Content Protection for Recordable Media Specification

SD Memory Card Book
SD-SD (Separate Delivery)
Audio Profile Part

Intel Corporation
International Business Machines Corporation
Matsushita Electric Industrial Co., Ltd.
Toshiba Corporation

Revision 0.9
May 15, 2007

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, MEI, 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.

Contact Information

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

- Licensing inquiries and requests should be addressed to cprm-licensing@4Centity.com.
- Feedback on this specification should be addressed to cprm-comment@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

List of Figures

This page is intentionally left blank.

List of Tables

This page is intentionally left blank.

Chapter 1
Introduction

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 comprised of 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-Sound, SD-ePublish, SD-Image, SD-Video, SD-Binding, SD-SD)*

This document is the *SD-SD (Separate Delivery) Part* of the *SD Memory Card Book*, and describes details of CPRM that are specific to the SD-SD Audio format.

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 use of CPRM to protect SD-SD Audio content

1.3. References

This specification shall be used in conjunction with the following documents. When the documents 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 1.0*

4C Entity, LLC, *CPRM Specification: SD Memory Card Book Common Part, Revision 0.96*

4C Entity, LLC, *CPRM Specification: SD Memory Card Book Audio Part, Revision 0.96*

4C Entity, LLC, *CPRM Specification: SD Memory Card Book SD-SD (Separate Delivery) Part, Revision 0.90*

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

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

SD Association, *SD Memory Card Specifications, Part 15: SD-SD (Separate Delivery) Specification, Version 1.0*

SD Association, *SD Memory Card Specifications, Part 15: Audio Profile Specifications, Addendum to Separate Delivery Specification, Version 1.0*

CPRM Specification SD Memory Card Book Common Part describes the general CPRM technology for SD Memory Card and all SD applications. *CPRM Specification: SD Memory Card Book SD-SD (Separate Delivery) Part* describes how to handle an SD-SD Key. This book describes how to protect SD-SD Audio content using SD-SD Keys. Export to SD-Audio process in this book requires *CPRM Specification: SD Memory Card Book Audio Part*. For your information, Figure 1-1 is the specifications structure.

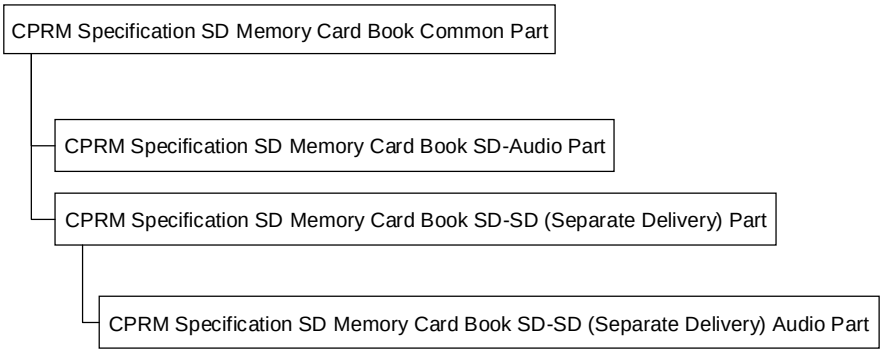


Figure 1-1 Specification structure for SD-SD Audio

1.4. 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.

In addition, this specification uses two other representations for numerical values. Binary numbers are represented as a string of binary (0, 1) digits followed by a suffix ‘b’ (e.g., 1010b). Hexadecimal numbers are represented as a string of hexadecimal (0..9, A..F) digits followed by a suffix ‘h’ (e.g., 3C2h).

Chapter 2
Abbreviations and Acronyms

2. Abbreviations and Acronyms

The following abbreviations and acronyms are used in this document:

4C	4 Companies (IBM, Intel, MEI, and Toshiba)
C-CBC	Converted Cipher Block Chaining
C2	Cryptomeria Cipher
CKI	Content Key Information
CKMG	Content Key Manager
CPRM	Content Protection for Recordable Media
ECKUR	Encrypted Content Key and Usage Rule
ID	Identifier
LLC	Limited Liability Company
MKB	Media Key Block
SD	Secure Digital
UKURE	User Key & Usage Rule Entry
UKURE_SRN	UKURE Search Number
UKURMG	User Key & Usage Rule Manager
UKURMMG	User Key & Usage Rule Master Manager
UR_A	Usage Rules for Audio

Chapter 3
CPRM for SD-SD (Separate Delivery) Audio

3. CPRM for SD-SD (Separate Delivery) Audio

3.1. Introduction

This chapter specifies details for using CPRM to protect SD-SD Audio content and dscribes details on using CPRM to realize some features. Regarding the SD-SD Audio Profile, refer to *SD Memory Card Specifications – Part15 Audio Profile Specifications Addendum to SD-SD Specifications.*

3.2. Device Requirements

Regarding the Device Requirements, refer to Section 3.2 of *SD Memory Card Book Common Part.*

3.3. CPRM Components

Regarding the CPRM Components, refer to Section 3.3 of *SD Memory Card Book Common Part.*

3.4. SD-SD Key data format for SD-SD Audio

This section describes parameters included in Content Key Information and User Key.

