Content Protection for Recordable Media Specification

SD Memory Card Book
SD-Audio Part

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

Revision 0.97
February 22, 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 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-Audio Part, and,*
- *Other SD-Application Specific Parts (e.g. SD-Sound, SD-ePublish, SD-Image, SD-Video)*

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

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-Audio content stored on SD Memory Card media.
- Appendix A describes additional details for realizing "Move" operations for SD-Audio content.
- Appendix B describes additional details for realizing "Migrate" operations for SD-Audio content.
- Appendix C describes additional details for realizing "Preview" operations for SD-Audio content.

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 1.0*

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

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

SD Group, *SD Specifications, Part 3: Security Specification, Version 2.00*

SD Group, *SD Memory Card Specifications, Part 4: Audio Specifications, Version 1.01*

SD Group, *SD Memory Card Specifications, Part 4: Audio Specifications, MOVE, MIGRATE AND PREVIEW EXTENSION (from AUDIO SPECIFICATION Version1.0 to AUDIO SPECIFICATION Version 1.1)*

Secure Digital Music Initiative (SDMI), *SDMI Portable Device Specification Version 1.0*

1.4 Future Directions

This document currently describes the use of CPRM for the specific SD-Audio formats, e.g. AAC, MP3, WMA, and JPEG. It is anticipated that CPRM technology will also be applied to other formats under future extensions to this specification, as authorized by the 4C Entity, LLC.

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.
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. Alphabetical List of Abbreviations and Acronyms

The following abbreviations and acronyms are used.

4C	4 Companies (IBM, Intel, MEI, and Toshiba)
AAC	Advanced Audio Coding
AKE	Authentication and Key Exchange
C-CBC	Converted Cipher Block Chaining
C2	Cryptomeria Cipher
CCI	Copy Control Information
CPRM	Content Protection for Recordable Media
ECB	Electronic Codebook
FAT	File Allocation Table
ID	Identifier
JPEG	Joint Photographic Experts Group
LCM	Licensed Compliant Module
LLC	Limited Liability Company
lsb	Least Significant Bit
MKB	Media Key Block
MP3	MPEG Layer 3
PC	Personal Computer
PD	Portable Device
PM	Portable Media
RCC	Redundancy Check Code
SD	Secure Digital
SDMI	Secure Digital Music Initiative
TBD	To Be Determined
TBUR	Time-Based Usage Rules
TS	Time Stamp
UR	Usage Rules
WMA	Windows Media Audio
XOR	Exclusive-OR

This page is intentionally left blank.

Chapter 3
CPRM for SD-Audio

3. CPRM for SD-Audio

3.1 Introduction

This chapter and appendices A, B, and C specify details for using CPRM to protect SD-Audio content stored on SD Memory Card media. This chapter describes details for using CPRM to realize “Check-in” and “Check-out” operations for SD-Audio content. In a “Check-in” and “Check-out” operation the following three processes are defined:

- Recording Process

  The process writes “SD-Audio content for local use” from a Recording Device (e.g. Kiosk) to an SD Memory Card.

  Here, “SD-Audio content for local use” is defined as the content, which is consistent with the “SDMI Protected Content for Local Use” defined in *SDMI Portable Device Specification Version 1.0.*

- Check-out Process

  The process copies “SD-Audio content for local use” via an LCM to an SD Memory Card and the number of permitted copies decremented by one.

- Check-in Process

  The process copies “SD-Audio content for local use”, which was checked out on an SD Memory Card, from the SD Memory Card to its original location via the LCM and the number of permitted copies is incremented by one and makes the Check-out content on the SD Memory Card permanently unusable.

Regarding the background of “Check-out and Check-in”, or content flow in the “Check-out and Check-in process”, refer to *SD Memory Card Specifications- Part4 Audio Specifications.* Regarding the definition of “LCM (Licensed Compliant Module), refer to 3.1 of *SDMI Portable Device Specification Version 1.0.*

The SD Audio and SD Memory Card formats are licensable from the SD Group, 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.

3.2 Device Requirements

Each CPRM compliant Recording or Playback Device that supports “Check-in and Check-out” operations must follow the protocols described in this specification. In addition, each device is given one set of 16 secret Device Keys associated with “MKB for SD-Audio”, which is defined in the Appendix C of *SD Specifications- Part3 Security Specification*.

3.3 CPRM Components

This section describes the logical location and format of the CPRM components that relate to protection of SD-Audio content that was checked out on the "SD Memory Card". Figure 3-1depicts the logical locations of these CPRM Components.

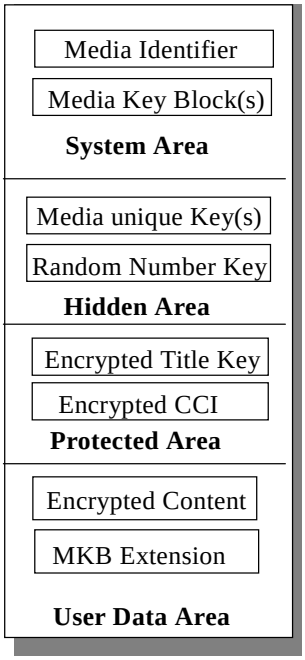


Figure 3-1– SD Memory Card

3.3.1 System Area

Regarding the System Area, refer to section 3.3.1 of the *Common Part* of the *SD Memory Card Book*.

In addition, the following sub-section applies.

3.3.1.1 Media Key Block (MKB)

In order to protect the Title Key and CCI (Copy Control Information) associated with SD-Audio content, which was checked out on the "SD Memory Card", the “MKB for SD-Audio” is used. The MKB number for SD-Audio is described in Appendix C of *SD Specifications Part3 Security Specification*.

3.3.2 Hidden Area

Regarding the Hidden Area, refer to section 3.3.2 of *Common Part* of *SD Memory Card Book*.

3.3.3 Protected Area

Regarding the Protected Area, refer to section 3.3.3 of *common part* of *SD Memory Card Book.*

In addition, the following descriptions and sub-section apply.

In the case of SD-Audio content, which was checked out on the "SD Memory Card", the Protected Area contains the Encrypted Title Key, and the Encrypted CCI (Copy Control Information). (not including UR (Usage Rules))

3.3.3.1 Encrypted Title Key and CCI (Copy control Information)

In the case of SD-Audio content, which was checked out on the "SD Memory Card", the Title Key and CCI (Copy Control Information) 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. The file system of the Protected Area and the detailed format of the Encrypted Title Keys and

CCI are described in section 3.7. Here, for first generation SD-Audio, the CCI length is 2 bits. For detailed format of CCI, refer to section 3.7.4.

3.3.4 User Data Area

Regarding the User Data Area, refer to section 3.3.4 of the *Common Part* of the *SD Memory Card Book*.

3.4 Content Encryption and Decryption Protocol.

Regarding the Content Encryption and Decryption Protocol, the same protocol as described in section 3.4 of the *Common Part* of the *SD Memory Card Book* is applicable. So, refer to section 3.4 of the *Common Part* of the *SD Memory Card Book*. In the case of SD-Audio content that was checked out on the "SD Memory Card", CCI is defined, but UR (Usage Rules) is not defined.

3.5 Accessing the Protected Area

Regarding accessing processes to the Protected Area, the same processes as described in section 3.5 of the *Common Part* of the *SD Memory Card Book* are applicable. So, refer to section 3.5 of the *Common Part* of the *SD Memory Card Book*.

3.6 Content Encryption and Decryption Format

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

In addition, the following sub-section applies.

3.6.1 Audio Object Encryption

3.6.1.1 AAC Audio Encryption

SD-Audio application treats the AAC data stream as one of audio content streams. The AAC data stream is encrypted by the Title Key as follows:

- The AAC data stream consists of multiple audio frames.
- Each frame of an AAC data stream is encrypted by the Title Key.
- Each frame consists of a header part (fixed to 7 bytes) and data part (variable size $N=4\sim2^{13}-1$).
- 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 ($N=8\sim2^{13}-1$), 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 3-1 through Table 3-3 shows the encrypted AAC frame format.

Table 3-1 – Encrypted AAC frame format without residual block (N=8*n)

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

Table 3-2 – Encrypted AAC frame format with residual block (N=8*n+m, m<8)

Byte \ Bit	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 3-3 – AAC frame format in the case Data Part is less than 8 bytes (N<8)

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

3.6.1.2 MPEG Layer3 Audio Encryption

SD-Audio application treats MPEG Layer3 (MP3) data stream as one of audio content stream. The MP3 data stream is encrypted by the Title Key as follows:

- MP3 data stream consists of multiple frames.
- Each frame of an MP3 data stream is encrypted by the corresponding Title Key.
- Each frame consists of a header part (fixed to 4 bytes) and data part (variable size N=44~1436).
- Each frame starts a new C-CBC cipher chain.
- Only the data part is encrypted as follows. The last residual block, if it is less than 8 bytes, is not encrypted.

Table 3-4 and Table 3-5 show the encrypted MP3 frame format.

Table 3-4 – Encrypted MP3 frame format without residual block (N=8*n)

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

Table 3-5 – Encrypted MP3 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								
3								
4	Data Part (Encrypted)							
5								
8n+3								
8n+4	Residual block of Data Part (Non-Encrypted)							
N+3								

3.6.1.3 Windows Media Audio Encryption

SD-Audio application treats the Microsoft's Windows Media Audio (WMA) data stream as one of audio content stream. The WMA data stream is encrypted by the Title Key as follows:

- The WMA data stream treated in SD-Audio specifications consists of an ASF Header Section, an ASF Data Section Object (fixed to 50 bytes) and multiple ASF Data Packets. An ASF Data Packet corresponds to an audio frame of the case of AAC or MP3.
- The ASF Header Section and the ASF Data Section Object are not encrypted.
- Each ASF Data Packet consists of a header part (variable size : less than or equal to 40bytes) and a data part (variable size N=40~2^32-40 bytes).
- Each ASF Data Packet is encrypted by the Title Key using C-CBC mode as follows.
  -Each ASF Data Packet starts a new C-CBC cipher chain.
  -Forty (40) bytes from the top of each ASF Data Packet is not encrypted.
  -The residual data part is encrypted. The last residual block, if it is less than 8 bytes, is not encrypted.

Table 3-6 and Table 3-7show the encrypted ASF Data Packet format of WMA data stream.

Table 3-6– Encrypted ASF Data Packet format without residual block (N=8*n)

<table>
<tr><th>Bit
Byte</th><th>7</th><th>6</th><th>5</th><th>4</th><th>3</th><th>2</th><th>1</th><th>0</th></tr>
<tr><td>0</td><td colspan="8" rowspan="4">40bytes from the top of the ASF Data Packet (Non-Encrypted)</td></tr>
<tr><td>1</td></tr>
<tr><td></td></tr>
<tr><td>39</td></tr>
<tr><td>40</td><td colspan="8" rowspan="5">Residual ASF Data Packet (Encrypted)</td></tr>
<tr><td>41</td></tr>
<tr><td></td></tr>
<tr><td></td></tr>
<tr><td>N+39</td></tr>
</table>

Table 3-7– Encrypted ASF Data Packet format with residual block (N=8*n+m, m<8)

Bit / Byte	7	6	5	4	3	2	1	0
0	40 bytes from the top of the ASF Data Packet (Non-Encrypted)							
1								
39								
40	Residual ASF Data Packet (8*n) (Encrypted)							
41								
8n+39								
8n+40	Last residual block (m<8) (Non-Encrypted)							
N+39								

3.6.2 Picture Object Encryption

3.6.2.1 JPEG Encryption

The SD-Audio application treats the JPEG data stream as one of images data stream. The JPEG data stream is encrypted by the Title Key as follows:

- The SD-Audio format defines an 8-byte header for the file containing the JPEG data. The header is kept unencrypted.
- The JPEG data following the header is encrypted using C2 in C-CBC mode. There is no break in the cipher chaining.

3.7 File System of the Protected Area

Regarding the general description of the file system of the Protected Area, refer to section 3.7 of *common part* of *SD Memory Card Book*. In addition, the following sub-section applies for SD-Audio.

3.7.1 File System of the Protected Area for SD-Audio

This section describes the file system of the Protected Area for SD-Audio, in which the Encrypted Title Key and CCI (Copy Control Information) are stored.

3.7.1.1 Title Key Manager (TKMG).

The Title Key and CCI (Copy Control Information) for each piece of SD-Audio content to be checked out are encrypted by the Media Unique Key and stored in a single file (e.g. AOBSA1.KEY) in the Protected Area. This file is generally called the Title Key Manager file (TKMG).

3.7.1.2 Directory and File Configuration in Protected Area

Figure 3-2 shows an example directory and file configuration of the Protected Area for SD-Audio.

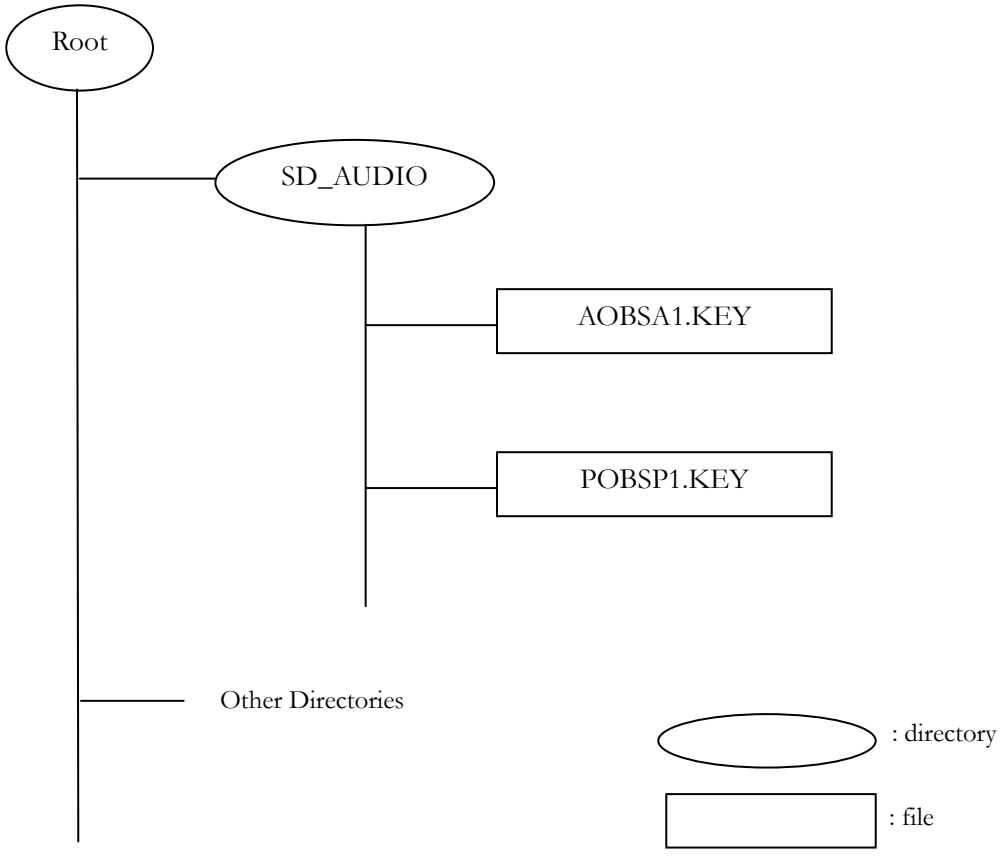


Figure 3-2– Directory and File Configuration

The Title Key Manager (TKMG) file for audio objects is named AOBSA1.KEY in the SD_AUDIO directory in the Protected Area. It contains each of the Title Keys for the audio content files, (the AOBxxx.SA1 files), which are stored in the SD_AUDIO directory in the User Data Area.

POBSP1.KEY is the Title Key Manager (TKMG) file that stores each of the Title Keys for picture objects (the POBxxx.SP1 files), which are stored in User Data Area. It is in the SD_AUDIO directory in the User Data Area.

The file name of the Title Key Manager is determined according to the names of encrypted content files in the User Data Area.

(1) Both the Protected Area and the User Data Area have file systems that are independent but are structured in the same way, as shown in Figure 3-3. The Title Key Manager file and the encrypted content file are stored in the corresponding directories (e.g. in Figure 3-3, SD_AUDIO).

(2) The file name of the Title Key Manager is a combination of the first three characters of the name of the encrypted content file in the User Data Area (e.g. In Figure 3-3, "AOB") and a file-name extension of the encrypted content file (e.g. In Figure 3-3, "SA1").

(3) The file-name extension of the Title Key Manager is '.KEY'.

(4) The number assigned to the encrypted content file name in the User Data Area corresponds to the Title Key Entry index in the Title Key Manager Area (As shown in Figure 3-3, “AOB00j.SA1” corresponds to ”Title Key Entry #j").

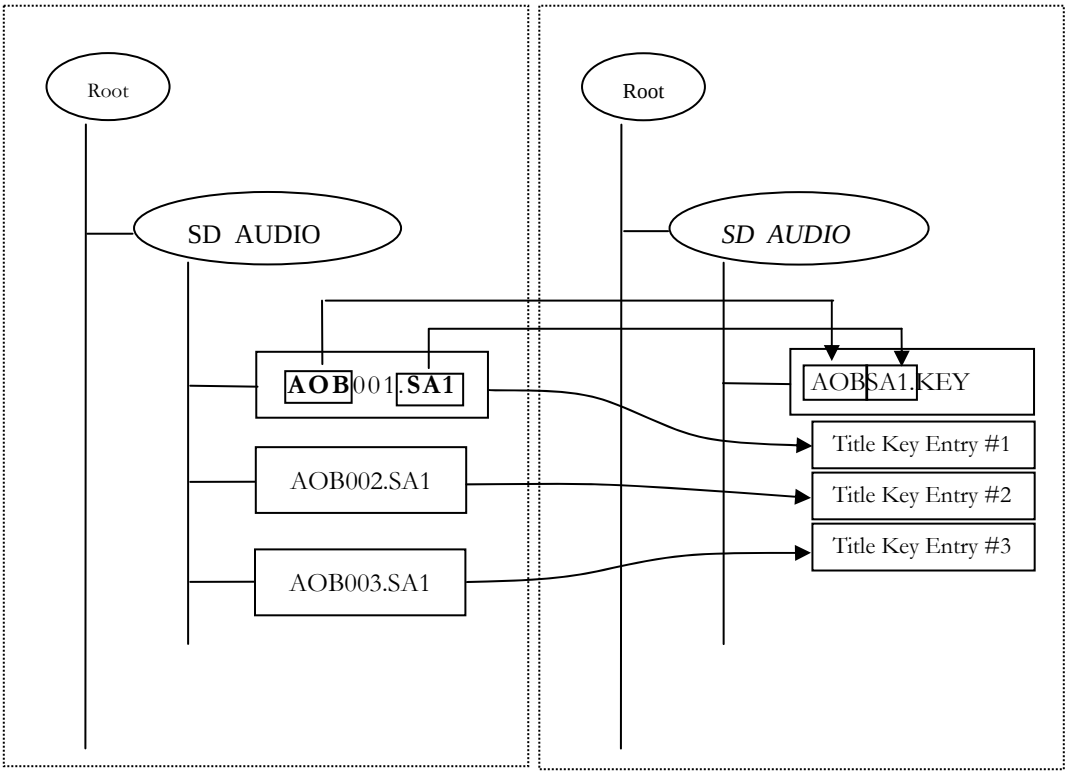


Figure 3-3– Relationship between Directory and File name

3.7.2 Title Key Manager Structure

Figure 3-4 shows the structure of Title Key Manager (TKMG).

