data (Encrypted Title Key and/or CCI and/or UR) before storing it in the Protected Area protects against save/restore attacks (where an Encrypted Title Key is saved before check-in, then restored afterwards).
- Use of a new Session Key to encrypt each Protected Data as it is read from the Protected Area protects against a “replay” attack, where all values stored on the media (including Encrypted Title Keys) are recorded and then “fed” into a compliant player.

Use of a random value in the explicit Delete Encrypted Title Key process protects against a potential man-in-the-middle attack where check-in would be circumvented by intercepting the delete command and forging a response.

3.6 Content Encryption and Decryption Format

3.6.1 General Principle

The content to be protected shall be encrypted. When the content is more than 64 bits, the content is split into 64-bit blocks and each block is encrypted using C2 cipher in C-CBC mode, as described in the *Introduction and Common Cryptographic Elements* book of this specification. If the last block is incomplete (a residual block, i.e. the length of the last block is less than 64 bits) it is left unencrypted (usually, each SD application does not contain critical data in the last few bytes). If the entire content is less than 64 bits, the data is unencrypted. A detail encryption and decryption format of each object (e.g. AAC, MP3, JPEG, MPEG etc.) is described in each application specific part of *CPRM SD Memory Card Book*.

3.7 File System of the Protected Area

This section shows the file system of the Protected Area. The physical allocation of the file system of the Protected Area is described in Chapter 5 of *SD Memory Card Specifications –Part3 Security Specification.*

3.7.1 Directory and file configuration in the Protected Area

The directory and file configuration in the Protected Area are as follows, unless explicitly noted otherwise in an application specific part of *CPRM SD Memory Card Book*:

- In the Protected Area, a directory is assigned by each application. The directory name is "XXX" (Here, "XXX" = the name of SD application which is defined by the SD Association)
- Within each directory, the file stored Encrypted Title Key is named "YYY.KEY" (Here, "YYY" is assigned by each SD application).

As shown in Figure 3-8, in the case of SD-Audio, the directory name is SD_AUDIO and the file stored Encrypted Title Key is AOBSA1.KEY or POBSP1.KEY

The detail of directory and file configuration in the Protected Area of each SD application is described in each application specific part of *CPRM SD Memory Card Book*.

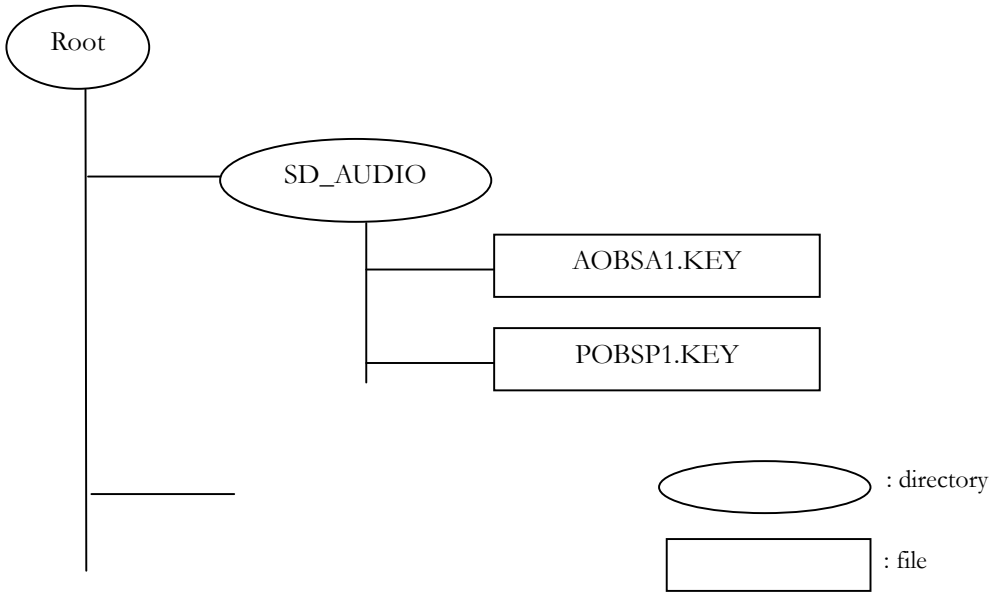

Figure 3-8 – Directory and File Configuration

3.8 Process

Each SD application specific Process, (e.g. Recording, Check-in/Check-Out, Move, Copy, Playback, Viewing etc.), are described in each application specific part of the *CPRM SD Memory Card Book*.

3.9 MKB Extensions on SD Memory Card

This section describes the MKB Extension file configuration on the SD Memory Card. MKB Extensions are described in the *Introduction and Common Cryptographic Elements* book of this specification.

The MKB Extension file configuration is as follows, unless explicitly noted otherwise in an application specific part of *CPRM SD Memory Card Book*:

- In the User Data Area, a directory is assigned by each application. The directory name is “XXX” (XXX = the name of the given SD application, which is defined by the SD Association).
- Within each such directory, the MKB Extension file is named "XXX.MKB" (XXX = the name of the SD application).

For example, in the case of SD-Audio, the directory name is SD_AUDIO and the file name of the MKB Extension file is SD_AUDIO.MKB.

All Playback and Recording Devices used for each application where MKB extensions are supported must recognize and use an MKB Extension if one is present. This applies even to such a Recording Device that is not capable of writing MKB extensions. Since writing MKB Extensions is not mandatory, even for applications where they are supported, MKB processing shall proceed as usual if no MKB Extension is present (i.e. it is not considered an error if an MKB Extension is not present).

For the SD Memory Card, the decision to write an MKB Extension shall be made *without* regard to the Revision fields in the Static MKB or the New MKB (also denoted as the MKB for MKB Extension).