3.4.1. Usage Rules for Audio

This section describes Usage Rules for Audio (UR_A) which defines specific usage rules for Audio Profile. UR_A is set in Reserved for Profiles in Encrypted Content Key and Usage Rule (ECKUR). Regarding ECKUR, refer to *CPRM Specification SD Memory Card Book SD-SD (Separate Delivery) Part.*

As shown in Table 3-1, UR_A consists of Trigger Bits for Audio Profile Processes, Current Fields Group for Audio, Initial Fields Group for Audio and Information for Export to SD-Audio. Trigger Bits for Audio Profile Processes is corresponding to UR_PF_TRIGGER in Reserved for Profile, Current Fields Group for Audio is corresponding to UR_PF_CURRENT, and Initial Fields Group for Audio is corresponding to UR_PF_INITIAL respectively.

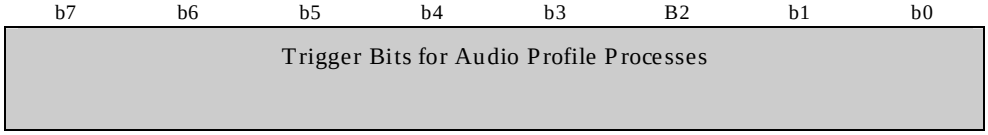
Table 3-1 Usage Rules for Audio

(Description order)

RBP	Field Name	Contents	Number of bytes
0	UR_A_TRIGGER	Trigger Bits for Audio Profile Processes	1 byte
1 to 2	UR_A_CURRENT	Current Fields Group for Audio	2 bytes
3 to 4	UR_A_INITIAL	Initial Fields Group for Audio	2 bytes
5 to 6	UR_A_EXSDA_INFO	Information for Export to SD-Audio	2 bytes
7 to 9	Reserved	Reserved	3 bytes
Total			10 bytes

(RBP 0) UR_A_TRIGGER

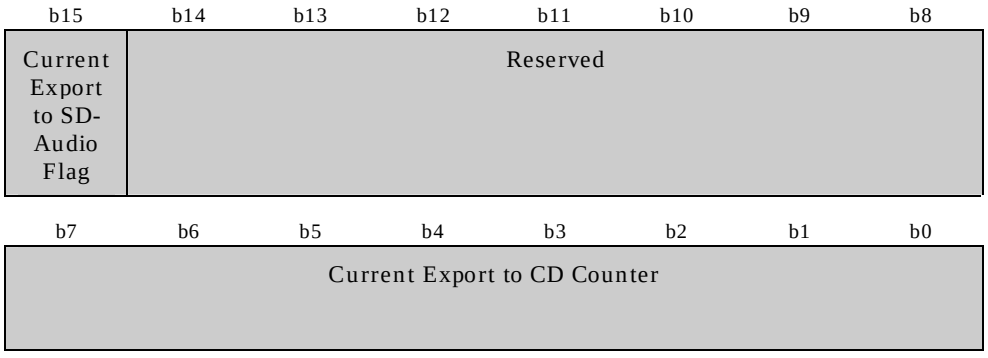
This field describes Trigger Bits for Audio Profile Processes.



Trigger Bits for Audio Profile Processes	...	00000000b: Accessing devices conforming to this specification can control the processes described in 3.6
		00000001b~11111111b: Accessing devices conforming to this specification shall not be permitted the processes described in 3.6.
		Accessing devices conforming to this specification shall always set this value to '00000000b' as appropriate, when writing an encrypted content to an SD Memory Card.
		In a future version, the Usage Rules may be expanded, or other information for controlling playback processes may be added. Accessing devices of the future version shall process the new information for controlling processes correctly when this bit is set to the value except '00000000b.'

(RBP 1 to 2) UR_A_CURRENT

This field describes Current Fields Group for Audio. This filed consists of Current Export to SD-Audio Flag and Current Export to CD Counter.



Current Export to SD-Audio Flag ... 0b: Export to SD-Audio is not permitted.

1b: Export to SD-Audio is permitted.

Current Export to CD Counter ... 00h: Export to CD is never permitted.

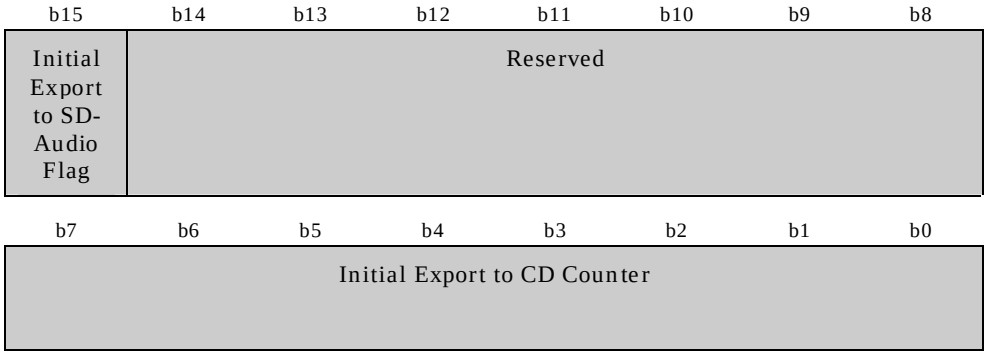
01h~FEh: Export to CD is permitted specified times.

FFh: Export to CD is permitted unlimited times.

This field may change when the corresponding content is exported. This field shall not be inherited to a replicated content when copying. For details on how conforming devices shall change this field, refer to the Export process described in this book.