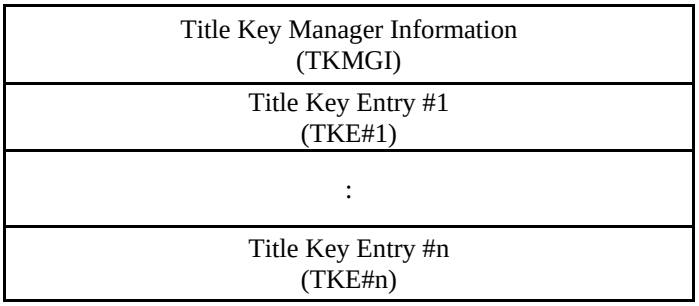


Figure 3-4– Title Key Manager (TKMG)

Title Key Manager (TKMG) consists of the Title Key Manager Information (TKMGI) and a number of Title Key Entries (TKEs). TKMGI is a 16-byte structure and consists of the TKMG Identifier, the size of TKMG, and the attributes of Title Key Entry (TKE), etc. Each TKE is 16-byte long and consists of the Encrypted Title Key, Encrypted CCI (Copy Control Information) and the Content ID.

3.7.3 Title Key Manager Information (TKMGI)

As shown in Table 3-8, TKMGI consists of the size of TKMG, size of a Title Key Entry, the number of Title Key Entries, and other elements.

Table 3-8– TKMGI

TKMGI (Description order)

RBP	Field Name	Contents	Number of bytes
0 to 1	TKMGI_ID	TKMGI Identifier	2 bytes
2 to 3	VERN	Version number	2 bytes
4 to 7	TKMG_SZ	Size of TKMG	4 bytes
8 to 9	TKMG_AP_ID	Application Identifier of TKMG	2 bytes
10 to 11	TKE_N	The number of Title Key Entries	2 bytes
12	TKE_SZ	Size of Title Key Entry	1 byte
13	TKE_ATR	Attribute of Title Key Entry	1 byte
14 to 15	Reserved	Reserved	2 bytes
Total			16 bytes

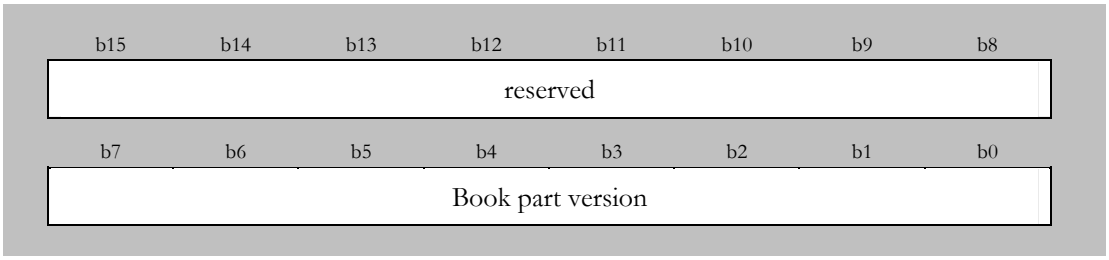
(RBP 0 to 1) TKMGI_ID

When the Title Key Manager is associated with AOB (audio objects), the TKMGI_ID is "A1". When the Title Key Manager is associated with POB (picture objects), the TKMGI_ID is "P1".

All characters are in the standard ISO646 code.

(RBP 2 to 3) VERN

Describes the version number of the *SD Memory Card Specifications, Part 4: Audio Specifications.*



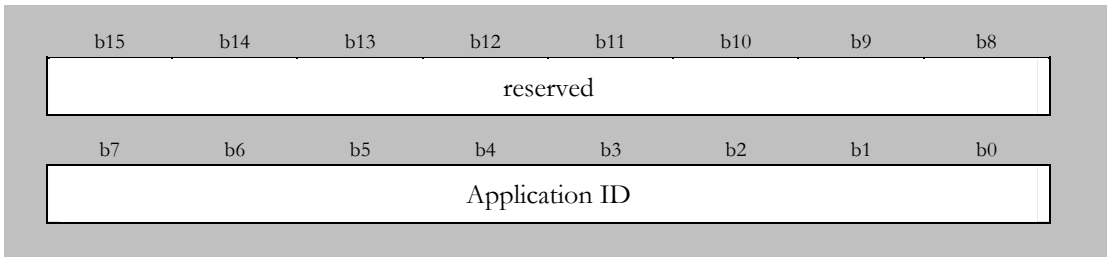
Book part version	09h : version 0.9
	10h : version 1.0
	Others : reserved

(RBP 4 to 7) TKMG_SZ

Describes the data size of the TKMG in bytes. For SD-Audio this value is fixed at '16000'.

(RBP 8 to 9) TKMG_AP_ID

Describes the Application ID of TKMG. For SD-Audio this value is fixed at '00h'. Other values will be assigned by the SD Association.



Application ID	00h : SD-Audio
	Others : reserved

(RBP 10 to 11) TKE_N

Describes the number of Title Key Entries. For SD-Audio this value is fixed at '999'.

(RBP 12) TKE_SZ

Describes data size of Title Key Entry. For SD-Audio this value is fixed at '16'.

(RBP 13) TKE_ATR

Describes the Title Key Entry attribute. Indicates whether the Title Key Entry includes CCI, in addition to the key. For SD-Audio this value is fixed at '01h'.

3.7.4 Title Key Entry (TKE)

As shown in Table 3-9, TKE consists of Title Key Entries.

Table 3-9– TKE

TKE (Description order)

RBP	Field Name	Contents	Number of bytes
0 to 15	TKE	Title Key Entry	16 bytes
Total			16 bytes

(RBP 0 to 15) TKE

Describes the Title Key Entry for each encrypted content file.

As shown in Table 3-10, the first 6-bits (from b122 to b127) of the TKE are reserved. The next 2-bits (from b120 to b121) are the CCI (Copy Control Information) in the first generation of SD-Audio. The next 56-bits (from b64 to b119) are the Title Key (EKEY field). The next 1-bit (b63) is the Availability flag. The next 53-bits (from b10 to b62 are reserved. The last 10-bits (from b0 to b9) are a local Content ID on SD Memory Card. The Content ID is used in the Check-in/Check-out procedure described the section 3.8.

The first 8-bytes field (from b64 to b127) of TKE is encrypted using Media Unique Key with C2_E and the last 8-bytes field (from b0 to b63) of TKE is not encrypted.

When the content is checked in (i.e., it is no longer on the SD Memory Card), the first 8-bytes encrypted field (from b64 to b127) shall be set to the random number using the Secure Title Key Delete process described in section 3.5.3 of the *Common Part* of the *CPRM SD Memory Card Book*, and the Availability flag field shall be set to '0'. Table 3-10 shows the detail of Title Key Entry (TKE).

CCI	00b : Copying is permitted without restriction. 01b : reserved 10b : One generation of copies may be made. 11b : No more copying is permitted.
EKEY	Stores the Title Key.
Availability flag	0b : EKEY is not available. 1b : EKEY is available
Content ID	Stores the Content ID, which is used for locally identifying the content on the SD Memory Card by the SD-Audio Application. 1~999 are available as content IDs. If Content ID == 0, this means the TKE is not in use.

In SD-Audio, it is possible to divide a single audio content into several files. In that case, the Title Key (EKEY field) is treated in a special way. For example, say an audio content is divided into 'n' files, AOB00j.SA1 (j=1, 2, …, n). Then TKE#j is associated with audio file AOB00j.SA1, and:

(1) One of the TKEs shall have the following:

- Title Key stored in the EKEY field.
- "1" stored in the Availability flag field.
- Any number (1 ~ 999) stored in the Content ID field

(2) The other TKEs shall have the following:

- A random number stored in the EKEY field.
- "0" stored in the Availability flag field.
- The same Content ID as above stored in the Content ID field.

An accessing device finds the Title Key of the audio file AOB00j.SA1 as follows:

(i) The accessing device reads TKE#j and checks the Availability flag.

(ii) If the Availability flag == '0', the device must find another TKE with the same Content ID whose Availability flag is '1'.

(iii) Upon finding such TKE, the accessing device decrypts the encrypted field (from b64 to b127) of TKE, reads the EKEY field and obtains the Title Key.

Note: All reserved bits within the TKE (from b10 to b62, and from b122 to b127) shall be set to '0'. For forward compatibility, devices shall ignore non-zero values in these fields.

Table 3-10 – Detail of Title Key Entry

b127	b126	b125	B124	b123	b122	b121	b120
Reserved						CCI	
b119	b118	b117	B116	b115	b114	b113	b112
EKEY [48…55]							
b111	b110	b109	B108	b107	b106	b105	b104
EKEY [40…47]							
b103	b102	b101	b100	b99	b98	b97	b96
EKEY [32…39]							
b95	b94	b93	b92	b91	b90	b89	b88
EKEY [24…31]							
b87	b86	b85	b84	b83	b82	b81	b80
EKEY [16…23]							
b79	b78	b77	b76	b75	b74	b73	b72
EKEY [8…15]							
b71	b70	b69	b68	b67	b66	b65	b64
EKEY [0…7]							
b63	b62	b61	b60	b59	b58	b57	b56
Availability flag	Reserved						
b55	b54	b53	b52	b51	b50	b49	b48
Reserved							
b47	b46	b45	b44	b43	b42	b41	b40
Reserved							
b39	b38	b37	b36	b35	b34	b33	b32
Reserved							
b31	b30	b29	b28	b27	b26	b25	B24
Reserved							
b23	b22	b21	b20	b19	b18	b17	b16
Reserved							
b15	b14	b13	b12	b11	b10	b9	b8
Reserved						Content ID[8,9]	
b7	b6	b5	b4	b3	b2	b1	b0
Content ID[0….7]							

3.8 Recording and Check-in/Check-out

This section describes the Recording and Check-in/Check-out protocols. In the following protocols, regarding the Secure Read Process, the Secure Write Process, the Secure Title Key Delete Process and the AKE Process, refer to Sections 3.5.1, 3.5.2, 3.5.3 and 3.4.1 of the *Common Part* of the *CPRM SD Memory Card.*

3.8.1 Recording Process

The Recording Device securely holds information associated with SD-Audio content to be recorded. The information includes the Title Key and the CCI. The Title Key is a secret unpredictable value (e.g., given by the Content Provider or selected at random), and the CCI is either given by the Content Provider or set according to the default rules.

(1) The Recording Device securely reads the Title Key Manager (TKMG) file, AOBSA1.KEY, from the SD Memory Card using the Secure Read Process.

(2) The Recording Device finds a Title Key Entry (TKE) that is not in use, and updates the Content ID field with a number that has not been currently assigned in the TKMG file on this SD Memory Card. It also updates the CCI field and the EKEY field of the TKE.

(3) The Recording Device securely writes the updated TKMG file as the new TKMG file to the SD Memory Card using the Secure Write Process.

3.8.2 Check-in and Check-out Process

This section describes the Check-in and Check-out protocol. Regarding the definition of check-in and check-out, refer to Sections 3.16 and 3.17 of the *SDMI Portable Device Specification Part 1 Version 1.0* and, for understanding the requirement, refer to Section 5.7.2 of the *SDMI Portable Device Specification Part 1 Version 1.0.*

Check-out Process:

The LCM securely holds *CO-information* about the check-out content. The CO-information includes CO-counter #i (the number of remaining permitted copies), and, for each SD Memory Card for which the content has been checked out, the Media ID, the Content ID, and the Title Key.

(1) The LCM securely reads the Title Key Manager (TKMG) file, AOBSA1.KEY, from the SD Memory Card using the Secure Read Process.

(2) The LCM securely decrements CO-counter #i. To protect against a "Pull Card Attack", this step shall be done before the following steps are executed.

(3) The LCM updates the Content ID field with a number that has not currently assigned on this SD Memory Card. It also updates the CCI field and the EKEY field of the TKE associated with the check-out content on the received TKMG file.

(4) The LCM securely writes the updated TKMG file as the new Key Manager file to the SD Memory Card using the Secure Write Process.

Check-in Process:

(1) The LCM securely reads the Title Key Manager (TKMG) file, AOBSA1.KEY, from the SD Memory Card using the Secure Read Process.

(2) The LCM has the CO-information (the Content ID, the Media ID and the Title Key) of the check-in content.

(3) The LCM verifies that the check-in content has the expected Content ID, Media ID and the expected Title Key. If not, the process is aborted.

(4) The LCM 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 check-in content on the TKMG file, using the Secure Title Key Delete protocol. In addition, the Availability flag is set to '0'.

(5) If the Secure Title Key Delete Process does not succeed in step (4), the LCM must assume the check-in has not occurred and aborts the process.

(6) The LCM securely increments CO-counter #i. To protect against the "Pull Card Attack", this step shall only be done after all the previous steps have completed. In other words, the following steps require that the host has direct access to the device; the read and write operations are not locally buffered in the host.

3.9 MKB Extensions for SD-Audio

The MKB Extension file configuration in the User Date Area for SD-Audio is as follows:

The directory name is SD_AUDIO and the file name of the MKB Extension file is SD_AUDIO.MKB.

This page is intentionally left blank.

Appendix A
Move Extension for SD-Audio

A. Move Extension for SD-Audio

A.1 Introduction

This appendix specifies additional details for using CPRM technology to realize "Move" operation for SD-Audio content. In a Move operation, the following three processes are defined:

- Recording Process

  The process writes "SD-Audio content for distribution" from a Recording Device (e.g. Kiosk) to an SD Memory Card.

  Here, "SD-Audio content for distribution" is defined as the content, which consists of SD-Audio content and its "Usage Rules" for controlling Move operation and is consistent with the "SDMI Protected Content for distribution" defined in *SDMI Portable Device Specification Version 1.0.* "Usage Rules" are expressed by Content Providers and are consistent with the one defined in *SDMI Portable Device Specification Version 1.0.*

- Move Process I (from SD Memory Card to Host)

  The process copies "SD-Audio content for distribution" stored on an SD Memory Card to its Destination Device (e.g. personal computer) and makes the original on the SD Memory Card permanently unusable.

- Move Process II (from Host to SD Memory Card)

  The process copies "SD-Audio content for distribution", which was Moved from an SD Memory Card to the Destination Device by the Move Process I, to an SD memory Card and makes the original on the Destination Device permanently unusable. Hereafter we call the Destination Device in the Move Process II a Source Device in this appendix.

Note: "SD-Audio content for distribution" can be moved from one Host to another via a SD Memory Card, or from one SD Memory Card to another via a Host, using the Move Process I and II. However, direct move from one Host to another is outside scope of this specification.

Regarding the background of "Move" or content flow in the "Move" process, refer to *SD Memory Card Specifications- Part4 Audio Specifications MOVE, MIGRATE AND PREVIEW EXTENSION (from AUDIO SPECIFICATION Version1.0 to AUDIO SPECIFICATION Version 1.1).*

A.2 Device Requirements

Each CPRM compliant Recording or Destination (Source) Device, which supports "Move" operation must follow the protocols described in this Appendix A besides the body part of this specification. In addition, each device is given two sets of 16 secret Device Keys, one associated with "MKB for SD-Audio" and the other associated with "MKB for Usage Rules" which is defined as the "MKB for SD-Audio EXTENSION" in Appendix C of *SD Specifications- Part3 Security Specification.*

A.3 CPRM Components

This section describes the logical location and format of the additional CPRM Components for Move extension, when stored on the "SD Memory Card". Figure A- 1 depicts the logical locations of CPRM Components on the "SD Memory Card" for Move extension.

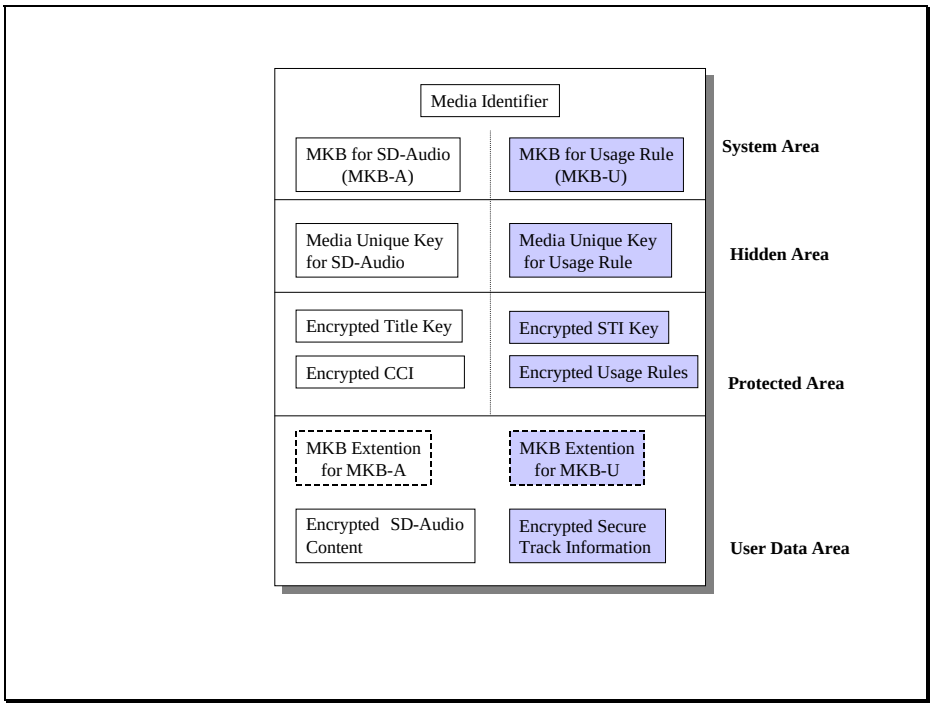


Figure A- 1– Logical location of the CPRM components for "Move" operation

A.3.1 System Area

Regarding the System Area, refer to section 3.3.1 of the *Common Part* of the *SD Memory Card Book*.