3.10 Updateable MKB

In addition to the extended MKB, a “read-only” MKB stored in a SD Memory Card can be updated via a special authorized accessing device (e.g., a Kiosk). This scheme is called the “dynamic MKB update scheme.”

In the SD Memory Card, 16 MKBs are pre-stored. Some of the 16 MKBs are updateable; some are not. The ones that are not updateable are therefore not affected by the security of the special Updating Device.

For the purpose of updating MKBs, a special MKB called the Master MKB ("M_MKB") is used.

The special authorized accessing device is called an “Updating Device.” The M_MKB is stored on the System Area of SD Memory Card when manufactured. Master Device Key Set "M_DKS" corresponding to M_MKB are provided exclusively to the Updating Devices.

Suppose an application on an Updating Device uses A_MKB and the Updating Device has capability of updating the A_MKB. The procedure of the dynamic update scheme is sketched as follows:

- When necessary, a new A_MKB is issued from 4C Entity, LLC to the Updating Device.
- The Updating Device is allowed to update new A_MKB dynamically if and only if mutual authentication between the Updating Device and the SD Memory card succeeds using both the M_MKB and the present A_MKB.

The M_MKB itself is not updateable by applying this dynamic MKB update scheme.

3.10.1 Detailed procedure of the dynamic MKB update scheme

Figure 3-9, Figure 3-10 and Figure 3-11depict a detail procedure of a dynamic update MKB scheme:

(1) Generate a new MKB "A_MKB (new)" at 4C Entity, LLC.

- Generate a random value as a new Media Key A_K_m (new).
- Generate A_MKB (new) using the A_K_m (new), a Device Key Matrix "A_DKM" and Key Revocation Information "A_KRI.”
- Send A_MKB (new) securely from the 4C Entity, LLC to the Updating Device.

(2)-(4) Mutual Authentication (AKE) using M_MKB between the Updating Device and the SD Memory Card.

- Process M_MKB using a Master Device Key Set "M_DKS" and calculate the Master Media Key "M_K_m." If the Updating Device is revoked, the correct M_K_m cannot be calculated.
- Calculate the Master Media Unique Key "M_K_{mu}" using M_K_m and Media ID "ID_{media}."
- Authenticate mutually using "M_K_{mu}." Here, on the SD Memory Card, "M_K_{mu}" is pre-stored when it is manufactured. If this authentication step fails, stop the updating process. If this authentication step succeeds, the session key is generated at both the Updating Device and the SD Memory Card. This session key is used at step (6).

(5) If Mutual Authentication (AKE) using M_MKB succeeds, generate the new Media Unique Key "A_K_{mu} (new)" and the Redundancy Check Code (RCC) for the SD Memory Card.

- Process A_MKB (new) using a Device Key Set "A_DKS" and calculate the Media Key "A_K_m (new)." If the Updating Device is revoked, the correct A_K_m (new) cannot be calculated.
- Calculate the A_K_{mu} (new) using the A_K_m (new) and ID_{media} of the SD Memory Card.
- Calculate the Redundancy Check Code (RCC) for A_MKB (new) and A_K_{mu} (new). RCC is used for error detecting purpose on SD Memory Card. The detail of RCC Calculation is described in 3.10.2.

(6) Write A_MKB (new) from the Updating Device to the SD Memory Card.

- Send A_MKB (new), A_K_{mu} (new) and RCC value from the Updating Device to the SD Memory Card. Here, at least A_K_{mu} (new) is encrypted using the session key that is generated at step (4).
- A_MKB (new), A_K_{mu} (new) and RCC value are stored on a temporary register of the SD Memory Card.

(7) Check the Redundancy Check Code (RCC) on the SD Memory Card.

- Calculate RCC value from A_MKB (new) and A_K_{mu} (new) stored at step (6) at the SD Memory Card and verify the "calculated RCC" is equal to the "stored RCC at step (6)."
- After Calculation of the RCC value, A_MKB (new) and A_K_{mu} (new) are discarded.
- If this verification step fails, stop the updating process. If this verification step succeeds, go to the next step.

(8)-(10) Mutual Authentication (AKE) using present "A_MKB" between the Updating Device and the SD Memory Card.

- Process A_MKB using a Device Key Set "A_DKS" and calculate the present Media Key "A_K_m." If the Updating Device is revoked, the correct A_K_m cannot be calculated.
- Calculate the present Media Unique Key "A_K_{mu}" using A_K_m and ID_{media}.
- Mutually authenticate using "A_K_{mu}." Here, on the SD Memory Card, "A_K_{mu}" is pre-stored when manufactured. If this authentication step fails, stop the updating process. If this authentication step succeeds, the session key is generated at both the Updating Device and the SD Memory Card. This session key is used for encryption at step (11).

(11) If Mutual Authentication (AKE) using present A_MKB succeeds, re-write A_MKB (new) and A_K_{mu} (new) from the Updating Device to the SD Memory Card.

- Re-send A_MKB (new), A_K_{mu} (new) and RCC value. Here, at least A_K_{mu} (new) is encrypted using the session key that is generated step (10).
- A_MKB (new) is stored temporary on a System Area of the SD Memory Card and A_K_{mu} (new) is stored temporary on a Hidden Area of the SD Memory Card. RCC value is stored on a temporary register of the SD Memory Card.

(12) Verify the Redundancy Check Code (RCC) on the SD Memory Card.

- Calculate RCC value from A_MKB (new) and A_K_{mu} (new) stored at step (11) at the SD Memory Card and verify the "calculated RCC" is equal to both the "stored RCC at step (11)," and the "stored RCC at step (6)."