(RBP 3 to 4) UR_A_INITIAL

This field describes Initial Fields Group for Audio. This filed consists of Initial Export to SD-Audio Flag and Initial Export Counter.



Initial Export to SD-Audio Flag ... 0b: Export to SD-Audio is not permitted.

1b: Export to SD-Audio is permitted.

Initial Export to CD Counter ... 00h: Export to CD is never permitted.

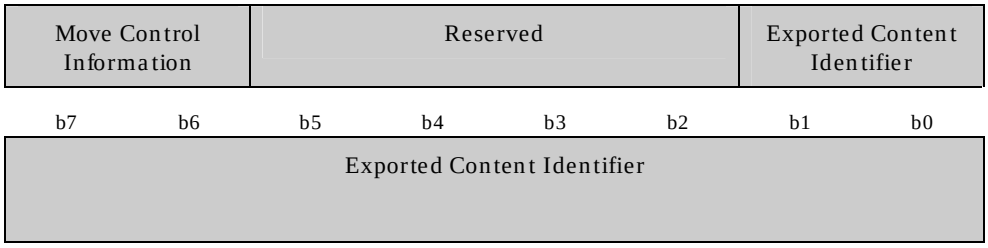
01h~FEh: Export to CD is permitted specified times.

FFh: Export to CD is permitted unlimited times.

This field is set when the corresponding content is distributed. It never changes even when the content is viewed. This field shall be inherited to a replicated content when copying.

(RBP 5 to 6) UR_A_EXSDA_INFO

This field describes Information for Export to SD-Audio Processes. This filed consists of Move Control Information and Exported Content Identifier.



Move Control Information ... When the content is exported, exporting device shall store the Current Move Control Information in this CKI.

Exported Content Identifier ... When the content is exported, exporting device shall store the Content ID of the content stored in SD-Audio.

When the content is not exported, this field shall be set to '0000000000b'.

3.4.2. User Key Type

SD-SD specification prepares two types of User Key. The type describes whether or not a device executes the Hash Calculation Process described in *CPRM Specification SD Memory Card Book SD-SD (Separate Delivery) Part*. When the value of User Key Type is 0b, all CKIs encrypted with the User Key are handled with the hash calculation in processes described in Section 3.6. On the other hand, when User Key Type is 1b, all content encrypted with the User Key are handled without the hash calculation in processes. Regarding usage rule, content encrypted with the User Key whose type is 1b have some restrictions. Use of dynamic Usage Rules for Audio is prohibited. As shown in Table 3-2, some fields in Usage Rules for Audio are restricted. The device shall not set each field to other than the value on this table.

Table 3-2 Restriction of Usage Rules for Audio

Field Name	Restriction
Current Export to SD-Audio Flag	0b
Current Export to CD Counter	00h or FFh

These parameters are not updated once the content key is stored. Note that a device can not securely erase a content key from CKMG file encrypted with User Key whose type is 1b.

3.5. Content Encryption and Decryption Format

SD-SD Audio Profile treats Audio data stream in Audio Unit, Picture data stream in Picture Unit and Text data stream in Text Unit.

Regarding the general principle for Content Encryption and Decryption format, refer to section 3.6 of *CPRM Specification: SD Memory Card Book Common Part.*

In addition, the following sub-section applies.

3.5.1. Audio Unit Encryption

3.5.1.1. AAC Audio Encryption

SD-SD Audio Profile application treats the AAC data stream. The AAC data stream is encrypted by the Content Key as follows:

- The SD-SD Audio Profile format defines an 8-byte header (AU_HEAD) for the Audio Unit containing the AAC data stream. The header (AU_HEAD) is kept unencrypted.
- The Audio Unit contains AAC data stream in the area of Audio Unit Data (AU_DATA). Table 3-3 shows the structure of Audio Unit.

Table 3-3 Audio Unit structure

Bit / Byte	7	6	5	4	3	2	1	0
0	**Header Part (AU_HEAD)** - This area contains header information for AU_DATA. (Non-encrypted)							
1								
7								
8	**Data Part (AU_DATA)** - This area contains AAC data stream.							
9								
N-1								

- The AAC data stream consists of multiple audio frames.
- Each frame of an AAC data stream is encrypted by the Content Key.
- Each frame consists of a header part (fixed to 7 bytes) and data part (variable size N=4~2^{13}-1).
- Each frame starts a new C-CBC mode cipher chain.
- Only the data part is encrypted as follows:
  -If the data part is 8 bytes or more (N=8~2^{13}-1), the data part is encrypted using C-CBC mode. The last residual block, if it is less than 8 bytes, is not encrypted
  -If the data part is 7 bytes or less (N=4~7), no encryption is performed.

Table 3-4 through Table 3-6 shows the encrypted AAC frame format.