In addition, the following sub-section applies.

A.3.1.1 Media Key Block (MKB)

Two MKBs are used for the Move extension.

1) “MKB for Usage Rule”(MKB-U)

   In order to protect the Usage Rules, “MKB for Usage Rule” is used. The MKB number of “MKB for Usage Rule” is defined as the “MKB for SD-Audio EXTENSION” in Appendix C of *SD Specifications-Part3 Security Specification*.

2) “MKB for SD-Audio”(MKB-A)

   In order to protect Title Key and CCI (Copy Control Information) of SD-Audio content, the “MKB for SD-Audio” is used.

In this appendix, MKB for Usage Rule is described "MKB-U", and MKB for SD-Audio is described "MKB-A".

A.3.2 Hidden Area

Regarding the Hidden Area, refer to section 3.3.2 of the *Common Part* of the *SD Memory Card Book*.

In addition, the following sub-section applies.

A.3.2.1 Media Unique Key

Two Media Unique Keys are used for Move extension, which are associated with MKB-U (MKB for Usage Rule) and MKB-A (MKB for SD-Audio).

A.3.3 Protected Area

Regarding the Protected Area, refer to section 3.3.3 of the *Common Part* of the *SD Memory Card Book*.

In addition, the following descriptions and sub-section applies.

The Protected Area contains the following data:

-Encrypted Usage Rules, which are protected by MKB-U

-Encrypted STI Key (Secure Track Info Key), which is protected by MKB-U

-Encrypted Title Key, which is protected by MKB-A

-Encrypted CCI, which is protected by MKB-A

A.3.3.1 Encrypted Title Key

Regarding Encrypted Title Key, refer to Section 3.3.3.1 of the *Common Part* of the *CPRM SD Memory Card Book*.

A.3.3.2 Encrypted CCI

Regarding Encrypted CCI, refer to Section 3.3.3.1 of the *Common Part* of the *CPRM SD Memory Card Book*.

A.3.3.3 Encrypted Usage Rules

Usage Rules (UR) consist of the following information:

-"Move Control Information" is the Usage Rule for controlling the Move operation.

-"Check-out Control Information" specifies the Check-out Counter, which would be used for controlling the Check-out Process after SD-Audio content is “Moved” to its destination device.

-Hash value (C_HASH) of the concatenated “the least significant 7 bytes of Encrypted Title Key, i.e. $[\text{Encrypted Title Key}]_{lsb\_56}$, ”, “the Encrypted Secure Track Information” and “the Encrypted SD-Audio content”. The hash value (C_HASH) is used in the Destination Device to check that the Encrypted Secure Track Information and the Encrypted SD-Audio content are edited or not. (see A.4.2 (4a-1), (4b-4), A.8.1 (3), and A.8.2 (3))

The detail format of the Usage Rules is described in Section A.7.2.3.

A.3.3.4 Encrypted STI Key (Secure Track Information Key)

STI Key (Secure Track Info Key) is used to encrypt the “Secure Track Information”, which includes content specific information, e.g. a song name, artist names, a content provider name, and content distributor identification. The detail is defined in *SD Memory Card Specifications- Part4 Audio Specifications MOVE, MIGRATE AND PREVIEW EXTENSION (from AUDIO SPECIFICATION Version 1.0 to AUDIO SPECIFICATION Version 1.1).*

The detail format of STI Key is described in Section A.7.2.3.

A.3.4 User Data Area

Regarding the User Data Area, refer to section 3.3.4 of the *Common Part* of the *SD Memory Card Book*.

In addition, the following sub-section applies.

A.3.4.1 Encrypted Content

Regarding Encrypted Content, refer to Section 3.3.4.1 of the *Common Part* of the *CPRM SD Memory Card Book.*

A.3.4.2 Encrypted Secure Track Information

Each Secure Track Information shall be encrypted with a unique STI Key and stored as an encrypted file in the User Data Area. The directory structure and file names of the encrypted Secure Track Information is defined in *SD Memory Card Specifications - Part4 Audio Specifications MOVE, Migrate AND PREVIEW EXTENSION (from AUDIO SPECIFICATION Version 1.0 to AUDIO SPECIFICATION Version 1.1).*

A.3.4.3 MKB Extension for MKB-A or for MKB-U

The User Data Area may also contain an MKB Extension file. Regarding the MKB Extension file, refer to section A.9.

A.4 Content and Usage Rule Encryption and Decryption Protocol

A.4.1 SD-Audio content

Regarding the SD-Audio Content Encryption and Decryption Protocol, the same protocol as described in section 3.4 of the *Common Part* of the *SD Memory Card Book* is applicable. So, refer to section 3.4 of the *Common Part* of the *SD Memory Card Book*.

A.4.2 Usage Rules

Figure A- 2 illustrates a protocol for Usage Rules Encryption and Decryption for Move extension.

-(1) The accessing device (Recording, Source or Destination Device) executes Process_MKB

(1a, 1b) Calculate Media Key from MKB-U (MKB for Usage Rule) using Device Key for MKB-U (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 (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 accessing device and SD Memory Card. (The detail of AKE process is shown in Section 3.4.1of *Common Part of CPRM SD Memory Card*.

-(4a) Encrypt STI Key and Usage Rules process.

The accessing device (Recording Device or Source Device) shall execute the following three processes before the Encrypt STI Key and Usage Rules process:

1) Encrypt Title Key and CCI process

Regarding the Encrypt Title Key and CCI process, refer to the section 3.4 (4a) of the *Common Part* of the *CPRM SD Memory Card Book.*

2) Encrypt Secure Track Information process. (Figure A- 2(5))

The accessing device shall protect Secure Track Information by encrypting it using the STI Key in the C2_ECBC (the C2 cipher algorithm in C-CBC mode) described in the *Introduction and Common Cryptographic Elements* book of this specification. The result (Encrypted Secure Track Information) is sent to the SD Memory Card, and stored in the User Data Area.

3) Encrypt SD-Audio content process

Regarding the encrypt SD-Audio content process, refer to the Section 3.4 (5a) of the *Common Part* of the *CPRM SD Memory Card Book.*

Then, the Encrypt STI Key and Usage Rules process is executed as follows:

(4a-1) Calculate C_HASH.

The accessing device concatenates "the least significant 7-bytes of Encrypted Title Key, i.e. $[\text{Encrypted Title Key}]_{lsb\_56}$," "the encrypted Secure Track Information" and "the encrypted SD-Audio content" in that order, and calculates C_HASH as follows:

C_HASH= [SHA-1 (Concatenated $[\text{Encrypted Title Key}]_{lsb\_56}$, Encrypted Secure Track Information and Encrypted SD-Audio content)]$_{lsb\_64}$.

Regarding SHA-1, refer to FIPS PUB 180-1.

(4a-2) Encrypt the STI Key and Usage Rules by the Media Unique Key

The accessing device concatenates the STI Key (K_{sti}) and UR (Usage Rules) and then encrypts them together using the Media Unique Key (K_{mu}) associated with MKB-U with C2_ECBC (the C2 cipher algorithm in C-CBC mode) described in the *Introduction and Common Cryptographic Elements* book of this specification.

(4a-3) Encrypt the encrypted STI Key and Usage Rules by the Session Key

Then, the Encrypted STI Key and UR are further encrypted by the Session Key (K_s) , which is shared at the 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 STI Key and UR are sent to the SD Memory Card.

(4a-4) Decrypt the doubly encrypted STI Key and Usage Rules by the Session Key

In the SD Memory Card, the (doubly-encrypted Encrypted STI Key and UR) are decrypted by the Session Key (K_s) , which is shared at the step (3a), using the C2_DCBC, and those results (Encrypted STI Key and UR) are stored in the Protected Area.

-(4b) Decrypt Encrypted STI Key and UR process.

(4b-1) Encrypt the encrypted STI Key and Usage Rules by the Session Key.

The Encrypted STI Key (K_{site}) and UR are further encrypted by the SD Memory Card using the Session Key (K_s)that 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.

(4b-2) Decrypt the doubly encrypted STI Key and Usage Rules by the Session Key.

The doubly-encrypted Encrypted STI Key and UR are sent to the Destination Device. Then, in the Destination Device, they are decrypted by the Session Key (K_s) , which is shared at step (3b), using the C2_DCBC.

(4b-3) Decrypt the Encrypted STI Key and Usage Rules by the Media Unique Key

Destination Device decrypts the Encrypted STI Key and UR using the Media Unique Key (K_{mu}) associated with MKB-U with C2_DCBC (the C2 cipher algorithm in C-CBC mode) described in the *Introduction and Common Cryptographic Elements* book of this specification.

(4b-4) Calculate C_HASH-ref and check the C_HASH-ref with the decrypted C_HASH.

The Destination Device concatenates "the least significant 7-bytes of Encrypted Title Key, i.e. $[\text{Encrypted Title Key}]_{lsb\_56}$", "the encrypted Secure Track Information" and "the encrypted SD-Audio content" in that order, and calculates C_HASH-ref as follows:

C_HASH-ref= [SHA-1 (Concatenated $[\text{Encrypted Title Key}]_{lsb\_56}$,

Encrypted Secure Track Information and Encrypted SD-Audio content)]$_{lsb\_64}$.

The Destination Device checks the calculated C_HASH-ref with the decrypted C_HASH from step (4b-3).

-(5a) Encrypt STI process

The accessing device (Recording Device or Source Device) shall protect each piece of Secure Track Information (STI) by encrypting it using the STI Key and 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 Secure Track Information (STI) delivered to the Recording Device is already encrypted in this way, the Recording Device does not perform this encryption step. The result (Encrypted Secure Track Information) is sent to the SD Memory Card, and stored in the User Data Area.

-(5b) Decrypt encrypted STI process

The Destination Device uses the STI Key which is decrypted at the step (4b-3) to decrypt encrypted Secure Track Information (STI) using C2_DCBC (C2 cipher algorithm in C-CBC mode) described in the *Introduction and Common Cryptographic Elements* book of this specification.

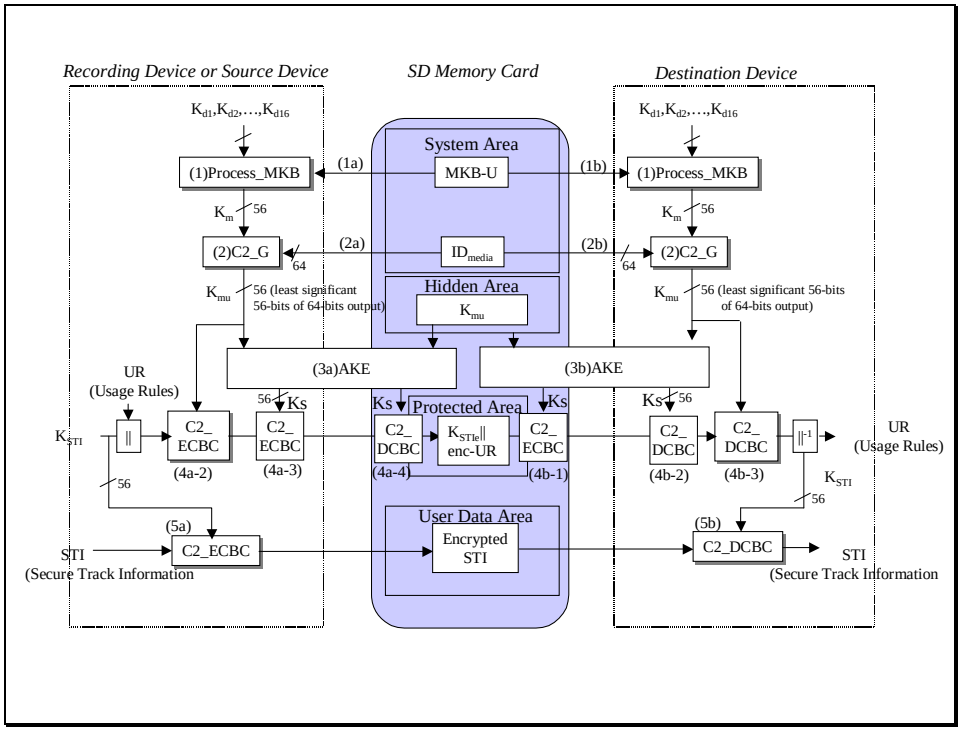


Figure A- 2– Encryption and Decryption for Usage Rules on SD Memory Card

A.5 Accessing the Protected Area

For Move extensions, the Secure Write, Secure Read and Secure Title Key Delete Processes described in Section 3.5 of the *Common Part* of the *CPRM SD Memory Card* are applied. In addition, the following process is applied for Move extensions.

A.5.1 Secure STI Key and Usage Rule Delete Process

A Destination Device deletes the Encrypted STI Key and Usage Rules from the Protected Area using a process that is nearly identical to the Secure Title Key Delete Process described in Section 3.5.3 of *Common Part of CPRM SD Memory Card.* First, a write operation overwrites the Encrypted STI Key and UR (Usage Rules) with a selected value, and then a read operation reads the value to confirm that the overwriting was successful. Figure A- 3 shows the protocol flow for Secure STI Key and Usage Rule Process in the Protected Area.

In Figure A- 3, it is supposed that a Destination 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 protocol.

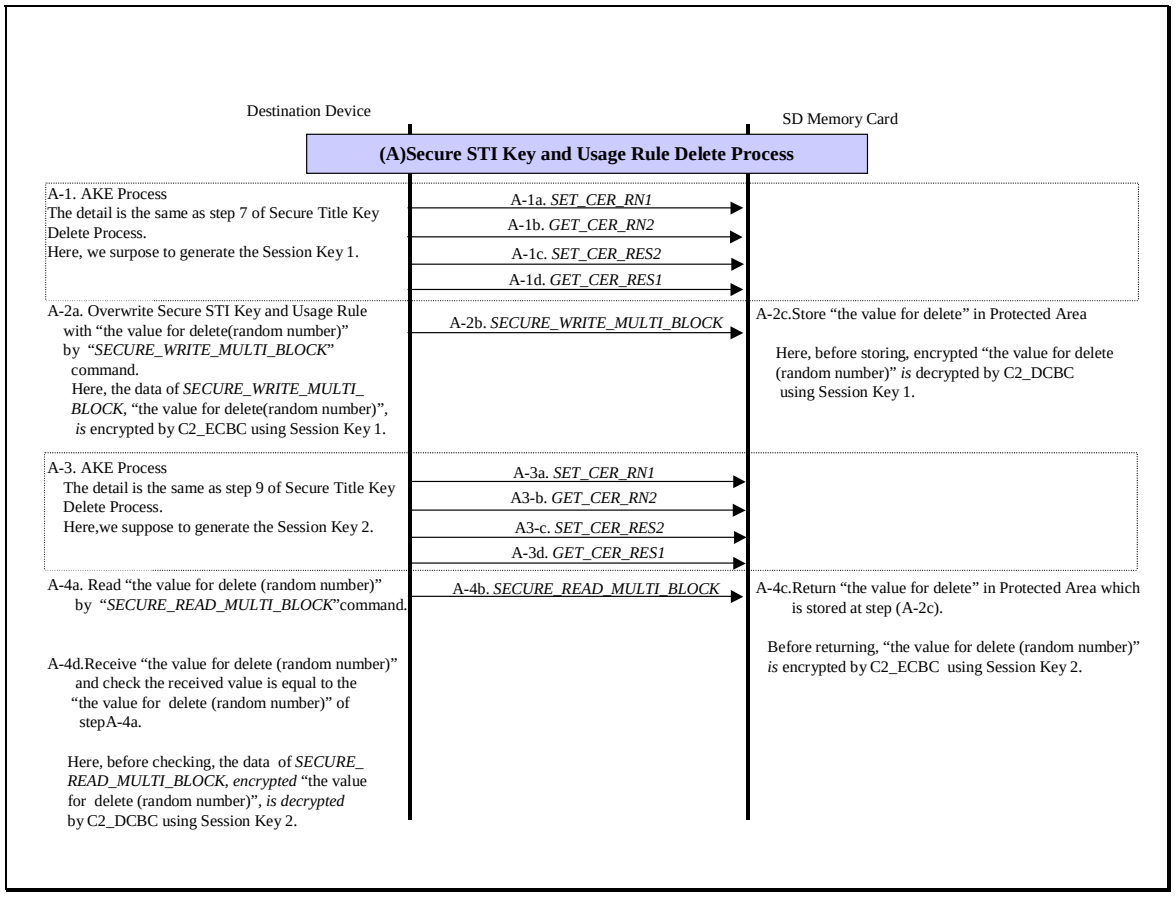


Figure A- 3– Protocol Flow of "Secure STI Key and Usage Rule Delete Process"

Note: In step (A2-a) of Figure A- 3, 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 Specifications – Part3 Security Specification*.

A.6 Content Encryption and Decryption Format

A.6.1 SD-Audio Object Encryption

The same formats described in Section 3.6.1 and 3.6.2 are applicable.

A.6.2 Secure Track Information Encryption

The Secure Track Information is encrypted as follows:

- The size of Secure Track Information is 512 bytes (fixed).
- The whole of Secure Track Information is encrypted by the STI Key (Secure Track Information Key), using C2_ECBC (C2 cipher algorithm in C-CBC mode) described in the *Introduction and Common Cryptographic Elements* book of this specification.

A.7 File System of the Protected Area

This section describes the additional directory and file configuration in the Protected Area for Move Extension.

Figure A- 4 shows an example directory and file configuration of the Protected Area.