(13) Update the A_MKB (new) and A_K_{mu} (new).

- If these verifications of step (12) fail, A_MKB (new) and A_K_{mu} (new) are discard and stop the updating process. If these verifications succeed, update the present MKB "A_MKB" with new MKB "A_MKB (new)" and the present A_K_{mu} with new A_K_{mu} (new).

(14)-(20) Update Encrypted Title Key.

- Process A_MKB (new) using a Device Key Set "A_DKS" and calculate the new Media Key A_K_m(new)." If the Updating Device is revoked, the correct A_K_m(new) could not be calculated.
- Calculate the new Media Unique Key "A_K_{mu} (new)" using A_K_m (new) and ID_{media}.
- Mutually authenticate using "A_K_{mu} (new)." If this authentication step fails, stop the updating process. If this authentication step succeeds, the session key is generated at both the Updating Device and the SD Memory Card. This session key is used for encryption at the next step.
- If Mutual Authentication (AKE) using A_MKB (new) succeeds, read the Encrypted Title Key "K_{te}." Here, K_{te} is encrypted using the session key.
- Mutually authenticate using "A_K_{mu} (new)." If this authentication step fails, stop the updating process. If this authentication step succeeds, the session key is generated at both the Updating Device and the SD Memory Card. This session key is used for encryption at the next step.
- If Mutual Authentication (AKE) using "A_K_{mu} (new)" succeeds, decrypt each Encrypted Title Key (K_{te}) using K_{mu} and re-encrypt each Title Key using K_{mu} (new) to generate K_{te} (new).
- Write K_{te} (new) from the Updating Device to SD Memory Card. Here, K_{te} (new) is encrypted using the session key.

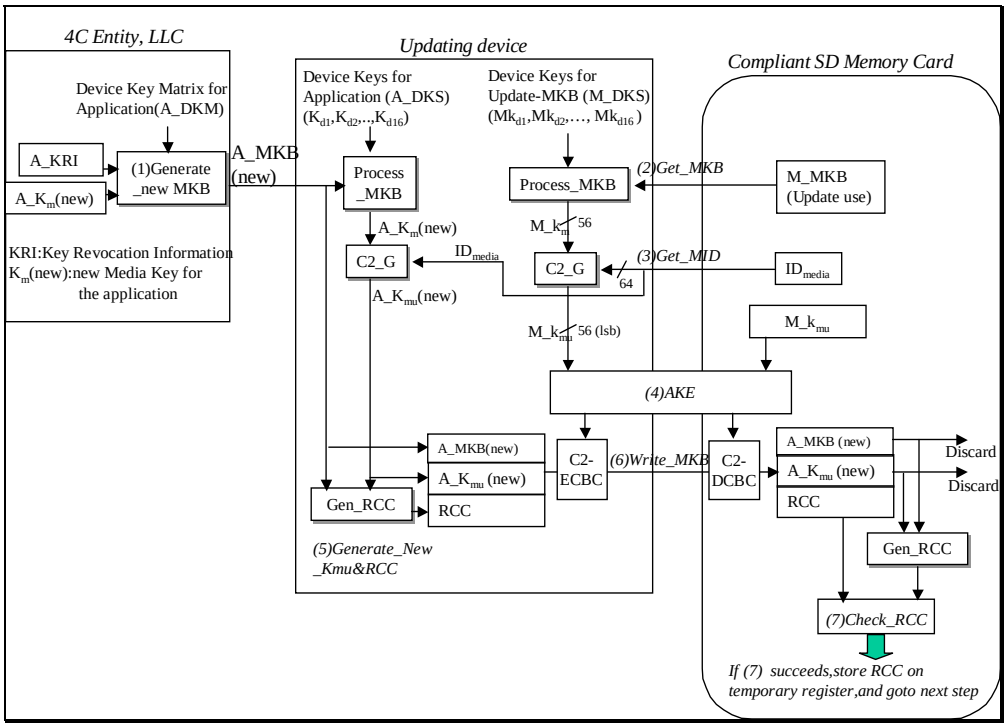

Figure 3-9 – Dynamic Update MKB Scheme (Step1)