Table 3-4 Encrypted AAC frame format without residual block (N=8*n)

Bit / Byte	7	6	5	4	3	2	1	0
0	Header Part (Non-Encrypted)							
1								
6								
7	Data Part (Encrypted)							
8								

N+6	

Table 3-5 Encrypted AAC frame format with residual block (N=8*n+m, m<8)

Bit / Byte	7	6	5	4	3	2	1	0
0	Header Part (Non-Encrypted)							
1								
6								
7	Data Part (Encrypted)							
8								
8n+6								
8n+7	Residual block of Data Part (Non-Encrypted)							
N+6								

Table 3-6 AAC frame format in the case Data Part is less than 8 bytes (N<8)

Bit / Byte	7	6	5	4	3	2	1	0
0	Header Part (Non-Encrypted)							
1								
6								
7	Data Part (Non-Encrypted)							
8								
N+6								

3.5.2. Picture Unit Encryption

3.5.2.1. JPEG Encryption

SD-SD Audio Profile application treats the JPEG data stream. The JPEG data stream is encrypted by the Content Key as follows:

- The SD-SD Audio Profile format defines an 8-byte header (PU_HEAD) for the Picture Unit containing the JPEG data. The header (PU_HEAD) is kept unencrypted.
- The Picture Unit contains JPEG data stream in the area of Picture Data in Picture Unit Data (PU_DATA). The area of Picture Unit Data (PU_DATA) except for Picture Data (JPEG data stream) is kept unencrypted. Table 3-7 shows the structure of Picture Unit.

Table 3-7 Picture Unit structure

Bit / Byte	7	6	5	4	3	2	1	0
0	**Header Part (PU_HEAD)** - This area contains header information for PU_DATA (Non-encrypted.)							
1								
7								
8	**Data Part (PU_DATA)** - This area contains JPEG data stream.							
9								
N-1								

- The Picture Data (JPEG data stream) is encrypted using C2 in C-CBC mode. There is no break in the cipher chaining.
- The data is encrypted as follows:

  -If the data is 8 bytes or more, the data is encrypted using C-CBC mode. The last residual block, if it is less than 8 bytes, is not encrypted

Table 3-8 through Table 3-9 shows the encrypted JPEG format.

Table 3-8 Encrypted JPEG format without residual block (N=8*n)

Bit / Byte	7	6	5	4	3	2	1	0
0	Picture Data (Encrypted)							
1								
N-1								

Table 3-9 Encrypted JPEG format with residual block (N=8*n+m, m<8)

Bit / Byte	7	6	5	4	3	2	1	0
0	Picture Data (Encrypted)							
1								
8n-1								
8n	Residual block of Picture Data (Non-Encrypted)							

N-1	

3.5.3. Text Unit Encryption

3.5.3.1. Text Encryption

SD-SD Audio Profile application treats the Text data stream. The Text data stream is encrypted by the Content Key as follows:

- The SD-SD Audio Profile format defines an 8-byte header (TU_HEAD) for the Text Unit containing the Text data. The header (TU_HEAD) is kept unencrypted.
- The Text Unit contains Text data stream in the area of Text Data in Text Unit Data (TU_DATA). The area of Text Unit Data (TU_DATA) except for Text Data (Text data stream) is kept unencrypted. Table 3-10 shows the structure of Text Unit.

Table 3-10 Text Unit structure

Bit / Byte	7	6	5	4	3	2	1	0
0	**Header Part (TU_HEAD)** - This area contains header information for TU_DATA. (Non-encrypted)							
1								
7								
8	**Data Part (TU_DATA)** - This area contains Text data stream.							
9								
N-1								

- The Text Data (Text data stream) is encrypted using C2 in C-CBC mode. There is no break in the cipher chaining.
- The data is encrypted as follows:

  -If the data is 8 bytes or more, the data is encrypted using C-CBC mode. The last residual block, if it is less than 8 bytes, is not encrypted

  -If the data part is 7 bytes or less, no encryption is performed.

Table 3-11 through Table 3-13 shows the encrypted Text format.

Table 3-11 Encrypted Text data without residual block (N=8*n)

Bit / Byte	7	6	5	4	3	2	1	0
0	Text Data (Encrypted)							

1	
N-1	

Table 3-12 Encrypted Text data with residual block (N=8*n+m, m<8)

Bit / Byte	7	6	5	4	3	2	1	0
0	Text Data (Encrypted)							
1								
8n-1								
8n	Residual block of Text Data (Non-Encrypted)							
N-1								

Table 3-13 Text data in the case Data Part is less than 8 bytes (N<8)

Bit / Byte	7	6	5	4	3	2	1	0
0	Text Data (Non-Encrypted)							
1								
N-1								

3.6. Process Description for Audio Profiles

This section describes Export to CD, Export to SD-Audio and Reimport from SD-Audio processes.

- Export to CD Process

Specifies how an exporting device starts to export CPRM protected Content to a CD media as CD-Audio content . When the content is allowed to execute this process, a user can make a CD including the content.

- Export to SD-Audio Process

Specifies how an exporting device stores a title key of SD-Audio which is the same as of Content Key on an SD Memory Card. Using this function, a user can playback the content both SD-SD Audio format and SD-Audio format in the SD Memory Card. Note that the SD-SD Audio content shall not be moved (LOCKED) during exporting to SD-Audio because the copied content is made.

- Reimport from SD-Audio Process

Specifies how a reimporting device erases exported title key of SD-Audio. In this process, the exported SD-Audio content is removed and at the same time the SD-SD content turns into be movable (UNLOCKED) when the SD-SD content is originally movable.

For the sake of readability, some flowcharts are added to processes as an example of process flow. A parenthetic number on a box in flowcharts shows which step an action or bifurcation described inside the box is done in.

In these processes, when a device updates a CKMG file, devices may update two or more CKIs from a CKMG at one process. For example, in deleting process, a device may delete all or selected CKIs in a CKMG at one process.