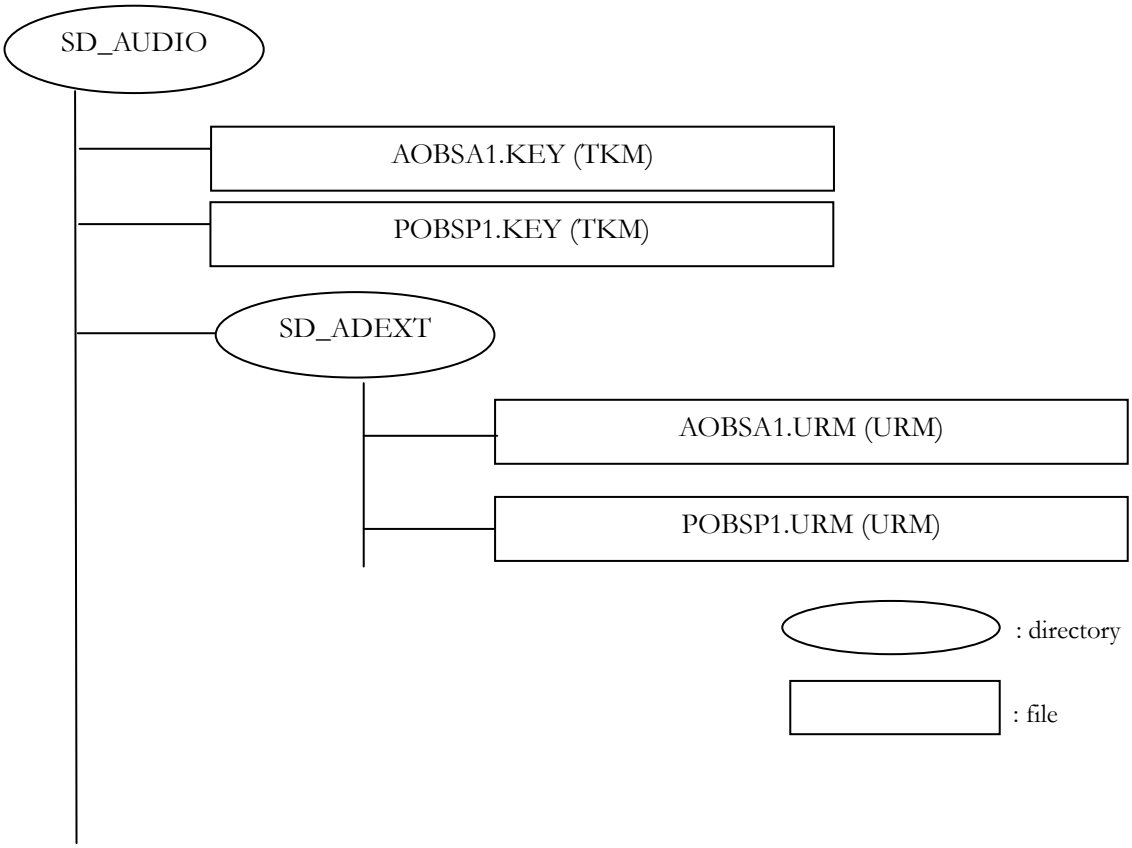


Figure A- 4– Directory and File Configuration for Move Extension

Regarding the Title Key Manager (TKMG) file for "SD-Audio content for distribution", the same directory and file name are used as defined in Section 3.7. The Usage Rule Manager (URMG) file for audio objects is named AOBSA1.URM in the SD_AUDIO/SD_ADEXT directory in the Protected Area. It contains each of the Usage Rules for the audio content files, (the AOBxxx.SA1 files), which are stored on SD_AUDIO directory in the User Data Area. It also contains each of the STI Keys for the Secure Track Information files, (the STKIxxx.SDT files), which are stored on SD_AUDIO/SD_ADEXT directory in the User Data Area.

The Usage Rule Manager (URMG) file for picture objects is named POBSP1.URM in the SD_AUDIO/SD_ADEXT directory in the Protected Area. It contains each of the Usage Rules for the picture content files, (the POBxxx.SP1 files), which are stored on SD_AUDIO directory in the User Data Area. It contains the random data in STI Keys field.

[Note: POBSA1.URM does not contain STI Keys for the Secure Track Information files, (the STKIxxx.SDT files), since picture objects do not have Secure Track Information.]

The file name of the Usage Rule Manager is determined according to the names of encrypted content files in the User Data Area.

(1) Both the Protected Area and the User Area have file systems that are independent but are structured in the same way, as shown in Figure A- 5.

(2) The file name of Usage Rule Manager is a combination of the first three characters of the name of the encrypted content file in the User Data Area (e.g. In Figure A- 5, "AOB") and a file-name extension of the encrypted content file (e.g. In Figure A- 5, "SA1").

(3) The file-name extension of Usage Rule Manager is '.URM'.

(4) The number assigned to the encrypted file name in the User Data Area corresponds to the Usage Rule entry index in the Usage Rule Manager (As shown in Figure A- 5, “AOB00j.SA1” corresponds to ”Usage Rule Entry #j").

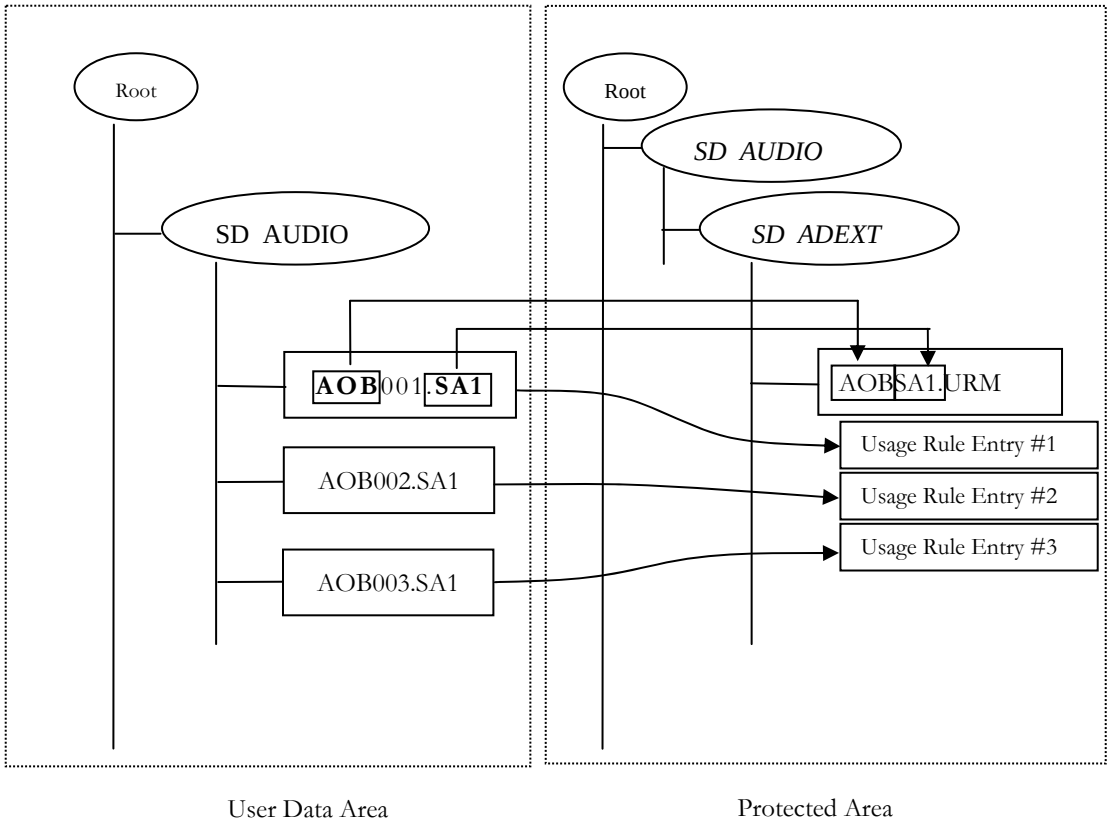


Figure A- 5– Relationship between Directory and File name

A.7.1 Title Key Manager (TKMG)

A.7.1.1 Title Key Manager (TKMG) Structure

The structure of TKMG is the same as defined in Section 3.7.2.

A.7.2 Usage Rule Manager (URMG)

A.7.2.1 Usage Rule Manager (URMG) Structure

Figure A- 6 shows the structure of Usage Rule Manager (URMG).

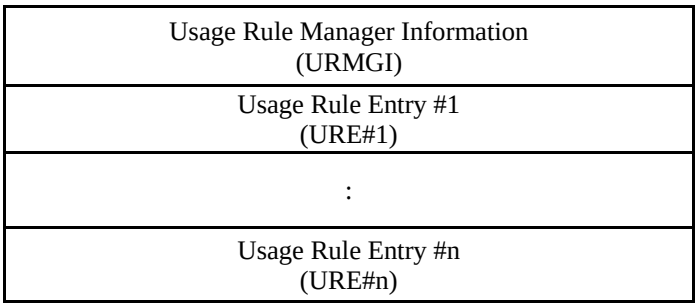


Figure A- 6– Usage Rule Manager (URMG)

The Usage Rule Manager (URMG) consists of the Usage Rule Manager Information (URMGI) and a number of Usage Rule Entries (UREs). URMGI is a 32-byte structure and consists of the URMG Identifier, the size of URMG and the attributes of Usage Rule Entry (URE), etc. Each URE is 32-byte long and consists of the Encrypted Usage Rules, and Encrypted STI Key.

A.7.2.2 Usage Rule Manager Information (URMGI)

As shown in Table A- 1, URMGI consists of the size of URMG, size of a Usage Rule Entry, the number of Usage Rule Entries, and other elements.

Table A- 1– URMGI

URMGI (Description order)

RBP	Field Name	Contents	Number of bytes
0 to 1	URMGI_ID	URMGI Identifier	2 bytes
2 to 3	VERN	Version number	2 bytes
4 to 7	URMG_SZ	Size of URMG	4 bytes
8 to 9	URMG_AP_ID	Application Identifier of URMG	2 bytes
10 to 11	URE_N	The number of Usage Rule Entries	2 bytes
12	URE_SZ	Size of Usage Rule Entry	1 byte
13	URE_ATR	Attribute of Usage Rule Entry	1 byte
14 to 31	Reserved	Reserved	18 bytes
Total			32 bytes

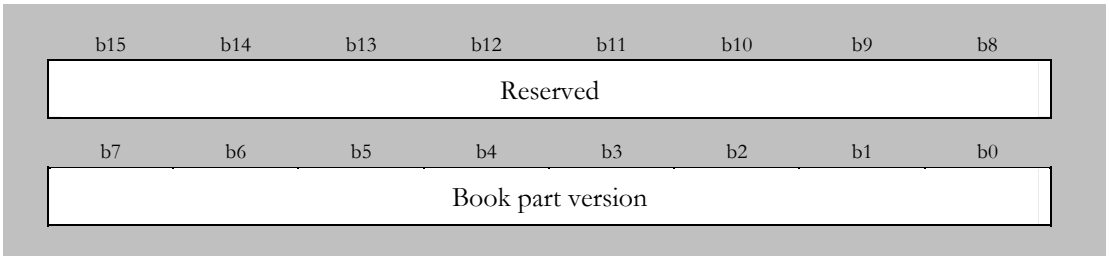
(RBP 0 to 1) URMGI_ID

When the Usage Rule Manager is associated with AOB (audio objects), the URMGI_ID is "M1". When the Usage Rule Manager is associated with POB (picture objects), the URMGI_ID is "P1".

All characters are in the standard ISO646 code.

(RBP 2 to 3) VERN

Describes the version number of the *SD Memory Card Specifications, Part 4: Audio Specifications.*



Book part version	11h: version 1.1 Others: reserved

For forward compatibility, when the Book part version is more than '11h', the devices shall not treat it as an error.

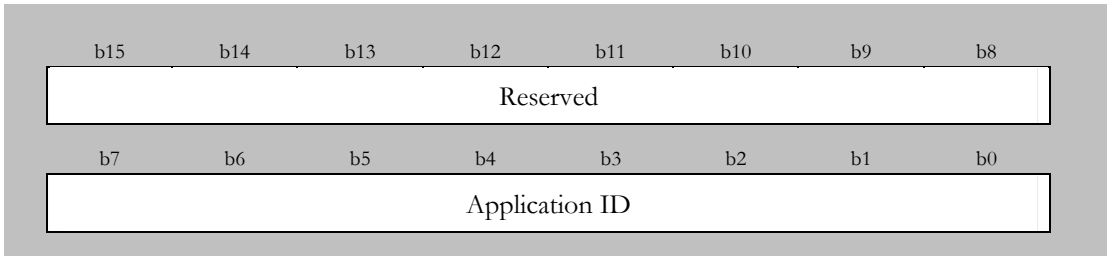
This Book part version in URMGI is independent of the Book part version in TKMGI defined in Section 3.7.3, i.e. VERN field in TKMGI shall be set to '10h'.

(RBP 4 to 7) URMG_SZ

Describes the data size of the URMG in bytes. For SD-Audio content for distribution this value is fixed at '32000'.

(RBP 8 to 9) URMG_AP_ID

Describes the Application ID of URMG. For SD-Audio content for distribution this value is the same number as the MKB number for SD-Audio extension for Move and Preview assigned by SD Association. For the MKB number, refer to Appendix C of *SD Specifications- Part3 Security Specification.*



Application ID	Stores the same number as the MKB number for SD-Audio EXTENSION For the MKB number, refer to Appendix C of *SD Specifications- Part3 Security Specification.* Others: reserved

(RBP 10 to 11) URE_N

Describes the number of Usage Rule Entries. For SD-Audio content for distribution this value is fixed at '999'.

(RBP 12) URE_SZ

Describes data size of Usage Rule Entry. For SD-Audio content for distribution this value is fixed at '32'.

(RBP 13) URE_ATR

Describes the Usage Rule attribute. For SD-Audio for Move extension this value is '02h'.

A.7.2.3 Usage Rule Entry (URE)

As shown in Table A- 2, URE consists of Usage Rule Entries.

Table A- 2– URE

URE (Description order)

RBP	Field Name	Contents	Number of bytes
0 to 31	URE	Usage Rule Entry	32 bytes
Total			32 bytes

(RBP 0 to 31) URE

Describes the Usage Rule Entry for each encrypted content file.

As shown in Table A- 3, the first byte (from b248 to b255) of the URE is reserved. The next 7 bytes (from b192 to b247) are the STI Key. The next bit (b191) is the Availability flag. The next 53 bits (from b138 to b190) are reserved. The next 10 bits (from b128 to b137) are a local Content ID. The next 16 bytes (from b0 to b127) are the Usage Rules field.

The first 8-byte field (from b192 to b255) of the URE and the last 16-byte field (from b0 to b127) are concatenated in that order and encrypted together using the Media Unique Key associate with MKB_U with C2_ECBC.

When the content is moved from SD Memory Card to Destination Device (i.e., it is no longer on the SD Memory Card), the first 8-byte field (from b192 to b255) and the last 16-byte field (from b0 to b127) of the URE shall be set to the random number using the Secure Title Key and Usage Rule Delete Process described in section A.5.1 and the Availability flag field shall be set to '0'. Table A-3 shows the details of the Usage Rule Entry (URE).

STI Key	Stores the STI Key. In the case of the URE associated with the picture objects (POBxxx.SP1), stores the random number
Availability flag	0b: Usage Rule is not available. 1b: Usage Rule is available

Content ID	Stores the Content ID, which is used for locally identifying the content on the SD Memory Card by the SD-Audio Application. 1~999 is available as the Content ID. If Content ID == 0, this means the URE is not in use.
Trigger bit	Trigger bit for Move extensions. 0b: Accessing devices can control the "Move process" by "Move Control information" 1b: Accessing devices of this specification shall not permit Move. In a future version, the Move Control Information may be expanded, or other information for controlling Move may be added. Accessing devices of the future version shall process the new information for controlling Move correctly when this bit is set to '1b'.
Move Control Information	Stores the Move Control Information, which is applied in the Move Process. 0000b: Move is never permitted. 0001b~1110b: Move is permitted specified times 1111b: Move is permitted unlimited times.
Check-out Control Information	Stores the Check-out Counter, which will be applied in Check-out Process. 0000b: Check-out is never permitted. 0001b~1110b: Specified number of copies can be Checked-out simultaneously 1111b: Unlimited number of copies can be Checked-out simultaneously.
C_HASH	Stores the hash values of the concatenated "the least significant 7 bytes of Encrypted Title Key, i.e.$[\text{Encrypted Title Key}]_{lsb\_56}$", "Encrypted Secure Track Information" and "Encrypted SD-Audio content for distribution". In the case of the URE associated with the picture objects, POBxxx.SP1, stores the hash values of concatenated "the least significant 7 bytes of Encrypted Title Key, i.e.$[\text{Encrypted Title Key}]_{lsb\_56}$", and "Encrypted SD-Audio content for distribution".

In SD-Audio, it is possible to divide a single audio content into several files. In that case, the Title Key is treated in a special way described in 3.7.4. In addition to the Title Key, the STI KEY and Usage Rules (the Trigger bit field, the Move Control Information field, the Check-out Control Information field and the C_HASH) are also treated in a special way.

For example, say an audio content is divided into 'n' files, AOB00j.SA1 (j=1, 2, …, n). Then URE#j is associated with audio file AOB00j.SA1, and:

(1) One of the UREs shall have the following: (we suppose the one is URE#k)

- STI Key stored in the STI KEY field.
- "1" stored in the Availability flag field.
- Any number (1 ~ 999) stored in the Content ID field.
- Trigger bit stored in the Trigger bit field.
- Move Control Information stored in the Move Control Information field.
- Check-out Control Information stored in the Check-out Control Information field.
- The hash value for "the $[\text{Encrypted Title Key}]_{lsb\_56}$ associated with TKE#k", "the Encrypted Secure Track Information file (STKI00k.SDT)", and "the Encrypted audio content file (AOB00k.SA1), associated with the URE#k".

(2) The other UREs (URE#j, j=1,2,…,n, except for j=k) shall have the following:

- A random number stored in the STI KEY field.
- "0" stored in the Availability flag field.
- The same Content ID as above stored in the Content ID field.
- The hash value for "the $[\text{Encrypted Title Key}]_{lsb\_56}$ associated with TKE#k", "the Encrypted Secure Track Information file, STKI00j.SDT", and " the Encrypted audio content file, AOB00j.SA1, associated with the URE#j".

An accessing device finds the STI Key and Usage Rules (Trigger bit, Move Control Information, Check-out Control Information) of the audio file, AOB00j.SA1, as follows:

(i) The device reads URE#j and checks the Availability flag.