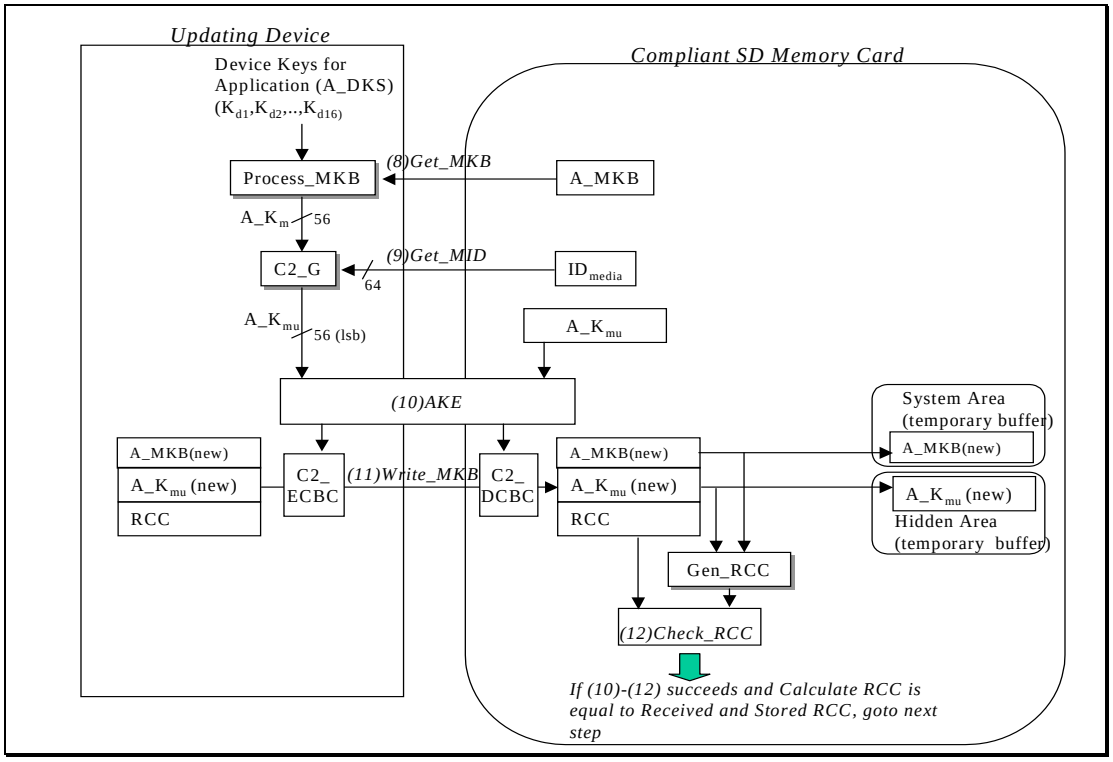

Figure 3-10 – Dynamic Update MKB Scheme (Step2)

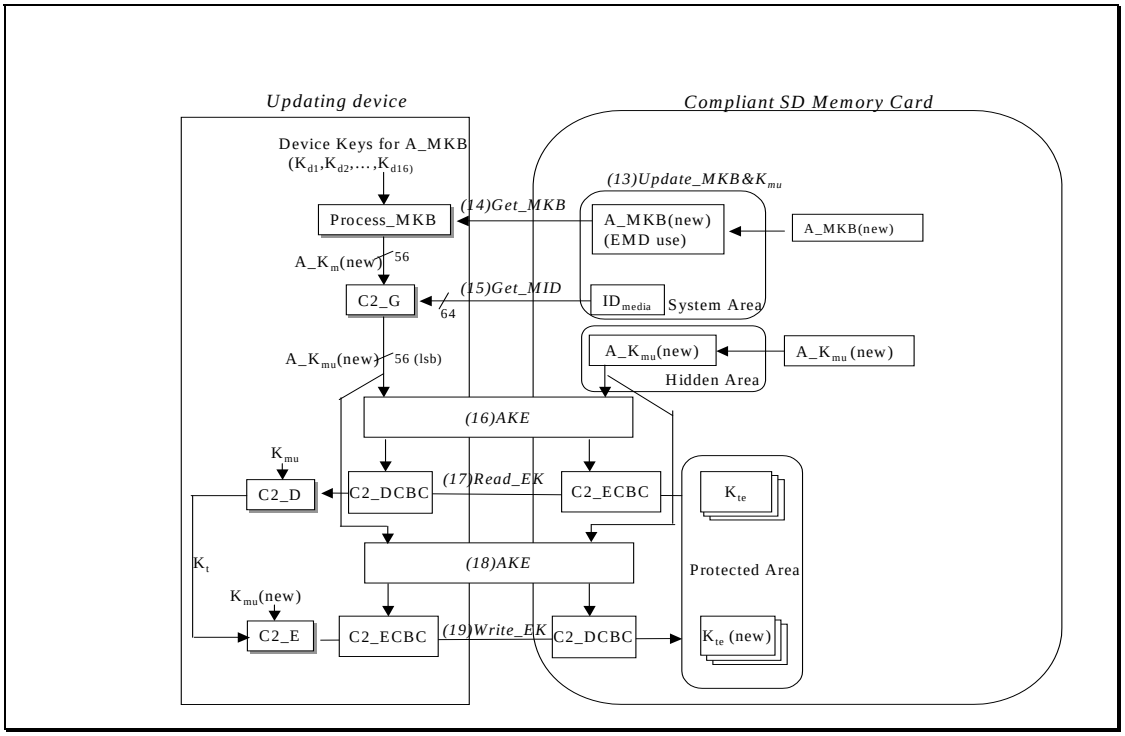

Figure 3-11 – Dynamic Update MKB Scheme (Step3)

3.10.2 Redundancy Check Code (RCC)

Figure 3-12 and Figure 3-13 show the Redundancy Check Code (RCC) generation and check scheme.

(1) RCC generation is as follows:

(1.1) Padding process

If the length (byte size) of the MKB (new) data, which consists of MKB (new) is not multiple of 8 bytes, the MKB is padded. The K_{mu} (new), which is always 7 bytes, is also padded to be 8 bytes. The padding method used is method 1 (all "0"'s padding) specified in ISO 10118-1 "*Information technology- Security techniques -Hash functions- Part 1 General*."

(1.2) As shown in Figure 3-12, Exclusive-OR is processed for each 8byte data block.

The result value is the RCC.

(2) RCC Check is as follows:

(2.1) As shown in Figure 3-13, each 8-byte data block (including RCC) Exclusive-OR'ed into an accumulator.

If the accumulator result value is 0, the data is correct.