3.6.1. Export to SD-Audio Process

When the Current Export to SD-Audio flag of an SD-SD Content is 1b, the SD-SD Content is permitted to be stored in the same SD Memory Card as an SD-Audio Content.

(1) Determine the CKMG file and CKI associated with the Content Key to be exported.

The Exporting Device determines the CKMG filename and the CKI.

(2) Read the CKMG file from the SD Memory Card.

The Exporting Device reads the CKMG file from the SD Memory Card and holds it as the temporary CKMG image.

Then, the Exporting Device checks the corresponding CKI Used flag in the temporary CKMG image. If it is equal to '0b,' the process shall be aborted.

Otherwise, the Exporting Device obtains the selected CKI in the temporary CKMG image.

(3) Determine the UKURMG file and UKURE associated with SD-SD content to be exported.

(3.1) Obtain UKURE_SRN.

The Exporting Device obtains the UKURE_SRN ***s*** associated with the SD-SD content to be exported.

(3.2) Determine the UKURMG file and UKURE associated with the SD-SD content to be exported.

The Exporting Device determines the UKURMG filename and the UKURE using the following formula:

s = (***n*** - 1) * 250 + ***m*** (***n***: UKURMG file number, ***m***: UKURE number in a UKURMG)

$1 \leq \boldsymbol{m} \leq 250, 1 \leq \boldsymbol{n} \leq 256$

For example, when the UKURE_SRN is 1020, the UKURMG filename shall be "SDSD0005.KEY" (the fifth UKURMG file) and the UKURE shall be the twentieth entry in the "SDSD0005.KEY."

(4) Read the UKURMG file from the SD Memory Card.

The Exporting Device securely reads the ***n***th UKURMG file from the SD Memory Card using Secure Read Process and holds it as the temporary UKURMG image.

Then, The Exporting Device checks the ***m***th UKURE Used flag in the temporary UKURMG image. If it is equal to '0b,' the process shall be aborted.

Otherwise, The Exporting Device obtains the ***m***th UKURE in the temporary UKURMG image.

(5) Check the UKURE in the temporary UKURMG image (Phase 1).

The Exporting Device decrypts the UKURE using the UKURE Decryption process and securely holds it as the decrypted UKURE image. The Exporting Device checks this decrypted UKURE image as follows:

- If the Check Value is not '0123456789ABCDEFh,' the process shall be aborted.
- If the Trigger Bits is not equal to '00h,' the process shall be aborted.
- If the User Key Type in the UKURE is equal to '0b', the Exporting Device checks the Hash Value in UKURE. If the stored Hash Value in UKURE is not equal to the calculated value from the temporary CKMG image using Hash Calculation Process, the device shall execute CKMG Recovery Process described in *CPRM Specification SD Memory Card Book SD-SD (Separate Delivery) Part*.
- If the User Key Type in the UKURE is equal to '1b', the process shall be aborted.

(6) Check the CKI in the temporary CKMG image.

The Exporting Device decrypts the CKI using the CKI Decryption process and securely holds it as the decrypted CKI image. The Exporting Device checks this decrypted CKI image as follows:

- If the Check Value is not '0123456789ABCDEFh,' the process shall be aborted.
- If the Trigger Bits for Audio Profile Processes is not equal to '00h,' the process shall be aborted.
- If Current Exporting to SD-Audio Flag is equal to '0b,' then the process shall be aborted.
- If Exported Content Identifier is not equal to '0000000000b,' the process shall be aborted.

(7) Obtain the Content ID for SD-Audio.

The Exporting Device shall execute the step (1) and (2) of Recording Process described in section 3.8.1, *CPRM SD Memory Card book SD-AudioPart.* In this Recording Process, the title key to be recorded shall be the same value of the content key. The CCI to be recorded shall be set to '11b' (No more copying is permitted.) The content to be recorded as SD-Audio format shall not be recorded as movable. After executing these steps, the Exporting Device obtains the Content ID for SD-Audio. If the Exporting Device can not obtain the Content ID for SD-Audio, then the process shall be aborted.

(8) Update the CKI in the temporary CKMG image.

The Exporting Device updates the CKI in the temporary CKMG image as follows:

- The Exported Content Identifier is set to the obtained Content ID for SD-Audio.
- The Move Control Information field is set to the same value as that of the Current Move Control Information field.

- The Current Move Control Information field is set to '00b.'

After all the fields in the CKI are set as above, the Exporting Device encrypts the CKI in the temporary CKMG image using the CKI Encryption process.

(9) Update the temporary UKURMG image.

The Exporting Device updates the UKURE in the temporary UKURMG image. The Hash Value in the UKURE is set to the value that is calculated for the temporary CKMG image using Hash Calculation Process. Then the Exporting Device encrypts the UKURE in the temporary UKURMG image using the UKURE Encryption process.

(10) Write the temporary UKURMG and CKMG images to the SD Memory Card.

The Exporting Device securely writes the updated temporary UKURMG and CKMG images as the updated UKURMG and CKMG files to the SD Memory Card using the CKMG Update Process in described in *CPRM Specification SD Memory Card Book SD-SD (Separate Delivery) Part.* Then the Exporting Device securely reads the updated UKURMG file from the SD Memory Card using the Secure Read Process and verifies that the update of the ***m***th UKURE in the UKURMG file has completed successfully.

If the verification of the UKURMG file fails, the Exporting Device shall abort this process.