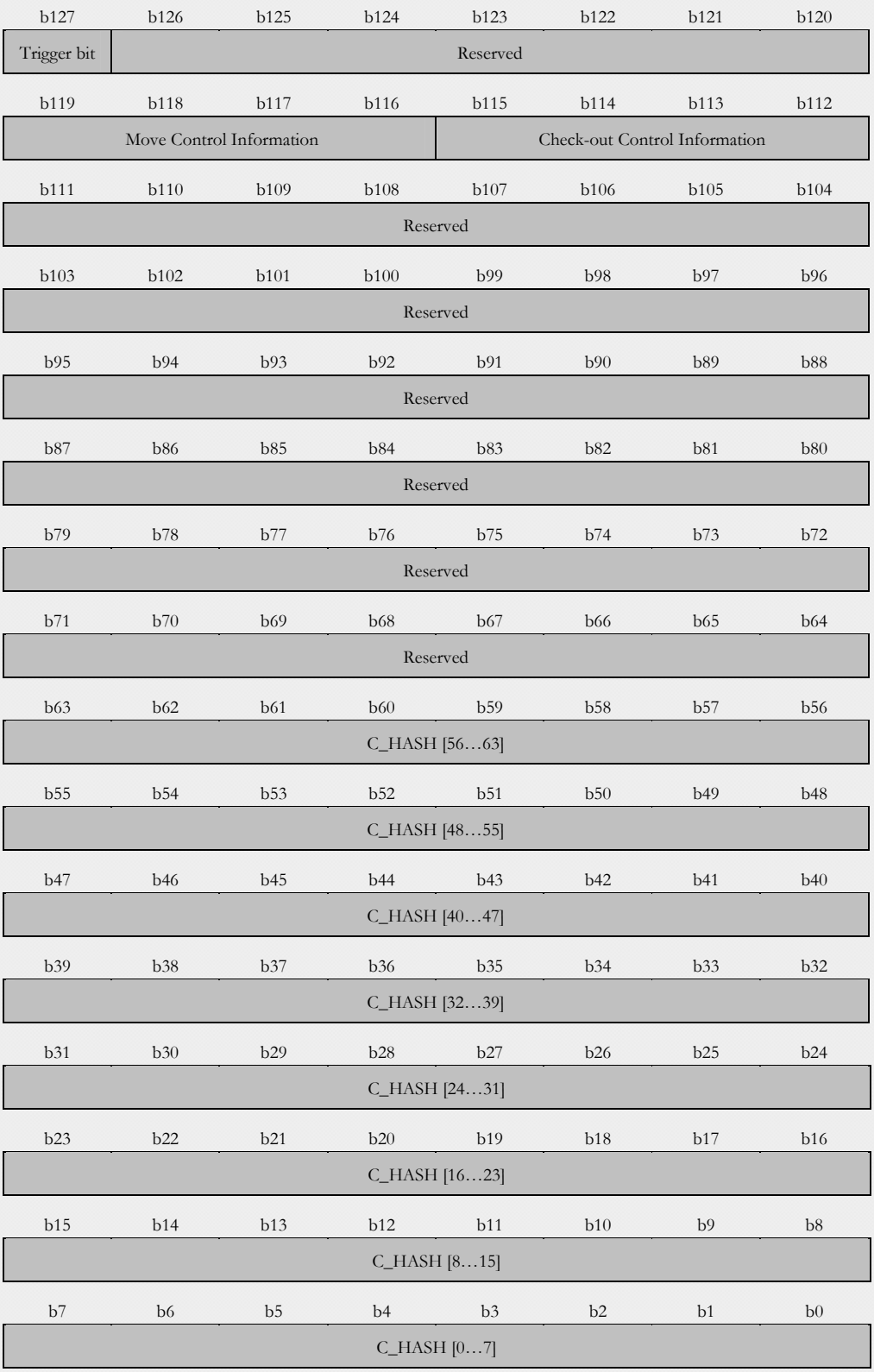
(ii) If the Availability flag == '0', the device must find another URE with the same Content ID whose Availability flag is '1'.

(iii) Upon finding such URE, the device decrypts the encrypted field of URE, reads the STI KEY field, and Usage Rules field (Trigger bit field, Move Control Information field, Check-out Control Information field) and obtains the STI Key, Trigger bit, Move Control Information, and Check-out Control Information.

Note: All reserved bits within the URE shall be set to '0'. Unless otherwise specified, for forward compatibility, devices shall ignore non-zero values in these fields.

Table A- 3– Detail of Usage Rule Entry for SD-Audio Content for Distribution

b255	b254	b253	b252	b251	b250	b249	b248
Reserved							
b247	b246	b245	b244	b243	b242	b241	b240
STI KEY [48…55]							
b239	b238	b237	b236	b235	b234	b233	b232
STI KEY [40…47]							
b231	b230	b229	b228	b227	b226	b225	b224
STI KEY [32…39]							
b223	b222	b221	b220	b219	b218	b217	b216
STI KEY [24…31]							
b215	b214	b213	b212	b211	b210	b209	b208
STI KEY [16…23]							
b207	b206	b205	b204	b203	b202	b201	b200
STI KEY [8…15]							
b199	b198	b197	b196	b195	b194	b193	b192
STI KEY [0…7]							
b191	b190	b189	b188	b187	b186	b185	b184
Availability flag	Reserved						
b183	b182	b181	b180	b179	b178	b177	b176
Reserved							
b175	b174	b173	b172	b171	b170	b169	b168
Reserved							
b167	b166	b165	b164	b163	b162	b161	b160
Reserved							
b159	b158	b157	b156	b155	b154	b153	b152
Reserved							
b151	b150	b149	b148	b147	b146	b145	b144
Reserved							
b143	b142	b141	b140	b139	b138	b137	b136
Reserved						Content ID[8,9]	
b135	b134	b133	b132	b131	b130	b129	b128
Content ID[0….7]							


b127 b126 b125 b124 b123 b122 b121 b120
Trigger bit
Reserved
b119 b118 b117 b116 b115 b114 b113 b112
Move Control Information
Check-out Control Information
b111 b110 b109 b108 b107 b106 b105 b104
Reserved
b103 b102 b101 b100 b99 b98 b97 b96
Reserved
b95 b94 b93 b92 b91 b90 b89 b88
Reserved
b87 b86 b85 b84 b83 b82 b81 b80
Reserved
b79 b78 b77 b76 b75 b74 b73 b72
Reserved
b71 b70 b69 b68 b67 b66 b65 b64
Reserved
b63 b62 b61 b60 b59 b58 b57 b56
C_HASH [56…63]
b55 b54 b53 b52 b51 b50 b49 b48
C_HASH [48…55]
b47 b46 b45 b44 b43 b42 b41 b40
C_HASH [40…47]
b39 b38 b37 b36 b35 b34 b33 b32
C_HASH [32…39]
b31 b30 b29 b28 b27 b26 b25 b24
C_HASH [24…31]
b23 b22 b21 b20 b19 b18 b17 b16
C_HASH [16…23]
b15 b14 b13 b12 b11 b10 b9 b8
C_HASH [8…15]
b7 b6 b5 b4 b3 b2 b1 b0
C_HASH [0…7]

A.8 Recording and Move

This section describes the Recording and Move process .

In the following protocols, regarding the Secure Read Process, the Secure Write Process, the Secure Title Key Delete Process and the AKE Process, refer to Sections 3.5.1, 3.5.2, 3.5.3 and 3.4.1 of the *Common Part* of the *CPRM SD Memory Card* and regarding the Secure STI Key and Usage Rule Delete Process, refer to Sections A.5.1.

A.8.1 Recording Process

The Recording Device securely holds information associated with SD-Audio content for distribution to be moved. The information includes the Usage Rules given by the Content Provider and a secret unpredictable Title Key (e.g., given by the Content Provider or selected at random).

(1) Read the Title Key Manager (TKMG) file from the SD Memory Card

The Recording Device securely reads the TKMG file, AOBSA1.KEY, from the SD Memory Card using the Secure Read Process after the AKE Process using Media Unique Key associated with MKB-A.

(2) Read the Usage Rule Manager (URMG) file from the SD Memory Card

The Recording Device securely reads the URMG file, AOBSA1.URM, from the SD Memory Card using the Secure Read Process after the AKE Process using the Media Unique Key associated with MKB-U.

(3) Update the Usage Rule Entry (URE) in the URMG file

The Recording Device finds a URE that is not in use, and updates the Content ID field with a number that has not been currently assigned in the TKMG file on this SD Memory Card. It also updates the STI Key field, Usage Rules field (the Trigger bit field, Move Control Information field, Check-out Control Information field and C_HASH field) and the Availability flag field of the URE. Here, the hash value (C_HASH) is calculated as follows:

C_HASH= [SHA-1 (concatenated [Encrypted Title Key]$_{lsb\_56}$, Encrypted Secure Track Information (STKIxxx.SDT) and Encrypted SD-Audio content (AOBxxx.SA1)]$_{lsb\_64}$.

(4) Update the TKE in the TKMG file

The Recording Device finds a TKE that is not in use, and updates the Content ID field with the number, which is assigned in the step (3). It also updates the CCI and EKEY field and the Availability flag field of the TKE.

(5) Write the updated URMG file to the SD Memory Card

The Recording Device securely writes the updated URMG file as the new URMG file to the SD Memory Card using the Secure Write Process after the AKE Process using the Media Unique Key associated with MKB-U.

(6) Write updated TKMG file to the SD Memory Card

The Recording Device securely writes the updated TKMG file as the new TKMG file to the SD Memory Card using the Secure Write Process after the AKE process using Media Unique Key associated with MKB-A.

To protect against the “Pull Card Attack”, Recording Device must abort the process when any errors occur in step (5), and must assume that Recording Process has been completely done, when any errors occur in step (6).

A.8.2 Move Process I (from SD Memory Card to Host)

(1) Read the Title Key Entry (TKE) in the Title Key Manager (TKMG) file from the SD Memory Card

The Destination Device securely reads the TKE associated with the SD-Audio content to be moved in the TKMG file, AOBSA1.KEY, from the SD Memory Card using the Secure Read Process after the AKE Process using Media Unique Key associated with MKB-A.

(2) Read the Usage Rule Entry (URE) in the Usage Rule Manager (URMG) file from the SD Memory Card

The Destination Device securely reads the URE associated with the SD-Audio content to be moved in the URMG file, AOBSA1.URM, from the SD Memory Card using the Secure Read Process after the AKE Process using Media Unique Key associated with MKB-U.

(3) Check the Usage Rules

The Destination Device checks the Trigger bit field. If Trigger bit field is "1", the process is aborted. The Destination Device checks the Move Control Information field and judges whether the content is moveable or not. If not (i.e. the Move Control Information is equal to "0000b"), the process is aborted.

The Destination Device calculates the hash value (C_HASH_ref) of Encrypted SD-Audio content on the SD Memory Card as follows:

$$C\_HASH\_ref = [\text{SHA-1 (concatenated [Encrypted Title Key]}_{lsb\_56}\text{, Encrypted Secure Track Information (STKIxxxSDT) and Encrypted SD-Audio content (AOBxxx.SA1))}]_{lsb\_64},$$

and compares the calculated hash value(C_HASH_ref) with the hash value (C_HASH) stored in the URE. If C_HASH_ref is distinct from C_HASH, the process is aborted.

If the Move Control Information is not equal to "1111b", the Destination Device securely decrements the Move Control Information field of Usage Rules.

The Destination Device temporarily holds the Usage Rules.

(4) Invalidate the URE on the SD Memory Card

The Destination Device securely overwrites "the value for delete (random number)" to the encrypted field (first 8-byte field (including STI Key) and the last 16-byte field (including Usage Rules)) of the URE in the URMG file on the SD Memory Card using the Secure STI Key and Usage Rule Delete protocol.

In addition, the Availability flag and the Content ID are set to '0'.

If the Secure STI Key and Usage Rule Delete protocol does not succeed, the Destination Device must assume the "Move " process has not occurred and aborts the process.

(5) Invalidate the TKE on the SD Memory Card

The Destination Device securely overwrites "the value for delete (random number)" to the encrypted first 8-byte field (including Title Key) of the TKE in the TKMG file on the SD Memory Card using the Secure Title Key Delete protocol defined in Section 3.4.3 of the *Common Part* of the *CPRM SD Memory Card Book*.

In addition, the Availability flag and the Content ID are set to '0'.

If Secure Title Key Delete protocol does not succeed, the Destination Device must assume the "Move " has not occurred and aborts the process.

If all above steps are executed successfully, the Destination Device securely holds the Title Key and Usage Rules.

A.8.3 Move Process II (from Host to SD Memory Card)

The Source Device securely holds information associated with SD-Audio content for distribution to be moved. The information includes the Usage Rules moved from an SD Memory Card and a secret unpredictable Title Key (e.g., moved from an SD Memory Card or selected at random).

(1) Check the Usage Rules

The Source Device checks the Usage Rules securely held in it.

If Trigger bit is "1", the process is aborted.

If the Move Control Information is equal to "0000b", the process is aborted.

(2) Read the Title Key Manager (TKMG) file from the SD Memory Card

The Source Device securely reads the TKMG file, AOBSA1.KEY, from the SD Memory Card using the Secure Read Process after the AKE Process using Media Unique Key associated with MKB-A.

(3) Read the Usage Rule Manager (URMG) file from the SD Memory Card

The Source Device securely reads the URMG file, AOBSA1.URM, from the SD Memory Card using the Secure Read Process after the AKE Process using the Media Unique Key associated with MKB-U.

(4) Update the Usage Rule Entry (URE) in the URMG file

The Source Device finds a URE that is not in use, and updates the Content ID field with a number that has not been currently assigned in the TKMG file on this SD Memory Card. It also updates the STI Key field, Usage Rule field (the Trigger bit field, Move Control Information field, which may be updated in step (1), Check-out Control Information field and C_HASH field) and the Availability flag field of the URE. Here, the hash value (C_HASH) is calculated as follows:

C_HASH= [SHA-1 (concatenated [Encrypted Title Key]$_{lsb\_56}$, Encrypted Secure Track Information (STKIxxx.SDT) and Encrypted SD-Audio content (AOBxxx.SA1)]$_{lsb\_64}$.

(5) Update the TKE in the TKMG file

The Source Device finds a TKE that is not in use, and updates the content ID field with the number, which is assigned in the step (4). It also updates the Title Key field, CCI field and the Availability flag field of the TKE.

(6) Make the original content held on the Source Device unusable

The Source Device makes the original SD-Audio content held on it permanently unusable.

(7) Write the updated URMG file to the SD Memory Card

The Source Device securely writes the updated URMG file as the new URMG file to the SD Memory Card using the Secure Write Process after the AKE Process using the Media Unique Key associated with MKB-U.

(8) Write updated TKMG file to the SD Memory Card

The Source Device securely writes the updated TKMG file as the new TKMG file to the SD Memory Card using the Secure Write Process after the AKE process using Media Unique Key associated with MKB-A.

To protect against the “Pull Card Attack”, Source Device must abort the process when any errors occur in step (7), and must assume that Move Process II has been completely done, when any error occur in step (8).

A.9 MKB Extension

This section describes the MKB Extension file configuration for MKB-U (“MKB for Usage Rules”) on the SD Memory Card. MKB Extensions are described in the *Introduction and Common Cryptographic Elements* book of this specification.

In the case of SD-Audio extension for Move, the directory name is SD_AUDIO and the file name of the MKB Extension file for MKB-U is SD_ADEX8.MKB.

Recording and Source devices must recognize SD_ADEX8.MKB file and process it if it is present on the SD Memory Card.

This MKB Extension file is shared by Preview Extension described in Appendix C.

This page is intentionally left blank.

Appendix B
Migrate Extension for SD-Audio

B. Migrate Extension for SD-Audio

B.1 Introduction

This appendix specifies additional details for using CPRM technology to realize "Migrate" operation for SD-Audio content. In Migrate operation, the following two processes are defined.

- Recording Process

  The process writes SD-Audio content that is permitted to "Migrate" to an SD Memory Card. Here, what kind of content may be "Migrated" from the PD/PM to the LCM and what kind of operations shall be executed are defined in *SDMI Portable Device Specification Part1Version 1.0*.

- Migrate Process

  The process copies SD-Audio content with CCI for migration stored on an SD Memory Card to its destination device and makes the original on the SD Memory Card permanently unusable.

  Regarding the background of "Migrate" or content flow in the "Migrate" process, refer to *SD Memory Card Specifications- Part4 Audio Specifications MOVE, MIGRATE AND PREVIEW EXTENSION (from AUDIO SPECIFICATION Version 1.0 to AUDIO SPECIFICATION Version 1.1).*

B.2 Device Requirements

Regarding Device Requirements for Migrate extension, the same Device Requirements described in section 3.2 are applicable. So, refer to section 3.2.

B.3 CPRM Components

Regarding the CPRM Components, refer to Section 3.3.

In addition, the following sub-section applies for Migrate extension.

B.3.1 Protected Area

B.3.1.1 Encrypted CCI (Copy Control Information)

For controlling Migrate, CCI is extended as follows:

- CCI (2bits): Regarding CCI, refer to Section B.7.4.
- Migrate Permission flag (MPF) (1bit): This flag is used for controlling for Migrate operation.

B.4 Content Encryption and Decryption Protocol

Regarding the Content Encryption and Decryption Protocol, refer to Section 3.4.

B.5 Accessing the Protected Area

For Migrate extension, the Secure Write, Secure Read and Secure Title Key Delete Processes described in Section 3.5 of the *Common Part* of the *CPRM SD Memory Card* are applied.

B.6 Encryption and Decryption Format

Regarding Encryption and Decryption Format, refer to Section 3.6.

B.7 File System of the Protected Area

This section describes additional control information in the Title Key Entry to control Migrate.

B.7.1 Directory and File configuration in Protected Area

Regarding the Directory and File configuration, the same directory and file configuration described in Section 3.7 is applied.

B.7.2 Title Key Manager (TKMG)

Regarding the Title Key Manager, the same structure described in Section 3.7.2 is applied.

B.7.3 Title Key Manager Information (TKMGI)

Regarding the Title Key Manager Information (TKMGI), the same structure described in Section 3.7.3 is applied, but VERN field shall be set to '10h'.

B.7.4 Title Key Entry (TKE)

The Migrate Permission Flag is added to the Title Key Entry structure described in Section 3.7.4.

(RBP 0 to 15) TKE

Migrate Permission Flag(MPF)	0b: Migrate is prohibited. 1b: Migrate is permitted.
CCI	00b : Copying is permitted without restriction. 01b : reserved 10b : One generation of copies may be made. 11b : No more copying is permitted.
EKEY	Stores the Title Key.
Availability flag	0b : EKEY is not available. 1b : EKEY is available
Content ID	Stores the Content ID, which is used for locally identifying the content on the SD Memory Card by the SD-Audio Application. 1~999 are available as content IDs. If Content ID == 0, this means the TKE is not in use.

In SD-Audio, it is possible to divide a single audio content into several files. In that case, the Migration Permission Flag (MPF) field and the Title Key (EKEY field) are treated in a special way. For example, say an audio content is divided into ‘n’ files, AOB00j.SA1 (j=1, 2, …, n). Then TKE#j is associated with audio file AOB00j.SA1, and:

(1) One of the TKEs shall have the following:

- Migration Permission Flag stored in the MPF field.
- CCI stored in the CCI field.
- Title Key stored in the EKEY field.
- “1” stored in the Availability flag field.
- Any number (1 ~ 999) stored in the Content ID field

(2) The other TKEs shall have the following:

- A random number stored in the EKEY field.
- “0” stored in the Availability flag field.
- The same content ID as above stored in the Content ID field.