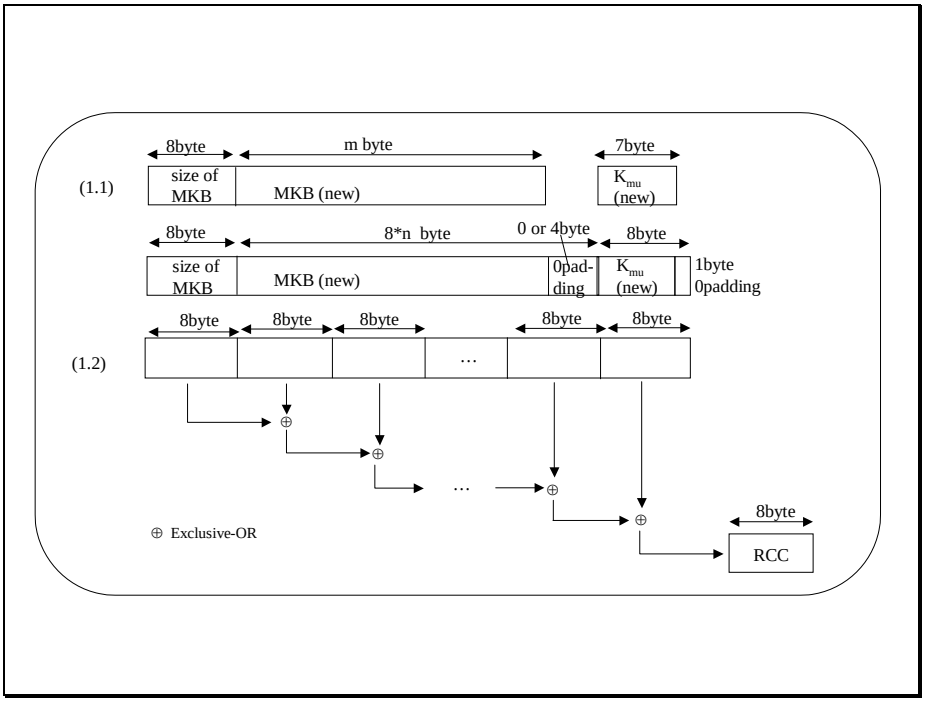

Figure 3-12 – RCC (Redundancy Check Code) Generation Scheme

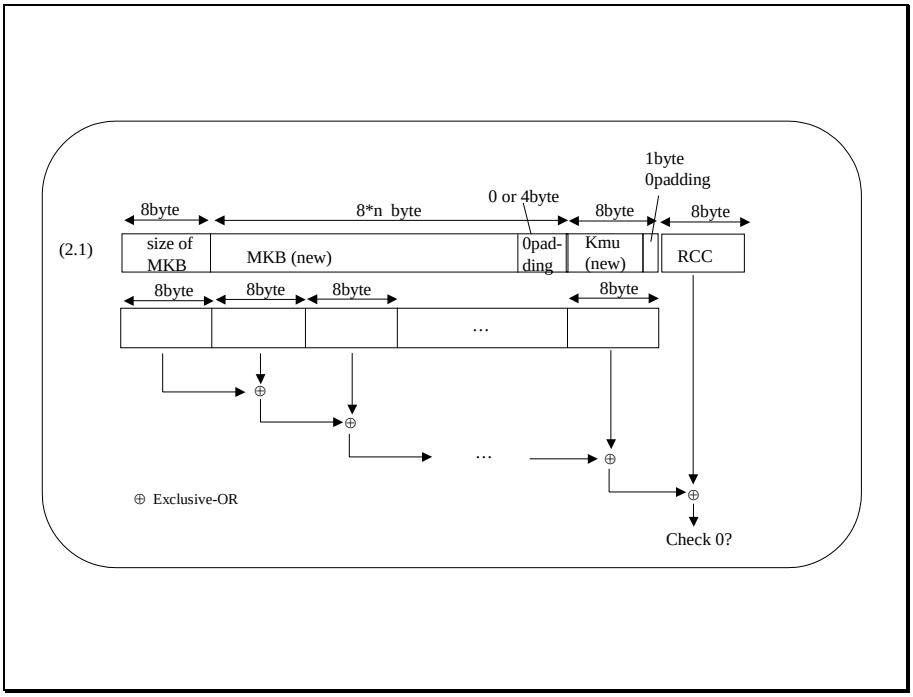

Figure 3-13 – RCC Check Scheme

3.11 Additional ID Binding

Through the use of the Media Unique Key (K_{mu}), content protected by CPRM on an SD Memory Card is always "bound" to the Media ID of that SD Memory Card. For some SD applications, it may be desirable to further "bind" such content to an additional identifier. In this section, such an additional identifier (e.g. Set ID, Holder ID) is generically referred to as a "Bind ID" (ID_{bind}).

Note that means for ensuring the integrity and uniqueness of the Bind ID itself are outside the scope of CPRM.

Even if Bind ID is used, contents are cryptographically bound to media.

This section specifies additional details for using CPRM to realize such "additional ID Binding" for each SD application.

- One such example of an additional ID is Set Identification (SET ID). In this case, the content is played back only on a device which is used to download that content.
- Other such example is Holder Identification (Holder ID). In this case, the content is played back only on each device which is owned by a holder (purchaser) of that content.
- The combination of above identifiers is also applicable.

The use of "additional ID Binding" functionality is determined by each SD application.

3.11.1 Device Requirements and Features

Each CPRM compliant device that supports "additional ID Binding" operation must follow the protocols described in this section in addition to those of section 3.4. In addition,

- In the case of supporting "Set ID Binding," each set contains a unique Set ID (ID_s), which is placed in the write-protected area of the set.
- In the case of supporting "Holder ID Binding," each holder (purchaser) has a unique Holder ID (ID_h). Holder ID (ID_h) is usually placed in the write-protected area of "secure portable module" that can be inserted to each set owned by the holder (purchaser).

3.11.2 CPRM Components

CPRM components used for "additional ID Binding" include those described in section 3.3. So, refer to both section 3.3 and the CPRM Components section in each application specific part of *CPRM SD Memory Card Book*.