(11) Start to Export to SD-Audio

The Exporting Device exports the Content Key into the Title Key, and then executes the remained Recording Process step (3) described in *CPRM SD Memory Card book SD-Audio Part.*

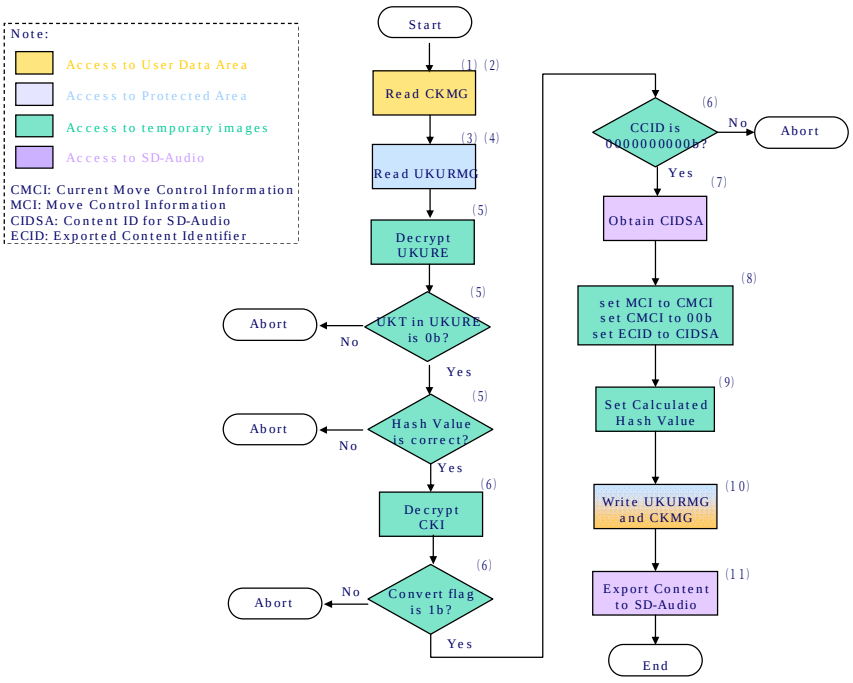


Figure 3-1 Flowchart of Export to SD-Audio Process

3.6.2. Reimport from SD-Audio Process

The Reimporting Device securely holds the Content ID for SD-Audio of the Title Key to be reimported.

(1) Determine the CKMG file and CKI associated with the Content Key to be reimported.

The Reimporting Device determines the CKMG filename and the CKI.

(2) Read the CKMG file from the SD Memory Card.

The Reimporting Device reads the CKMG file from the SD Memory Card and holds it as the temporary CKMG image.

Then, the Reimporting Device checks the corresponding CKI Used flag in the temporary CKMG image. If it is equal to '0b,' the process shall be aborted.

Otherwise, the Reimporting Device obtains the selected CKI in the temporary CKMG image.

(3) Determine the UKURMG file and UKURE associated with SD-SD content to be reimported.

(3.1) Obtain UKURE_SRN.

The Reimporting Device obtains the UKURE_SRN ***s*** associated with the SD-SD content to be reimported.

(3.2) Determine the UKURMG file and UKURE associated with the SD-SD content to be reimported.

The Reimporting Device determines the UKURMG filename and the UKURE using the following formula:

$s = (n - 1) * 250 + m$ (***n***: UKURMG file number, ***m***: UKURE number in a UKURMG)

$1 \leq m \leq 250, 1 \leq n \leq 256$

For example, when the UKURE_SRN is 1020, the UKURMG filename shall be "SDSD0005.KEY" (the fifth UKURMG file) and the UKURE shall be the twentieth entry in the "SDSD0005.KEY."

(4) Read the UKURMG file from the SD Memory Card.

The Reimporting Device securely reads the ***n***th UKURMG file from the SD Memory Card using Secure Read Process and holds it as the temporary UKURMG image.

Then, The Reimporting Device checks the ***m***th UKURE Used flag in the temporary UKURMG image. If it is equal to '0b,' the process shall be aborted.

Otherwise, The Reimporting Device obtains the ***m***th UKURE in the temporary UKURMG image.

(5) Check the UKURE in the temporary UKURMG image.

The Reimporting Device decrypts the UKURE using the UKURE Decryption process and securely holds it as the decrypted UKURE image. The Reimporting Device checks this decrypted UKURE image as follows:

- If the Check Value is not '0123456789ABCDEFh,' the process shall be aborted.
- If the Trigger Bits is not equal to '00h,' the process shall be aborted.
- If the User Key Type in the UKURE is equal to '0b', the Reimporting Device checks the Hash Value in UKURE. If the stored Hash Value in UKURE is not equal to the calculated value from the temporary CKMG image using Hash Calculation Process, the device shall execute CKMG Recovery Process described in *CPRM Specification SD Memory Card Book SD-SD (Separate Delivery) Part*.
- If the User Key Type in the UKURE is equal to '1b', the process shall be aborted.

(6) Check the CKI in the temporary CKMG image.

The Reimporting Device decrypts the CKI using the CKI Decryption process and securely holds it as the decrypted CKI image. The Reimporting Device checks this decrypted CKI image as follows:

- If the Check Value is not '0123456789ABCDEFh,' the process shall be aborted.

- If the Trigger Bits for Audio Profile Processes is not equal to '00h,' the process shall be aborted.
- If Current Export to SD-Audio Flag is equal to '0b,' then the process shall be aborted.
- If Exported Content Identifier is equal to '0000000000b,' the process shall be aborted.