An accessing device finds the Migration Permission Flag (MPF) and the Title Key of the audio content file AOB00j.SA1 as follows:

(i) The accessing device reads TKE#j and checks the Availability flag.

(ii) If the Availability flag == ‘0’, the device must find another TKE with the same Content ID whose Availability flag is ‘1’.

(iii) Upon finding such TKE, the accessing device decrypts the encrypted field (from b64 to b127), reads the MPF field and EKEY field, and obtains the Migration Permission Flag (MPF) and the Title Key.

Note: All reserved bits within the TKE shall be set to ‘0’. For forward compatibility, devices shall ignore non-zero values in these fields.

Table B- 1– Detail of Title Key Entry

b127	b126	B125	b124	b123	b122	b121	b120
Reserved					MPF	CCI	
b119	b118	B117	b116	b115	b114	b113	b112
EKEY [48…55]							
b111	b110	B109	b108	b107	b106	b105	b104
EKEY [40…47]							
b103	b102	B101	b100	b99	b98	b97	b96
EKEY [32…39]							
b95	b94	B93	b92	b91	b90	b89	b88
EKEY [24…31]							
b87	b86	B85	b84	b83	b82	b81	b80
EKEY [16…23]							
b79	b78	B77	b76	b75	b74	b73	b72
EKEY [8…15]							
b71	b70	B69	b68	b67	b66	b65	b64
EKEY [0…7]							
b63	b62	B61	b60	b59	b58	b57	b56
Availability flag	Reserved						
b55	b54	B53	b52	b51	b50	b49	b48
Reserved							
b47	b46	B45	b44	b43	b42	b41	b40
Reserved							
b39	b38	B37	b36	b35	b34	b33	b32
Reserved							
b31	b30	B29	b28	b27	b26	b25	b24
Reserved							
b23	b22	B21	b20	b19	b18	b17	b16
Reserved							
b15	b14	B13	b12	b11	b10	b9	b8
Reserved						Content ID[8,9]	

b7	b6	b5	b4	b3	b2	b1	b0
Content ID[0….7]							

B.8 Recording and Migrate

This section describes the Recording and Migrate processes. In the following protocols, regarding the Secure Read Process, the Secure Write Process, the Secure Title Key Delete Process and the AKE Process, refer to Sections 3.5.1, 3.5.2, 3.5.3 and 3.4.1 of the *Common Part* of the *CPRM SD Memory Card Book.*

B.8.1 Recording Process

The Recording Device securely holds information associated with SD-Audio content. The information includes the CCI, and Title Key that is picked at random.

(1) The Recording Device securely reads the Title Key Manager (TKMG) file, AOBSA1.KEY from the SD Memory Card using the Secure Read Process after the AKE process using Media Unique Key associated with MKB-A.

(2) The Recording Device finds a Title Key Entry (TKE) that is not in use, and updates the Content ID field with a number that has not been currently assigned in the TKMG file on this SD Memory Card. It also updates the Migrate Permission Flag field, CCI field and EKEY field of the TKE. For the content that is permitted to be migrated, the Migrate Permission Flag may be set to ‘1’; for other content, it shall be set to ‘0’.

(3) The Recording Device securely writes the updated TKMG file as the new TKMG file to the SD Memory Card using the Secure Write Process after the AKE process using Media Unique Key associated with MKB-A.

B.8.2 Migrate Process

(1) The Destination Device securely reads the Title Key Entry (TKE) associated with the SD-Audio content to be migrated in the Title Key Manager (TKMG) file, AOBSA1.KEY, from the SD Memory Card using the Secure Read Process after the AKE process using the Media Unique Key associated with MKB-A.

(2) The Destination Device checks the MPF field of the TKE in the TKMG file and judges whether the content is permitted to be migrated or not. If not, the process is aborted.

(3) The Destination Device securely overwrites "the value for delete (random number)" to the encrypted first 8-byte field (including Title Key) of the TKE in the TKMG file on the SD Memory Card, using the Secure Title Key Delete protocol after the AKE process using Media Unique Key associated with MKB-A. In addition, the Availability flag and the Content ID are set to ‘0’.

(4) If the Secure Title Key Delete Process does not succeed in step (3), the Destination Device must assume the Migrate process has not occurred and aborts the process.

If all above steps are executed successfully, the Destination Device securely holds the Title Key associated with SD-Audio content to be migrated.

This page is intentionally left blank.

Appendix C
Preview Extension for SD-Audio

C. Preview Extension for SD-Audio

C.1 Introduction

This appendix specifies additional details for using CPRM technology to realize "Preview" operation for SD-Audio content. In Preview operation, the following two processes are defined.

- Recording Process

  The process writes "SD-Audio content for Preview" to an SD Memory Card.

  Here, "SD-Audio content for Preview" is defined as the content, which consists of SD-Audio content and its "Usage Rules" for controlling Preview operation.

- Preview Process

  The process previews the SD-Audio content stored on an SD Memory Card according to the Usage Rule.

  Regarding the background of "Preview" or content flow in the "Preview" process, refer to *SD Memory Card Specifications- Part4 Audio Specifications MOVE, MIGRATE AND PREVIEW EXTENSION (from AUDIO SPECIFICATION Version 1.0 to AUDIO SPECIFICATION Version 1.1).*

C.2 Device Requirements

Each CPRM compliant recording or playback device that supports the "Preview" operation must follow the protocols described in this Appendix C besides the body part of this specification. In addition, each device is given a set of 16 secret Device Keys associated with "MKB for Usage Rule (MKB-U)" which is defined as the "MKB for SD-Audio EXTENSION" in Appendix C of *SD Specifications- Part3 Security Specification*.

Each device that supports the "Preview" operation described in this appendix shall have at least one of the following clock functions:

- Clock A: ordinary clock function, which may be changeable by the user and implemented without tamper resistant manner.
- Clock B: tamper resistant clock function, which shall be implemented with tamper resistant manner and not changeable by the user. Moreover, Clock B shall be accurate to within 5 minutes per month and synchronized at least 60 days period.

Moreover, Clock B is classified as follows;

- Clock B1: tamper resistant clock function (Clock B) without network capability. Clock B1 shall set by the timestamp in the timestamp file, when clock B1 is in an "unset state" or "inaccurate state". The details are described in C.7.3.5. Here, "unset state" means the state to which a clock stops (e.g. device is new or device has lost power). A clock in unset state shall not make the clock work, until being possible to adjust at appropriate time even if the battery recovers. "Inaccurate state" means the state to which a clock adjusts at inaccurate time.
- Clock B2: tamper resistant clock function (Clock B) with network capability. Clock B2 shall set by network capability, e.g. accessing Web-based, secure time service, or a network clock, when Clock B2 is in an "unset state".

In this appendix, it is called Mode “X” when a device has Clock ”X” and it operates based on the Clock “X”.

A device may have multiple clock functions described above and these clock functions may be switched as long as they are used appropriately. For example, a device may have two clock functions, Clock A and Clock B1, and use the Clock A as backup when the Clock B1 does not work. Another example, a device that works in Mode B2 may switch to Mode B1 when the network capability of the Clock B2 does not work.

Each device that does not support the “Preview” operation may have the above clock functions

C.3 CPRM Components

This section describes the logical location and format of the additional CPRM Components for Preview extension when stored on the “SD Memory Card”. Figure C- 1 depicts the logical locations of CPRM Components on the “SD Memory Card” for Preview extension.

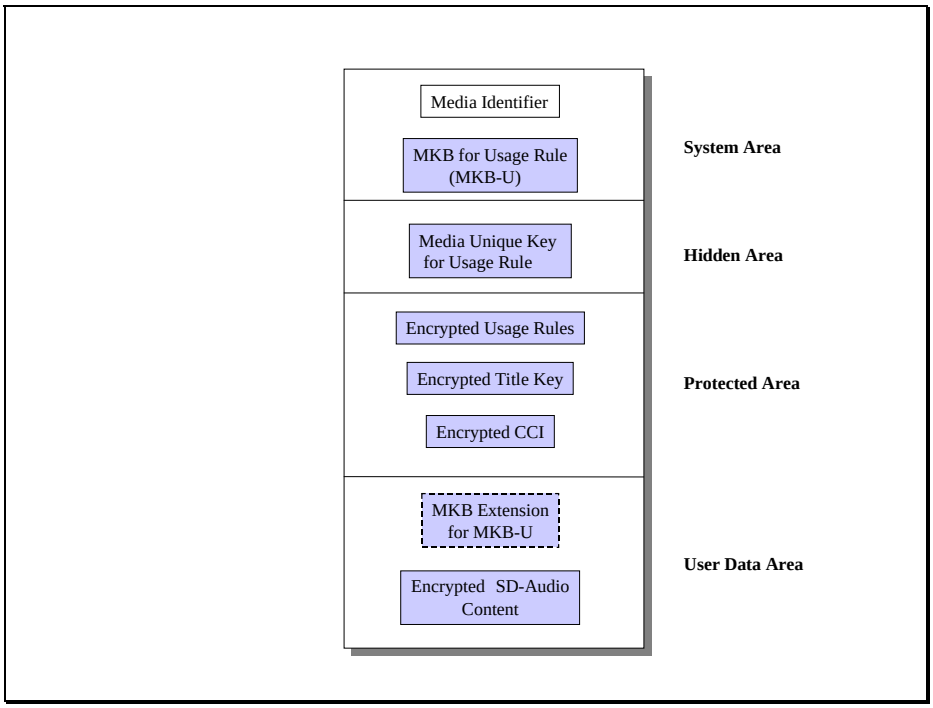


Figure C- 1– Logical location of the CPRM components for “Preview” operation

C.3.1 System Area

Regarding the System Area, refer to section 3.3.1 of the *Common Part* of the *SD Memory Card Book*.

In addition, the following sub-section applies.

C.3.1.1 Media Key Block (MKB)

For Preview extension, MKB for Usage Rule (MKB-U) described in Section A.3.1.1 is used in order to protect Usage Rules, Title Key and CCI.

C.3.2 Hidden Area

Regarding the Hidden Area, refer to section 3.3.2 of the *Common Part* of the *SD Memory Card Book*.

In addition, the following sub-section applies.

C.3.2.1 Media Unique Key

The Media Unique Keys is used for Preview extension, which is associated with MKB-U (MKB for Usage Rule).

C.3.3 Protected Area

Regarding the Protected Area, refer to section 3.3.3 of the *Common Part* of the *SD Memory Card Book*.

In addition, the following descriptions and sub-section applies.

The Protected Area contains the following data:

-Encrypted Usage Rules, which are protected by MKB-U

-Encrypted Title Key, which is protected by MKB-U

-Encrypted CCI, which is protected by MKB-U

In addition, the Protected Area may also contain timestamp. The detail of timestamp is described in Section C.7.3.

C.3.3.1 Encrypted Title Key

Regarding Encrypted Title Key, refer to Section 3.3.3.1.

C.3.3.2 Encrypted CCI

Regarding Encrypted CCI, refer to Section 3.3.3.1.

C.3.3.3 Encrypted Usage Rules

Usage Rules (UR) for controlling Preview operation consist of the following information:

-"Preview Counter" specifies the limited times of playback for preview content.

The initial value of Preview Counter is given by Content Provider. Preview Counter is decremented by one at every playback.

-"Preview Threshold " specifies playback duration, by which it is judged that one playback for preview has occurred and the Preview Counter is decremented by one.

-“Period Control Information”: Usage Rule for controlling the Preview operation. It describes the interval of time when playback is permitted. More precisely, period information corresponds to the start date and time plus the end date and time of such interval

-“Span Control Information”: Usage Rule for controlling the Preview operation. The span information indicates the number of days and hours of permitted playback for content with time-based usage rules

-“Check Value”: a fixed value placed at the end of the Usage Rules. This value is used for detecting whether the Title Key and Usage Rules are unexpectedly altered or not.

The detail format of Usage Rules is described in Section C.7.2.3.

C.3.4 User Data Area

Regarding the User Data Area, refer to section 3.3.4 of the *Common Part* of the *SD Memory Card Book*.

In addition, the following sub-section applies.

C.3.4.1 Encrypted Content

Regarding Encrypted Content, refer to Section 3.3.4.1 of the *Common Part* of the *SD Memory Card Book*.

C.3.4.2 MKB Extension for MKB-U

Regarding MKB Extension, refer to Section A.3.4.3.

C.4 Content and Usage Rule Encryption and Decryption Protocol

C.4.1 SD-Audio content and Usage Rule

Almost the same encryption and decryption protocol as defined in Section 3.4 of the *Common Part* of the *CPRM SD Memory Card Book* is applied for encrypting and decrypting the associated data of SD-Audio content for Preview (e.g. Title Key, CCI, and SD-Audio content itself) and the Usage Rules (e.g. Preview Counter and Preview Threshold), where, MKB-U shall be used.

Figure C- 2 illustrates a process for preview content encryption and decryption on “SD Memory Card”.

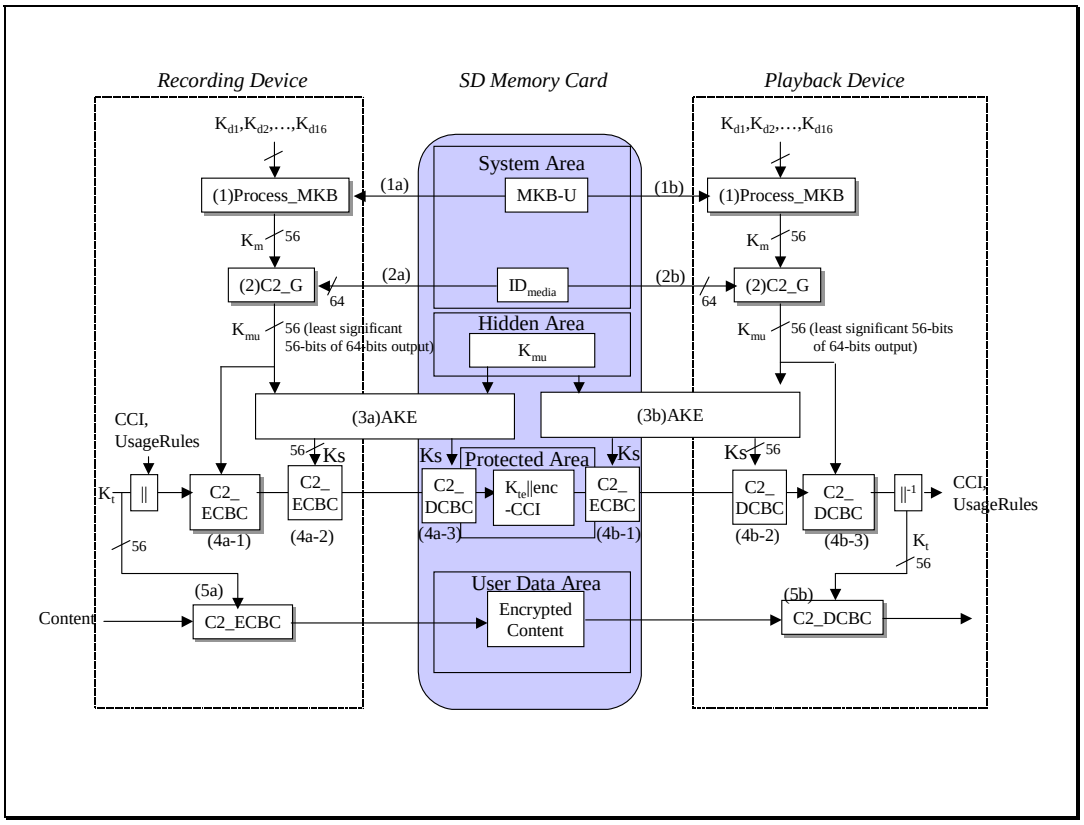


Figure C- 2– Encryption and Decryption for Preview Content on SD Memory Card

The SD Memory Card and the accessing device authenticate each other as follows:

- (1) The accessing device executes Process_MKB

  (1a, 1b) Calculate Media Key from MKB-U (MKB for Usage Rule) using Device Keys for MKB-U (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 accessing device and SD Memory Card. (The detail of AKE process is shown in Section 3.4.1 of the *Common Part* of the *CPRM SD Memory Card Book*.

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

When the content is encrypted, a Title Key is picked at random.

(4a-1) Encrypt the Title Key, CCI and Usage Rules (UR).

When the content is encrypted, a Title Key is picked at random. The accessing device concatenates the Title Key (K_t), CCI and Usage Rules (UR) and then encrypts them together using the Media Unique Key (K_{mu}) associated with MKB-U with C2_ECBC (the C2 cipher algorithm in C-CBC mode) described in the *Introduction and Common Cryptographic Elements* book of this specification.

(4a-2) Encrypt the Encrypted Title Key, CCI and Usage Rule by the Session Key.

The Encrypted Title Key, CCI and UR 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 UR are sent to the SD Memory Card.

(4a-3) Decrypt the doubly-encrypted Encrypted Title Key, CCI and Usage Rules (UR)

In the SD Memory Card, the (doubly-encrypted Encrypted Title Key and Usage Rule) are decrypted by the Session Key (K_s), which is shared at step (3a), using the C2_DCBC, and those results (Encrypted Title Key CCI and UR) are stored in the Protected Area.

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

(4b-1) Encrypt the Encrypted Title Key and Usage Rule by the Session Key.

The Encrypted Title Key (K_t), CCI and UR are encrypted by the SD Memory Card using the Session Key (K_s)that is shared at step (3b), using 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, CCI and UR are sent to the Playback Device.

(4b-2) Decrypt the doubly-encrypted Encrypted Title Key and Usage Rule

Then, in the Playback Device, the (doubly-encrypted Encrypted Title Key, CCI and UR) are decrypted by the Session Key (K_s) that is shared at step (3b), using C2_DCBC, and those results (Encrypted Title Key, CCI and UR) are decrypted using the Media Unique Key (K_{mu}) with C2_DCBC (the C2 cipher algorithm in C-CBC mode) described in the *Introduction and Common Cryptographic Elements* book of this specification

(4b-3) Decrypt the Encrypted Title Key, and Usage Rules (UR).

The accessing device uses the Media Unique Key (K_{mu}) associated with MKB-U to decrypt the Encrypted Title Key, CCI and Usage Rules with C2_DCBC (the C2 cipher algorithm in C-CBC mode) described in the *Introduction and Common Cryptographic Elements* book of this specification.

-(5a) Encrypt content process

The accessing device shall protect each piece of content by encrypting it using the Title Key (K_t) and 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 accessing device decrypts encrypted content using the Title Key (K_t) decrypted at step (4b), with C2_DCBC (C2 cipher algorithm in C-CBC mode) described in the *Introduction and Common Cryptographic Elements* book of this specification.