3.11.3 Content Encryption and Decryption Protocol for Additional ID Binding

Figure 3-14 illustrates an example process for content encryption and decryption using additional ID binding. As shown in Figure 3-14, the process of "additional ID binding" is almost same as that described in the chapter 3.1. The difference between these processes is to add steps (4a) and (4b) in Figure 3-14. This figure shows the case where CCI is defined. In the case where UR (Usage Rules) is defined, similar process is for content encryption and decryption is applicable, i.e.

1) CCI at step (5a), (5b) is replaced with UR (Usage Rules),
2) C2_E at step (5a) is replaced with C2_ECBC, and
3) C2_D at step (5b) is replaced with C2_DCBC,

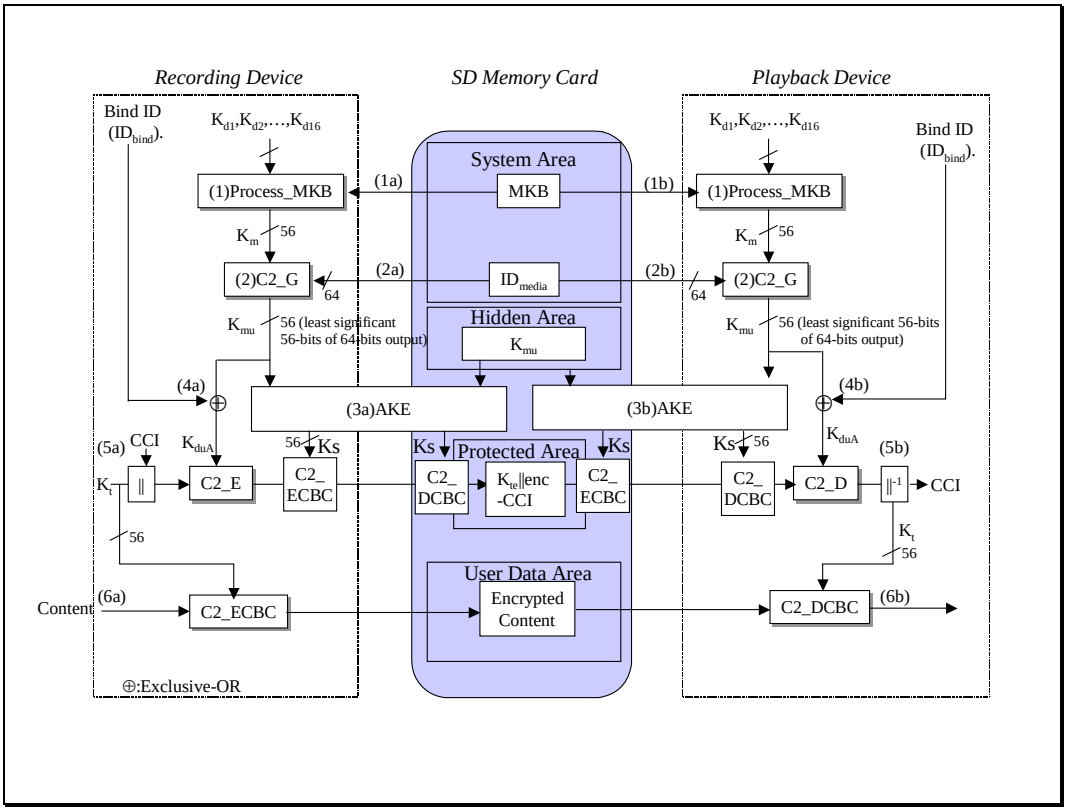

Figure 3-14 – Content Encryption and Decryption on additional ID Binding

The SD Memory Card and the accessing device (Recording Device, Playback Device) process as follows:

-(1) The accessing device executes Process_MKB

(1a, 1b) Calculate Media Key from MKB using Device Keys (see chapter 3 in the *Introduction and Common Cryptographic Elements* book of this specification)

-(2) The accessing devices executes the C2_G process

(2a, 2b) Calculate Media Unique Key (K_{mu}) from Media Key and Media Identifier (see chapter 3 in the *Introduction and Common Cryptographic Elements* book of this specification)

-(3) AKE process

(3a, 3b) If the AKE process succeeds, the Session Key (K_s), which is randomly generated in each AKE Process, is shared between Recording Device/Playback Device and SD Memory Card. (The detail of AKE Process is shown in the section 3.4.1)

-(4) Generate Device Unique Key process

(4a, 4b) Device Unique Key (K_{du}) is calculated as:

Device Unique Key (K_{du})= Media Unique Key (K_{mu}) $\oplus$ Bind ID (ID_{bind}).

-(5a) Encrypt Title Key and CCI process.

When the content is encrypted, a Title Key is picked at random. The Recording Device concatenates the Title Key (K_t) and CCI (Copy Control Information) and then encrypts them together using the Device Unique Key (K_{du}) with C2_E (the C2 cipher algorithm in ECB mode) described in the *Introduction and Common Cryptographic Elements* book of this specification. Then, the Encrypted Title Key and CCI are further encrypted by the Session Key (K_s) , which is shared at step (3a), using the C2_ECBC (C2 cipher algorithm in C-CBC mode) described in the *Introduction and Common Cryptographic Elements* book of this specification. The doubly-encrypted Encrypted Title Key and CCI are sent to the SD Memory Card. In the SD Memory Card, they are decrypted by the Session Key (K_s), which is shared at step (3a), using the C2_DCBC, and those results (Encrypted Title Key and CCI) are stored in the Protected Area.

-(5b) Decrypt Encrypted Title Key and CCI process.