(7) Check the Title Key to be reimported.

The Reimporting Device checks the validity of the Title Key to be reimported as follows:

- The Exported Content Identifier in CKI associated with the Content Key to be reimported is not equal to the Content ID for SD-Audio of the Title Key to be reimported, the process shall be aborted.
- The Content Key to be reimported is not equal to the value of the Title Key to be reimported, the process shall be aborted.

(8) Update the CKI in the temporary CKMG image.

The Reimporting Device updates the CKI in the temporary CKMG image as follows:

- The Exported Content Identifier is set to '0000000000b.'
- The Current Move Control Information field is set to the same value as that of the Move Control Information field.

After all the fields in the CKI are set as above, the Reimporting Device encrypts the CKI in the temporary CKMG image using the CKI Encryption process.

(9) Update the temporary UKURMG image.

The Reimporting Device updates the UKURE in the temporary UKURMG image. The Hash Value in the UKURE is set to the value that is calculated for the temporary CKMG image using Hash Calculation Process. Then the Reimporting Device encrypts the UKURE in the temporary UKURMG image using the UKURE Encryption process.

(10) Delete the TKE in the TKMG file in SD Memory Card.

The Reimporting Device securely overwrites "the value for delete (random number)" to the first 8-bytes encrypted field (from b64 to b127) of TKE (including Title Key) associated with the Title Key to be reimported on the TKMG file, using the Secure Title Key Delete protocol described in *CPRM SD Memory Card book SD-Audio Part.*

(11) Write the temporary UKURMG and CKMG images to the SD Memory Card.

The Reimporting Device encrypts this decrypted UKURE image using the UKURE Encryption process, and sets the ***m***th UKURE in the temporary UKURMG image to the resulting value.

The Reimporting Device securely writes the updated temporary UKURMG and CKMG images as the updated UKURMG and CKMG files to the SD Memory Card using the CKMG Update Process in described in *CPRM Specification SD Memory Card Book SD-SD (Separate Delivery) Part.* Then the Reimporting Device securely reads the updated UKURMG file from the SD Memory Card using the Secure Read Process and verifies that the update of the ***m***th UKURE in the UKURMG file has completed successfully.

If the verification of the TKURMG file fails, the Reimporting Device shall abort this process.

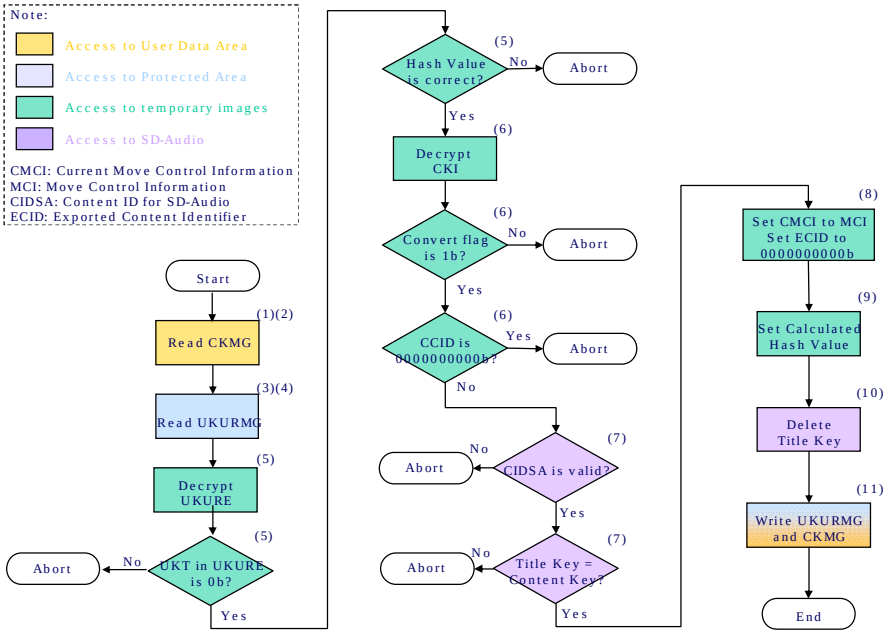


Figure 3-2 Flowchart of Reimport from SD-Audio Process

3.6.3. Export to CD Process

(1) Determine the CKMG file and CKI associated with the Content Key to be exported.

The Exporting Device determines the CKMG filename and the CKI.

(2) Read the CKMG file from the SD Memory Card.

The Exporting Device reads the CKMG file from the SD Memory Card and holds it as the temporary CKMG image.

Then, the Exporting Device checks the corresponding CKI Used flag in the temporary CKMG image. If it is equal to '0b,' the process shall be aborted.

Otherwise, the Exporting Device obtains the selected CKI in the temporary CKMG image.

(3) Determine the UKURMG file and UKURE associated with SD-SD content to be exported.

(3.1) Obtain UKURE_SRN.

The Exporting Device obtains the UKURE_SRN ***s*** associated with the SD-SD content to be exported.

(3.2) Determine the UKURMG file and UKURE associated with the SD-SD content to be exported.