C.5 Accessing the protected Area

For Preview extension, the Secure Write, Secure Read and Secure Title Key Delete Processes described in Section 3.5 of the *Common Part* of the *CPRM SD Memory Card Book* are applied. In addition, the following process is applied for Preview extension.

C.5.1 Secure Title Key and Usage Rule Delete Process

A Playback Device deletes the Encrypted Title Key and Usage Rules from the Protected Area using a process that is nearly identical to the Secure Title Key Delete Process described in Section 3.5.3 of the *Common Part* of the *CPRM SD Memory Card Book*. First, a write operation overwrites the Encrypted Title Key and UR (Usage Rules) with a selected value, and then a read operation reads the value to confirm that the overwriting was successful. Figure C- 3 shows the typical protocol flow for the Playback Device deleting an Encrypted Title Key and Usage Rule Process in the Protected Area.

In Figure C- 3, it is supposed that a Playback 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 protocol.

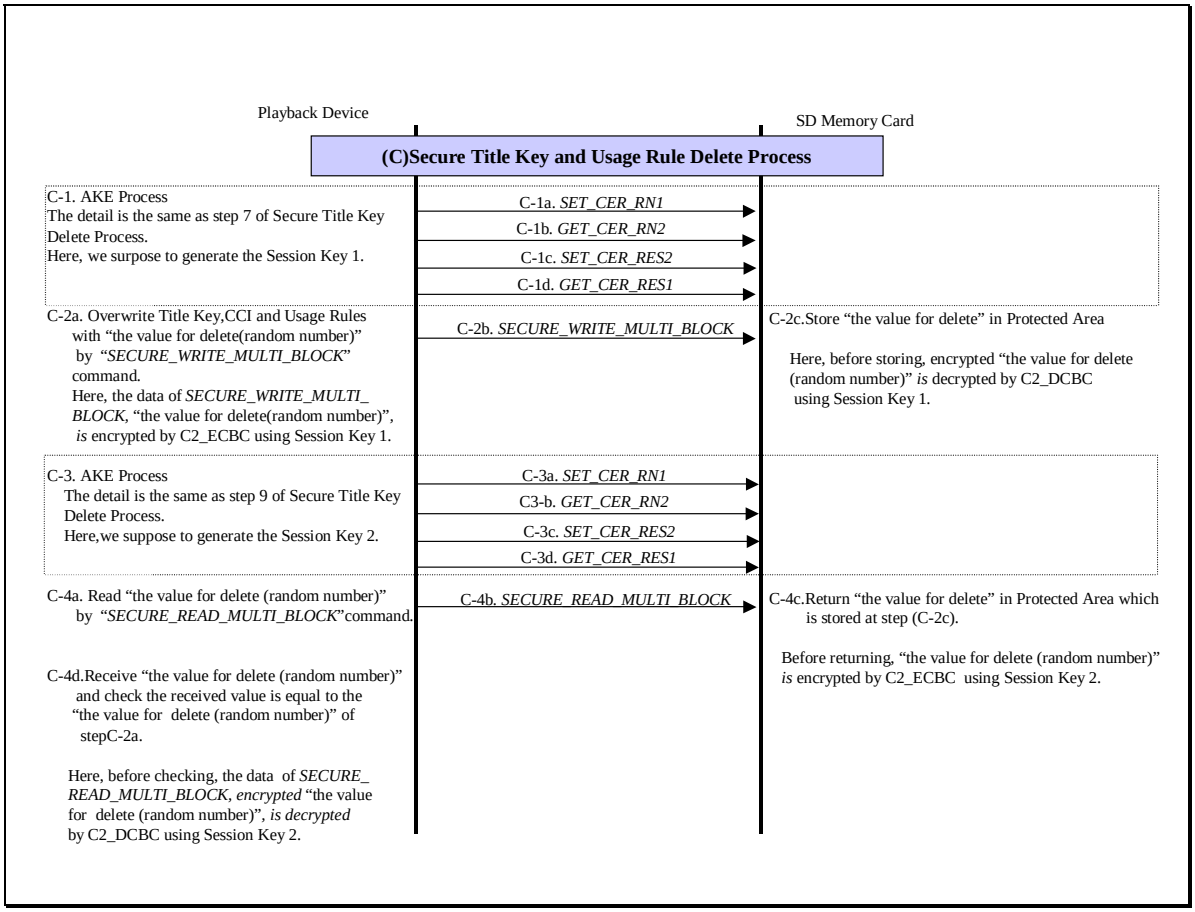


Figure C- 3– Protocol Flow of "Secure Title Key and Usage Rule Delete Process"

Note: In step (C2-a) of Figure C- 3, 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 Specifications – Part3 Security Specification*.

C.6 Encryption and Decryption Format

C.6.1 SD-Audio Object Encryption

The same formats described in Section 3.6.1 and 3.6.2 are applicable.

C.7 File System of the Protected Area

This section describes the additional directory and file configuration in Protected Area for Preview Extension. Almost the same directory and file configuration is used to store the Title Key, CCI and Usage Rule of SD-Audio content for preview as defined in Section 3.7. That is, the Title Key, CCI and Usage Rules of SD-Audio content for preview are encrypted by the Media Unique Key associated with MKB-U and stored in a single file (e.g. /SD_AUDIO/SD_ADPRV/P_AOBSA1.KEY, P_POBSP1.KEY) in the Protected Area.

C.7.1 Directory and File Configuration in Protected Area

Figure C- 4 shows an example directory and file configuration of the Protected Area.

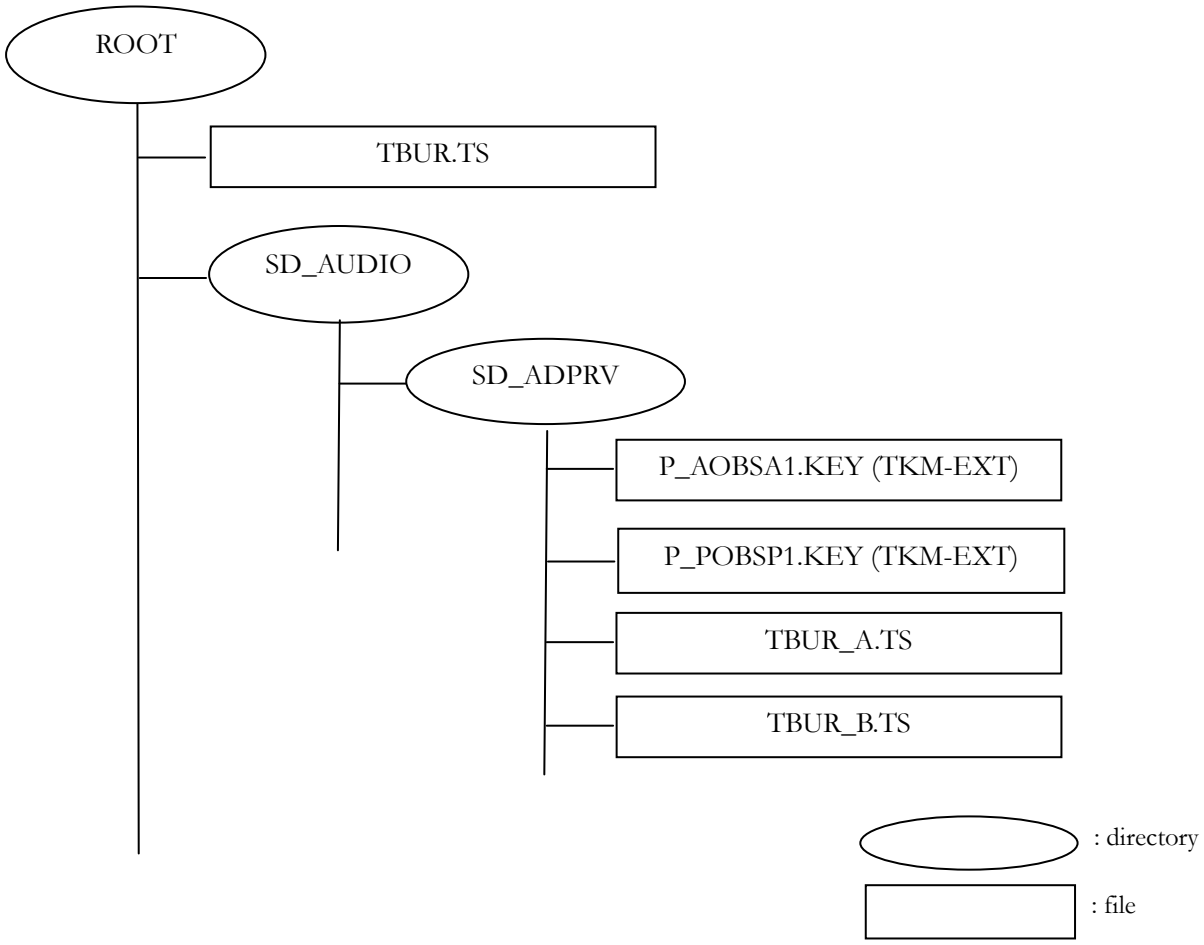


Figure C- 4– Directory and File Configuration for Preview Extension

For preview extension, the Extended Title Key Manager file for audio objects is named P_AOBSA1.KEY in the SD_AUDIO/SD_ADPRV directory in the Protected Area. It contains each of the Title Keys and Usage Rules for the audio content files, (the P_AOBxxx.SA1 files), which are stored in the SD_AUDIO/SD_ADPRV directory in the User Data Area.

P_POBSP1.KEY is the Extended Title Key Manager file that stores each of the Title Keys and Usage Rules for picture objects (the P_POBxxx.SP1 files), which are stored in User Data Area. It is in the SD_AUDIO/SD_ADPRV directory in the User Data Area.

The file name of the Extended Title Key Manager is determined according to the names of encrypted files in the User Data Area.

(1) Both the Protected Area and the User Data Area have file systems that are independent but are structured in the same way, as shown in Figure C- 5. The Extended Title Key Manager file and the encrypted content file are stored in the corresponding directories (e.g. in Figure C- 5, SD_AUDIO/SD_ADPRV).

(2) The file name of the Extended Title Key Manager file is a combination of the first five characters of the name of the encrypted content file in the User Data Area (e.g. In Figure C- 5, "P_AOB") and a file-name extension of the Extended Title Key Manager file (e.g. In Figure C- 5, "SA1").

(3) The file-name extension of the Extended Title Key Manager is '.KEY'.

(4) The number assigned to the encrypted content file name in the User Data Area corresponds to the Extended Title Key entry index in the Extended Title Key Manager (e.g. In Figure C- 5, "P_AOB00j.SA1" corresponds to the Extended Title Key Entry "#j").

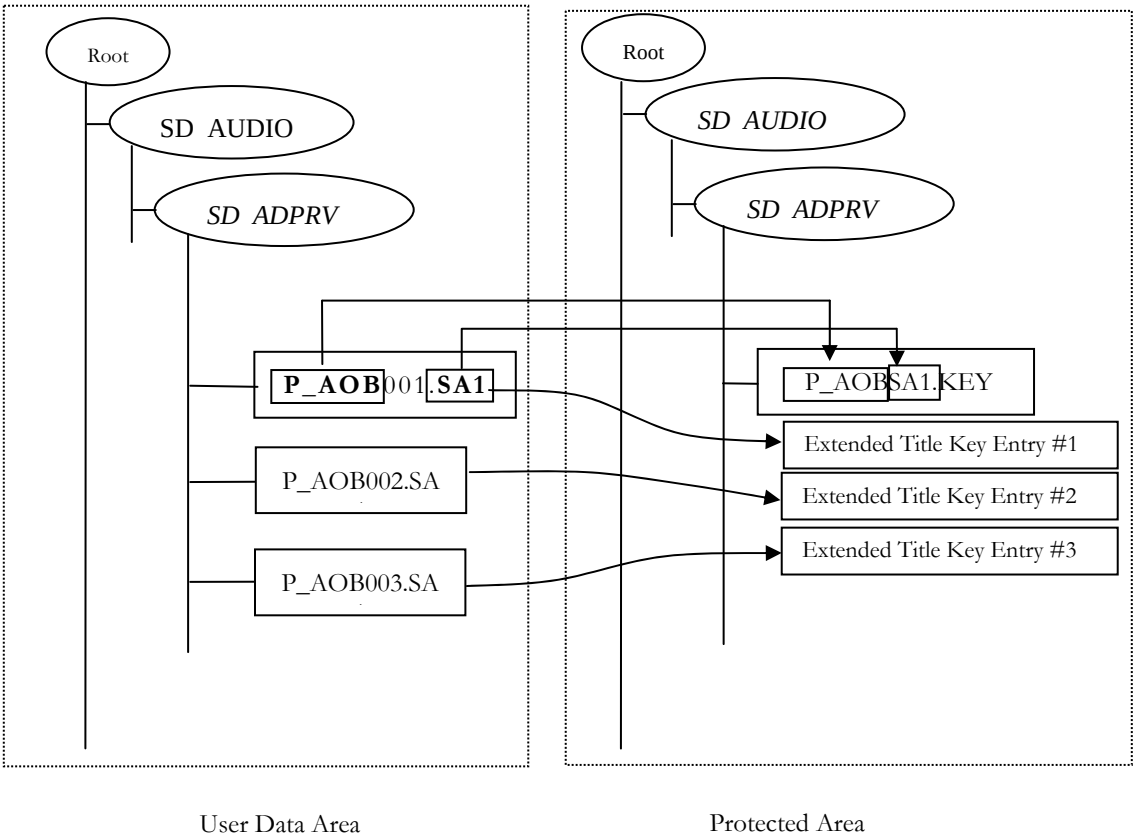


Figure C- 5– Relationship between Directory and File name

In order to assist devices to enforce time-based usage rules (TBUR), SD-Audio applications which support "Preview Extension" may store a timestamp in the Protected Area of the SD Memory Card. In the case where the SD-Audio content in the SD Memory Card includes time-based usage rules, at most three timestamp files, denoted TBUR_A.TS, TBUR_B.TS, and TBUR.TS, will appear in the Protected Area as shown in Figure C- 4.

- /SD_AUDIO/SD_ADPRV/TBUR_A.TS

  This timestamp file is handled by devices that work in Mode A described in section C.2. This file is encrypted and written with Mode = 1 specified in chapter 3 of *SD Specifications, Part 3: Security Specification*, that is, accessible only to SD-Audio application..

- /SD_AUDIO/SD_ADPRV/TBUR_B.TS

This timestamp file is handled by devices that work in Mode B described in section C.2. This file is also encrypted and written with Mode = 1 specified in chapter 3 of *SD Specifications, Part 3: Security Specification,* that is, accessible only to SD-Audio application.

- /TBUR.TS (Option)

  This timestamp file is handled by not only SD-Audio but other SD Applications (e.g. SD-Video). Handling this timestamp file is optional. This file is plaintext and written with Mode = 0 specified in chapter 3 of *SD Specifications, Part 3: Security Specification,2.00,* that is, accessible to all SD applications

The detail structure of each timestamp file is described in section C.7.3.

C.7.2 Extended Title Key Manager (TKMG-EXT)

C.7.2.1 Extended Title Key Manager (TKMG-EXT) Structure

Figure C- 6shows the structure of Extended Title Key Manager (TKMG-EXT).

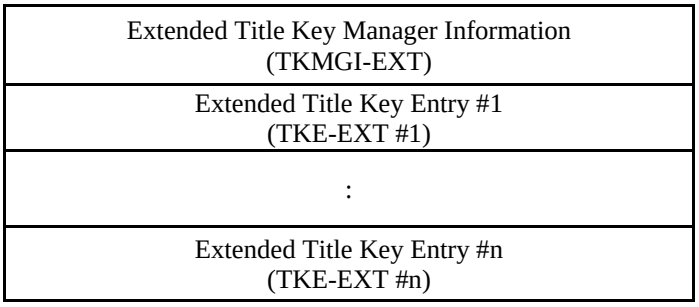


Figure C- 6– Extended Title Key Manager (TKMB-EXT)

Extended Title Key Manager (TKMG) consists of the Extended Title Key Manager Information (TKMGI-EXT) and a number of Extended Title Key Entries (TKE-EXTs). TKMGI-EXT is a 64-byte structure and consists of the TKMG-EXT Identifier, the size of TKMG-EXT, the attributes of Extended Title Key Entry (TKE-EXT), etc. Each TKE-EXT is 64-byte long and consists of the Encrypted Title Key, Encrypted CCI (Copy Control Information) the Content ID, and Encrypted Usage Rules.

C.7.2.2 Extended Title Key Manager Information (TKMGI-EXT)

As shown in Table C- 1, TKMGI-EXT consists of the size of TKMG-EXT, size of an Extended Title Key Entry, the number of Extended Title Key Entries, and other elements.

Table C- 1– TKMGI-EXT

TKMGI-EXT (Description order)

RBP	Field Name	Contents	Number of bytes
0 to 1	TKMGI-EXT_ID	TKMGI-EXT Identifier	2 bytes
2 to 3	VERN	Version number	2 bytes
4 to 7	TKMG-EXT_SZ	Size of TKMG-EXT	4 bytes
8 to 9	TKMG-EXT_AP_ID	Application Identifier of TKMG-EXT	2 bytes
10 to 11	TKE-EXT_N	The number of Extended Title Key Entries	2 bytes
12	TKE-EXT_SZ	Size of Extended Title Key Entry	1 byte
13	TKE-EXT_ATR	Attribute of Extended Title Key Entry	1 byte
14 to 63	Reserved	Reserved	50 bytes
Total			64 bytes

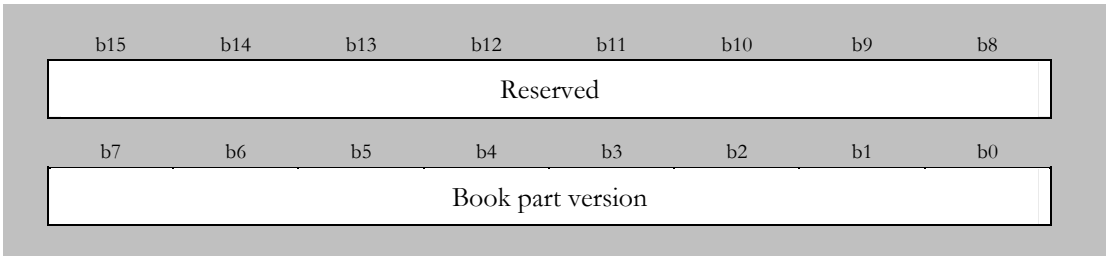
(RBP 0 to 1) TKMGI-EXT_ID

When the Extended Title Key Manager is associated with AOB (audio objects), the TKMGI-EXT_ID is "A1".
When the Extended Title Key Manager is associated with POB (picture objects), the TKMGI-EXT_ID is "P1".