The Encrypted Title Key (K_t) and CCI are encrypted by the SD Memory Card using the Session Key (K_s) , which is shard at step (3b), using the C2_ECBC (C2 cipher algorithm in C-CBC mode) described in the *Introduction and Common Cryptographic Elements* book of this specification. The doubly-encrypted Encrypted Title Key and CCI are sent to the Playback Device. Then, in the Playback Device, they are decrypted by the Session Key (K_s), which is shard at step (3b), using the C2_DCBC, and those results (Encrypted Title Key and CCI) are decrypted using the Device Unique Key (K_{du}) with C2_D (the C2 cipher algorithm in ECB mode) described in the *Introduction and Common Cryptographic Elements* book of this specification.

-(6a) Encrypt content process

The Recording Device shall protect each piece of content by encrypting it using the Title Key with C2_ECBC (C2 cipher algorithm in C-CBC mode) described in the *Introduction and Common Cryptographic Elements* book of this specification. Note that if the content delivered to the Recording Device is already encrypted in this way, the Recording Device does not perform this encryption step. It then sends it to the SD Memory Card, and stores it in the User Data Area.

-(6b) Decrypt encrypted content process.

The Playback Device uses the Title Key decrypted at step (4b) to decrypt encrypted content using C2_DCBC (C2 cipher algorithm in C-CBC mode) described in the *Introduction and Common Cryptographic Elements* book of this specification. The confidentiality of the Decrypted content must be maintained, as indicated in the Robustness Rules section of the CPRM License Agreement.

In Figure 3-14,

1) In the case of Set ID binding, Recording Device and Playback Device are identical.
2) In the case of Holder ID binding, the content is played back on each device, which is owned by a holder (purchaser) of that content. Therefore, Recording Device and Playback Device are not always identical but the same secure portable module that has same Holder ID shall be inserted to each device owned by a holder (purchaser).

3.12 Enhanced Version of CPRM (AES-CPRM)

The original CPRM (C2-CPRM) provides content protection with C2-cipher throughout the scheme. An enhanced version of CPRM (AES-CPRM) protects Content, Title Keys/Content Keys and CCI/Usage Rules with the AES cipher, although remaining parts are identical with the original CPRM. Additional functions based on AES cipher for implementing the AES-CPRM are described in Chapter 4 of *Introduction and Common Cryptographic Elements* book of this specification.

For accessing the Protected Area of the SD Memory Card, a 56-bit Media Unique Key (K_{mu}) is utilized the same as the original CPRM. For protecting Title Keys and CCI/Usage Rules, the Media Unique Key (K_{mu}) is expanded to a 128-bit Media Unique Key (K_{emu}) and encrypts these with the AES cipher using the Expanded Media Unique Key. Content is protected and encrypted with AES cipher using the 128-bit Title Key. Note that the Expanded Media Unique Key shall be treated as Highly Confidential, as defined in the CPRM License Agreement.

This section specifies additional details of AES-CPRM. Note that applications that adopt this AES-CPRM are specified in their application part book of this specification. Otherwise, AES-CPRM shall not be applied to the application.

Figure 3-15 illustrates an example process for content encryption and decryption on the SD Memory Card using AES-CPRM. This figure shows the case where UR is defined and assuming that CCI is included in UR. The details are described in each application specific part of the *CPRM Specification SD Memory Card Book*.