The Exporting Device determines the UKURMG filename and the UKURE using the following formula:

$s = (n - 1) * 250 + m$ (***n***: UKURMG file number, ***m***: UKURE number in a UKURMG)

$1 \leq m \leq 250, 1 \leq n \leq 256$

For example, when the UKURE_SRN is 1020, the UKURMG filename shall be "SDSD0005.KEY" (the fifth UKURMG file) and the UKURE shall be the twentieth entry in the "SDSD0005.KEY."

(4) Read the UKURMG file from the SD Memory Card.

The Exporting Device securely reads the ***n***th UKURMG file from the SD Memory Card using Secure Read Process and holds it as the temporary UKURMG image.

Then, The Exporting Device checks the ***m***th UKURE Used flag in the temporary UKURMG image. If it is equal to '0b,' the process shall be aborted.

Otherwise, The Exporting Device obtains the ***m***th UKURE in the temporary UKURMG image.

(5) Check the UKURE in the temporary UKURMG image.

The Exporting Device decrypts the UKURE using the UKURE Decryption process and securely holds it as the decrypted UKURE image. The Recording Device checks this decrypted UKURE image as follows:

- If the Check Value is not '0123456789ABCDEFh,' the process shall be aborted.
- If the Trigger Bits is not equal to '00h,' the process shall be aborted.
- If the User Key Type in the UKURE is equal to '0b', the Exporting Device checks the Hash Value in UKURE. If the stored Hash Value in UKURE is not equal to the calculated value from the temporary CKMG image using Hash Calculation Process, the device shall execute CKMG Recovery Process described in *CPRM Specification SD Memory Card Book SD-SD (Separate Delivery) Part.*

(6) Check the CKI in the temporary CKMG image.

The Exporting Device decrypts the CKI using the CKI Decryption process and securely holds it as the decrypted CKI image. The Exporting Device checks this decrypted CKI image as follows:

- If the Check Value is not '0123456789ABCDEFh,' the process shall be aborted.
- If the Trigger Bits for Audio Profile Processes is not equal to '00h,' the process shall be aborted.
- If the Current Export to CD Counter is equal to '00h,' then the process shall be aborted.

After all the fields in the CKI are checked as above, the Exporting Device additionally checks this decrypted CKI image. If the Current Export to CD Counter field is equal to 'FFh,' go to step (10).

(7) Update the CKI in the temporary CKMG image.

The Exporting Device updates the CKI in the temporary CKMG image as follows:

- The Exporting Device decrements the value of the Current Export to CD Counter of the CKI.

After all the fields in the CKI are updated as above, the Exporting Device encrypts this decrypted CKI image using the CKI Encryption process, and sets the CKI in the temporary CKMG image to the resulting value.

(8) Update the temporary UKURMG image.

The Exporting Device updates the UKURE in the temporary UKURMG image. The Hash Value in the UKURE is set to the value that is calculated for the temporary CKMG image using Hash Calculation Process. Then the Exporting Device encrypts the UKURE in the temporary UKURMG image using the UKURE Encryption process.

(9) Write the temporary UKURMG and CKMG images to the SD Memory Card.

The Exporting Device securely writes the updated temporary UKURMG and CKMG images as the updated UKURMG and CKMG files to the SD Memory Card using the CKMG Update Process in described in *CPRM Specification SD Memory Card Book SD-SD (Separate Delivery) Part.* Then the Exporting Device securely reads the updated UKURMG file from the SD Memory Card using the Secure

Read Process and verifies that the update of the ***m***th UKURE in the UKURMG file has completed successfully.

If the verification of the UKURMG file fails, the Exporting Device shall abort this process.

(10) Start Export

The Exporting Device starts to export the SD-SD content.

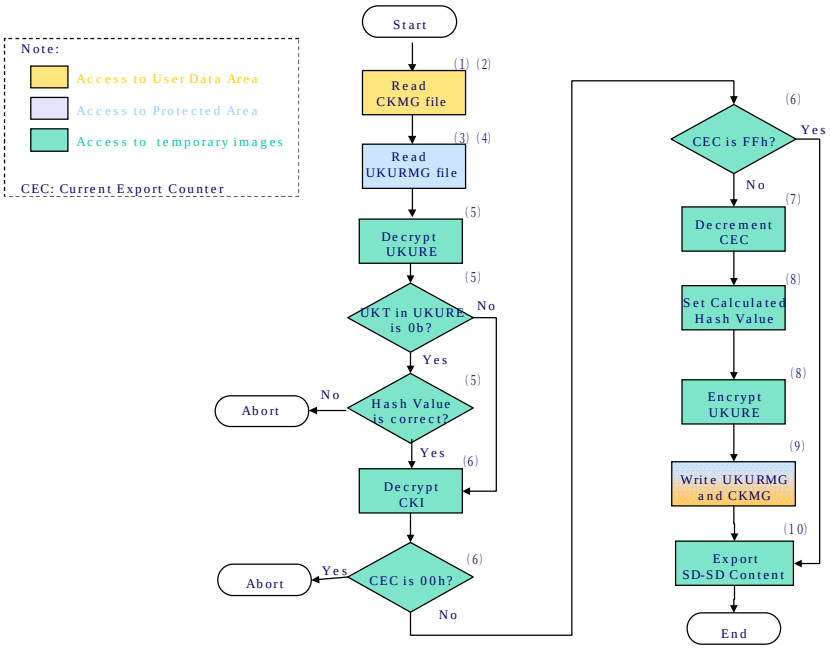


Figure 3-3 Flowchart of Export to CD Process