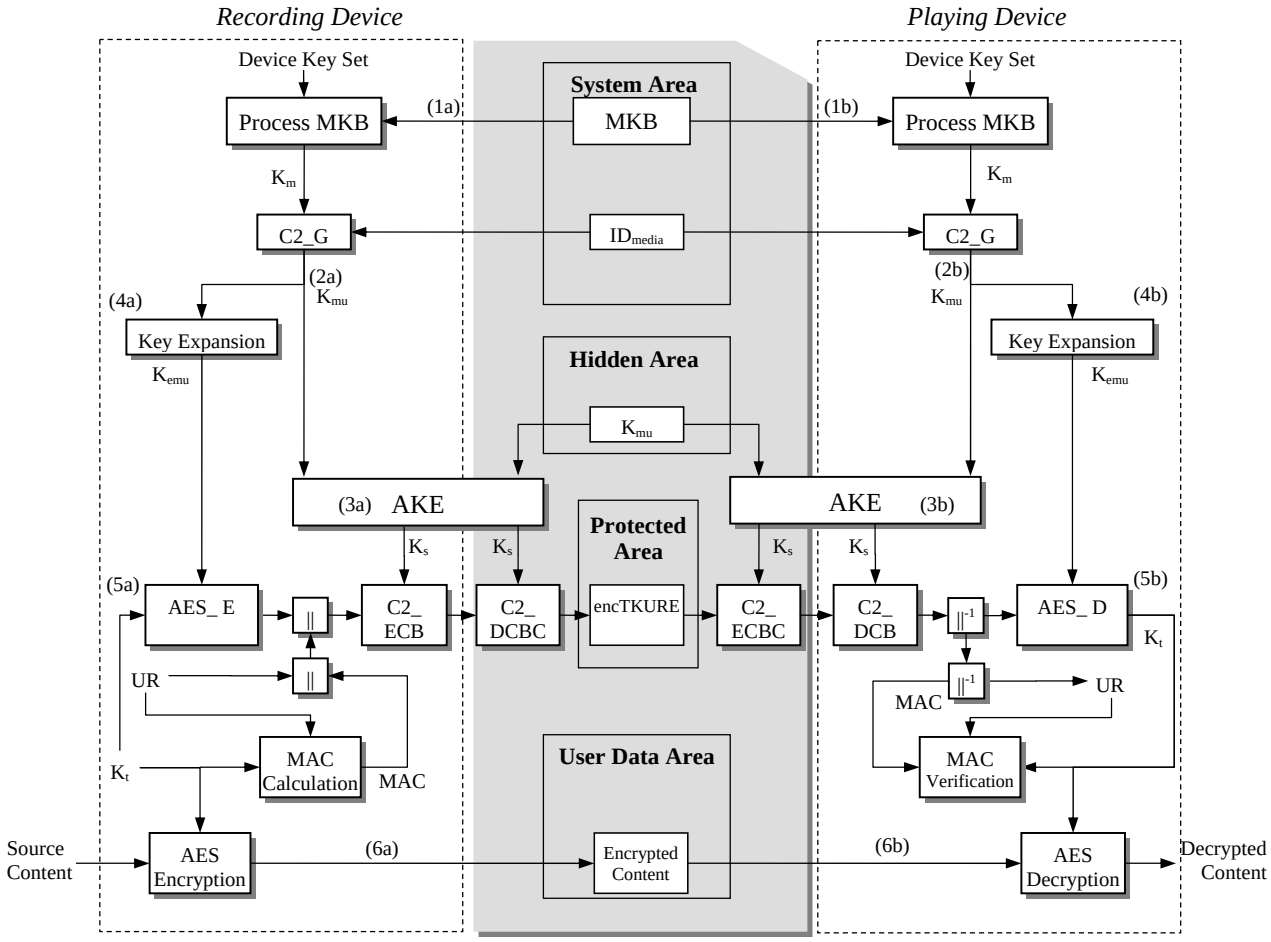

Figure 3-15 – AES-CPRM Content Encryption and Decryption

The SD Memory Card and the accessing device (Recording Device / Playback Device) authenticate each other, and encrypt or decrypt content as follows:

- (1) The accessing device executes Process_MKB

  (1a, 1b) Calculate Media Key from MKB using Device Keys (see chapter 3 in the *Introduction and Common Cryptographic Elements* book of this specification)

- (2) The accessing devices execute the C2_G process

  (2a, 2b) Calculate Media Unique Key (K_{mu}) from Media Key (K_m) and Media Identifier (ID_{media}) (see chapter 3 in the *Introduction and Common Cryptographic Elements* book of this specification)

- (3) AKE process

  (3a, 3b) If the AKE process succeeds, the Session Key (K_s), which is randomly generated in each AKE Process, is shared between Recording Device/Playback Device and SD Memory Card. (The detail of AKE Process is shown in 3.4.1)

- (4) The accessing devices execute Key Expansion Process

(4a, 4b) Calculate Expanded Media Unique Key (K_{emu}) from the Media Unique Key (K_{mu}) and other confidential value. The detail of the Key Expansion Process is specified in the application specific part of the *CPRM Specification SD Memory Card Book*.

- (5a) Encrypt Title Key and Usage Rules process

When the content is encrypted, a Title Key is picked at random. The Recording Device calculates a 16-byte MAC value from the Usage Rules using the Title Key with CMAC (the Cipher-based Message Authentication Code) described in the *Introduction and Common Cryptographic Elements* book of this specification. The Recording Device encrypts the Title Key using the Expanded Media Unique Key (K_{emu}) with AES_E (the AES cipher algorithm in ECB mode) described in the *Introduction and Common Cryptographic Elements* book of this specification. Then the Recording Device concatenates the encrypted Title Key (K_t), the UR (Usage Rules) and the MAC value as a TKURE. Then, the TKURE are further encrypted by the Session Key (K_s), which is shared at step (3a), using the C2_ECBC (C2 cipher algorithm in C-CBC mode) described in the *Introduction and Common Cryptographic Elements* book of this specification. The C2-encrypted TKURE are sent to the SD Memory Card. In the SD Memory Card, they are decrypted by the Session Key (K_s), which is shared at step (3a), using the C2_DCBC, and those results (the TKURE) are stored in the Protected Area.

- (5b) Decrypt Encrypted Title Key and Usage Rules process

The TKURE including an Encrypted Title Key (K_t) , UR and the MAC value are encrypted by the SD Memory Card using the Session Key (K_s), which is shared at step (3b), using the C2_ECBC (C2 cipher algorithm in C-CBC mode) described in the *Introduction and Common Cryptographic Elements* book of this specification. The C2-encrypted TKURE are sent to the Playback Device. Then, in the Playback Device, they are decrypted by the Session Key (K_s), which is shared at step (3b), using the C2_DCBC. The Playback Device decrypts the AES-encrypted Title Key using the Expanded Media Unique Key (K_{emu}) with AES_D (the AES cipher algorithm in ECB mode) described in the *Introduction and Common Cryptographic Elements* book of this specification. Then the Playback Device gets the decrypted Title Key and the Usage Rules. Then the Playback Device verifies the MAC value from the Usage Rules using the Title Key with CMAC (the Cipher-based Message Authentication Code) described in the *Introduction and Common Cryptographic Elements* book of this specification. If the verification fails, the Playback Device shall abort the entire process.

- (6a) Encrypt content process

The Recording Device shall protect each piece of content by encrypting it using the 128-bit Title Key (K_t) with AES_ECBC or AES_ECTR described in the *Introduction and Common Cryptographic Elements* book of this specification. Note that if the content delivered to the Recording Device is already encrypted in this way, the Recording Device does not perform this encryption step. It then sends it to the SD Memory Card, and stores it in the User Data Area.

- (6b) Decrypt encrypted content process

The Playback Device uses the 128-bit Title Key (K_t) decrypted at step (4b) to decrypt the encrypted content using AES_DCBC or AES_DCTR described in the *Introduction and Common Cryptographic Elements* book of this specification.