All characters are in the standard ISO646 code.

(RBP 2 to 3) VERN

Describes the version number of the *SD Memory Card Specifications, Part 4: Audio Specifications.*



Book part version	11h: version 1.1
	Others : reserved

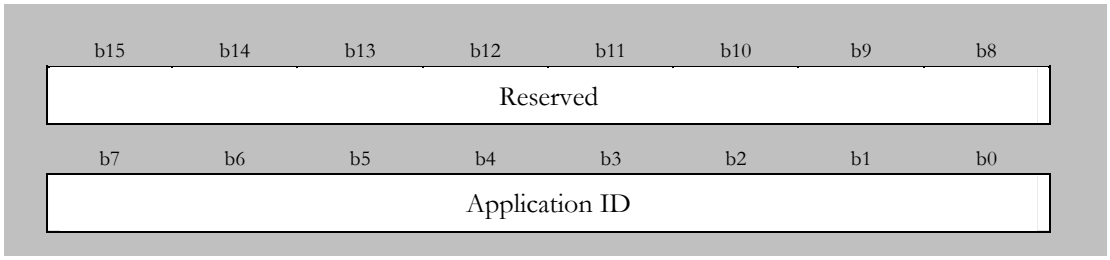
For forward compatibility, when the Book part version is more than '11h', the devices shall not treat it as an error.

(RBP 4 to 7) TKMG-EXT _SZ

Describes the data size of the TKMG-EXT in bytes. For SD-Audio Content for preview this value is fixed at '64000'.

(RBP 8 to 9) TKMG-EXT _AP_ID

Describes the Application ID of TKMG-EXT. For SD-Audio Content for preview, this value is the same number as the MKB number for SD-Audio extension for Move and Preview assigned by SD Association. For the MKB number, refer to Appendix C of *SD Specifications - Part3 Security Specification*.



Application ID	Stores the same number as the MKB number for SD-Audio extension for Move and Preview". For the MKB number, refer to *Appendix C of SD Specifications - Part3 Security Specification.*
	Others : reserved

(RBP 10 to 11) TKE-EXT _N

Describes the number of Extended Title Key Entries. For SD-Audio Content for preview this value is fixed at '999'.

(RBP 12) TKE-EXT _SZ

Describes data size of Extended Title Key Entry. For SD-Audio Content for preview this value is fixed at '64'.

(RBP 13) TKE-EXT _ATR

Describes the Extended Title Key Entry attribute. Indicates whether the Extended Title Key Entry includes CCI, in addition to the key. For SD-Audio Content for preview this value is fixed at '03h'.

C.7.2.3 Extended Title Key Entry (TKE-EXT)

As shown in Table C- 2, TKE-EXT consists of Extended Title Key Entries.

Table C- 2– TKE-EXT

TKE-EXT (Description order)

RBP	Field Name	Contents	Number of bytes
0 to 63	TKE-EXT	Extended Title Key Entry	64 bytes
Total			64 bytes

(RBP 0 to 63) TKE-EXT

Describes the Extended Title Key entry for each encrypted content file.

As shown in Table C- 3, the first 6 bits (from b506 to b511) of the TKE-EXT are reserved. The next 2 bits (from b504 to b505) are the CCI (Copy Control Information) in the first generation of SD-Audio. The next 56 bits (from b448 to b503) are the Title Key (EKEY field). The next bit (b447) is the Availability flag. The next 53 bits (from b394 to b446) are reserved. The next 10 bits (from b384 to b393) are a local Content ID. The last 48 bytes (from b0 to b383) are the Usage Rules field.

The first 8-byte field (from b448 to b511) of TKE-EXT and the last 48-byte field (from b0 to b383) are concatenated in that order and encrypted together using the Media Unique Key associated with MKB-U with C2_ECBC.

When the content is previewed at times specified by Preview Counter (i.e., it is no longer on the SD Memory Card), the first 8-byte field (from b448 to b511) and the last 48-byte field (from b0 to b383) of TKE-EXT shall be set to the random number using the Secure Title Key and Usage Rule Delete protocol described in section C.5.1 and the Availability flag field shall be set to '0'. Table C-3 shows the details of Extended Title Key Entry (TKE-EXT).

CCI	00b : Copying is permitted without restriction. 01b : reserved 10b : One generation of copies may be made. 11b : No more copying is permitted.
EKEY	Stores the Title Key.
Availability flag	0b : EKEY is not available. 1b : EKEY is available
Content ID	Stores the Content ID, which is used for locally identifying the content on the SD Memory Card by the SD-Audio Application. 1~999 are available as content IDs. If Content ID == 0, this means the TKE –EXT is not in use.

Trigger bit		Trigger bit for Preview extensions 0Xb: Accessing devices shall ignore fields b286 through b359 of TKE-EXT, that is, they shall ignore fields containing time-based usage rules. 10b: Accessing devices shall control the "Preview process" by "Preview Counter", "Preview Threshold", "Period control", and "Span control" 11b: Accessing devices of this specification shall not permit "Preview". Accessing devices conforming to this specification shall always set this Trigger bit value to either '0Xb' or '10b' as appropriate, when writing an encrypted content to an SD Memory Card. In a future version, the Preview Control Information would be expanded, or other information for controlling Preview would be added. Accessing devices of the future version shall process the new information for controlling Preview correctly when this bit is set to '11b'.
Preview Counter	…	00000000b: Preview is never permitted. 00000001b~11111110b: Preview is permitted specified times 11111111b: Preview is permitted unlimited times
Preview Threshold	…	00000000b~11111111b: specifies playback duration [by seconds], by which it is judged that one playback for preview has occurred and the Preview Counter is decremented by one.
Validity of Start Date		0b : The start date of permitted playback period is not specified. 1b : The start date of permitted playback period is specified.
First Playback Flag		This field describes whether or not the first playback has been performed when the playback span is specified. 0b : First playback has not been performed. 1b : First playback has been performed and so the Start Date and the End Date have already been fixed.
Start Date		This field describes the start date in Modified Julian Date format.
Start Time		This field describes the start time by the hour. 0 (00000b)~23 (10111b): Hours from midnight. others: Reserved.
Validity of End Date		0b : The end date of permitted playback period is not specified. 1b : The end date of permitted playback period is specified.
End Date		This field describes the end date in Modified Julian Date format

End Time		This field describes the end time by the hour 0 (00000b)~23 (10111b): Hours from midnight. others: Reserved.
Validity of Span		0b : The playback span is not specified. 1b : The playback span is specified.
Span Days		This field describes day portion of the permitted playback span.
Span Time		This field describes time portion of the permitted playback span by hours. 0 (00000b)~23 (10111b): Hours from midnight. others: Reserved.
Clock Usage flag		00b : No restriction for clock usage Preview is permitted for devices that have Clock A or Clock B1 or Clock B2. 01b :Reserve. 10b : Preview is permitted only for devices that have Clock B (i.e. Clock B1 or Clock B2). That is, the devices that work in Mode B (i.e. Mode B1 or Mode B2) can preview the content with 'Clock Usage flag' = '10b'. But the devices that work in Mode A can not preview the content with 'Clock Usage flag' = '10b'. 11b : Preview is permitted only for devices that have Clock B2. That is, the devices that work in Mode B2 can preview the content with 'Clock Usage flag' = '11b'. But the devices that work in Mode A or Mode B1 can not preview the content with 'Clock Usage flag' = '11b'.
Check Value	…	Stores the 64-bit Check Value 01234567 89ABCDEFh.

When the corresponding content is played for the first time, Start Date, Start Time, End Date, and End Time fields may change according to the validity of the playback span. For details how conforming devices shall change these fields, refer to the Playback process described in Section C.8 *Process Description* of this specification.

In SD-Audio, it is possible to divide a single audio content into several files. In that case, the Title Key (EKEY field) and Usage Rules field (Trigger bit, Preview Counter, and Preview Threshold) are treated in a special way. For example, say an audio content is divided into 'n' files, P_AOB00j.SA1 (j=1, 2, …, n). Then TKE-EXT#j is associated with audio file P_AOB00j.SA1, and:

(1) One of the TKE-EXTs shall have the following:

- Title Key stored in the EKEY field.
- "1" stored in the Availability flag field.
- Any number (1 ~ 999) stored in the Content ID field
- Trigger bit stored in the Trigger bit field

- Preview Counter and Preview Threshold stored in the Preview Counter and Preview Threshold fields
- Check Value “01234567 89ABCDEFh” stored in the Check Value field

(2) The other TKE-EXTs shall have the following:

- A random number stored in the EKEY field.
- “0” stored in the Availability flag field.
- The same content ID as above stored in the Content ID field.

An accessing device finds the Title Key and the Usage Rules (the Trigger bit, the Preview Counter and Preview Threshold) of the audio file P_AOB00j.SA1 as follows:

(i) The accessing device reads TKE-EXT#j and checks the Availability flag.

(ii) If the Availability flag == ‘0’, the device must find another TKE-EXT with the same Content ID whose Availability flag is ‘1’.

(iii) Upon finding such TKE-EXT, the accessing device decrypts the encrypted field (from b448 to b511 and from b0 to b383), reads the EKEY field and Usage Rules field and obtains the Title Key and Usage Rules (Trigger bit, Preview Counter, and Preview Threshold).

Note: All reserved bits within the TKE-EXT shall be set to ‘0’. Unless otherwise specified, for forward compatibility, devices shall ignore non-zero values in these fields.

Table C- 3– Detail of Extended Title Key Entry for Preview Content

b511	b510	b509	b508	b507	b506	b505	b504
Reserved						CCI	
b503	b502	b501	b500	b499	b498	b497	b496
EKEY [48…55]							
b495	b494	b493	b492	b491	b490	b489	b488
EKEY [40…47]							
b487	b486	b485	b484	b483	b482	b481	b480
EKEY [32…39]							
b479	b478	b477	b476	b475	b474	b473	b472
EKEY [24…31]							
b471	b470	b469	b468	b467	b466	b465	b464
EKEY [16…23]							
b463	b462	b461	b460	b459	b458	b457	b456
EKEY [8…15]							
b455	b454	b453	b452	b451	b450	b449	b448
EKEY [0…7]							
b447	b446	b445	b444	b443	b442	b441	b440
Availability flag	Reserved						
b439	b438	b437	b436	b435	b434	b433	b432
Reserved							
b431	b430	b429	b428	b427	b426	b425	b424
Reserved							
b423	b422	b421	b420	b419	b418	b417	b416
Reserved							
b415	b414	b413	b412	b411	b410	b409	b408
Reserved							
b407	b406	b405	b404	b403	b402	b401	b400
Reserved							
b399	b398	b397	b396	b395	b394	b393	b392
Reserved						Content ID[8,9]	
b391	b390	b389	b388	b387	b386	b385	b384
Content ID[0….7]							


b383 b382 b381 b380 b379 b378 b377 b376
Trigger Bit
Reserved
b375 b374 b373 b372 b371 b370 b369 b368
Preview Counter
b367 b366 b365 b364 b363 b362 b361 b360
Preview Threshold
b359 b358 b357 b356 b355 b354 b353 b352
Validity of Start Date
First Playback Flag
Start Date [16 .. 11]
b351 b350 b349 b348 b347 b346 b345 b344
Start Date [10 .. 3]
b343 b342 b341 b340 b339 b338 b337 b336
Start Date [2 .. 0]
Start Time [4 .. 0]
b335 b334 b333 b332 b331 b330 b329 b328
Validity of End Date
Reserved
End Date [16 .. 11]
b327 b326 b325 b324 b323 b322 b321 b320
End Date [10 .. 3]
b319 b318 b317 b316 b315 b314 b313 b312
End Date [2 .. 0]
End Time [4 .. 0]
b311 b310 b309 b308 b307 b306 b305 b304
Validity of Span
reserved
Span Days [16 .. 11]
b303 b302 b301 b300 b299 b298 b297 b296
Span Days [10 .. 3]
b295 b294 b293 b292 b291 b290 b289 b288
Span Days [2 .. 0]
Span Time [4 .. 0]
b287 b286 b285 b284 b283 b282 b281 b280
Clock Usage flag
reserved
b279 b278 b277 b276 b275 b274 b273 b272
Reserved
b271 b270 b269 b268 b267 b266 b265 b264
Reserved
b263 b262 b261 b260 b259 b258 b257 b256
Reserved

b255	b254	b253	b252	b251	b250	b249	b248
Reserved							

b247	b246	b245	b244	b243	b242	b241	b240
Reserved							

b239	b238	b237	b236	b235	b234	b233	b232
Reserved							

b231	b230	b229	b228	b227	b226	b225	b224
Reserved							

b223	b222	b221	b220	b219	b218	b217	b216
Reserved							

b215	b214	b213	b212	b211	b210	b209	b208
Reserved							

b207	b206	b205	b204	b203	b202	b201	b200
Reserved							

b199	b198	b197	b196	b195	b194	b193	b192
Reserved							

b191	b190	b189	b188	b187	b186	b185	b184
Reserved							

b183	b182	b181	b180	b179	b178	b177	b176
Reserved							

b175	b174	b173	b172	b171	b170	b169	b168
Reserved							

b167	b166	b165	b164	b163	b162	b161	b160
Reserved							

b159	b158	b157	b156	b155	b154	b153	b152
Reserved							

b151	b150	b149	b148	b147	b146	b145	b144
Reserved							

b143	b142	b141	b140	b139	b138	b137	b136
Reserved							

b135	b134	b133	b132	b131	b130	b129	b128
Reserved							

b127	b126	b125	b124	b123	b122	b121	b120
Reserved							
b119	b118	b117	b116	b115	b114	b113	b112
Reserved							
b111	b110	b109	b108	b107	b106	b105	b104
Reserved							
b103	b102	b101	b100	b99	b98	b97	b96
Reserved							
b95	b94	b93	b92	b91	b90	b89	b88
Reserved							
b87	b86	b85	b84	b83	b82	b81	b80
Reserved							
b79	b78	b77	b76	b75	b74	b73	b72
Reserved							
b71	b70	b69	b68	b67	b66	b65	b64
Reserved							
b63	b62	b61	b60	b59	b58	b57	b56
Check Value 01h							
b55	b54	b53	b52	b51	b50	b49	b48
Check Value 23h							
b47	b46	b45	b44	b43	b42	b41	b40
Check Value 45h							
b39	b38	b37	b36	b35	b34	b33	b32
Check Value 67h							
b31	b30	b29	b28	b27	b26	b25	b24
Check Value 89h							
b23	b22	b21	b20	b19	b18	b17	b16
Check Value ABh							
b15	b14	b13	b12	b11	b10	b9	b8
Check Value CDh							
b7	b6	b5	b4	b3	b2	b1	b0
Check Value EFh							

C.7.3 Time Based Usage Rules Time Stamp (TBUR.TS)

In SD-Audio, there are three timestamp files:

- timestamp file for devices that work in Mode A: \SD_AUDIO\SD_ADPRV\TBUR_A.TS (see C.7.3.1),

- timestamp file for devices that work in Mode B: \SD_AUDIO\SD_ADPRV\TBUR_B.TS (see C.7.3.2)

- timestamp file for not only SD-Audio but other SD Applications (e.g. SD-Video): \TBUR.TS (see C.7.3.3).

C.7.3.1 \SD_AUDIO\SD_ADPRV\TBUR_A.TS

TBUR_A.TS is handled by devices that work in Mode A described in Section C.2. More precisely, TBUR_A.TS shall be read and updated by devices that work in Mode A when a content with time-based usage rules is played or recorded.. The following table describes TBUR_A.TS.

Table C-4 \SD_AUDIO\SD_ADPRV\TBUR_A.TS

(Description order)

RBP	Field Name	Contents	Number of bytes
0 to 7	AN	Arbitrary Number	8 bytes
8 to 11	TS	Time Stamp Time	4 bytes
12 to 15	TS Verification Data	Time Stamp Verification Data	4 bytes
Total			16 bytes

The whole \SD_AUDIO\SD_ADPRV\TBUR_A.TS file is encrypted using C2_ECBC by the Media Unique Key (K_{mu}) associated with MKB for Usage Rule (MKB-U) described in Section A.3.1.1.. This encryption is performed with the same media unique key as the one used to encrypt TKE-EXT, that is, the media unique key calculated by processing both the base MKB and the MKB extension. (as described in Section 3.9 of *SD Memory Card Book Common Part.)*

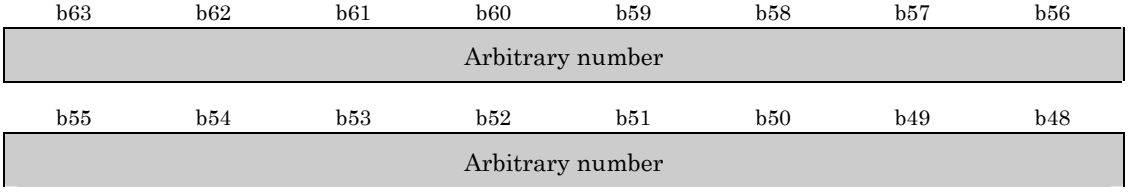
Namely, \SD_AUDIO\SD_ADPRV\TBUR_A.TS contains Encrypted Time Stamp Data (D_{tse}) as:

D_{tse} = C2_ECBC(K_{mu}, D_{ts}),

where D_{ts}= {AN||TS||TS Verification Data}

(RBP 0 to 7) AN

This field stores the 64-bit arbitrary number. For example, a random number may be stored in this field.



b47	b46	b45	b44	b43	b42	b41	b40
Arbitrary number							
b39	b38	b37	b36	b35	b34	b33	b32
Arbitrary number							
b31	b30	b29	b28	b27	b26	b25	b24
Arbitrary number							
b23	b22	b21	b20	b19	b18	b17	b16
Arbitrary number							
b15	b14	b13	b12	b11	b10	b9	b8
Arbitrary number							
b7	b6	b5	b4	b3	b2	b1	b0
Arbitrary number							

Arbitrary Number ... This field describes the 64-bit arbitrary number

(RBP 8 to 11) TS

This field describes the a timestamp indicating the date and time of the last time any content with time-based usage rules was played or recorded by devices that work in Mode A, a card 'In-Use' flag, and a 'Exception Termination' counter to keep track of how many times unexpected termination of playback has occurred while playing content with date and time-based usage rules.

The devices that work in Mode A use the 'In-Use' flag and the 'Exception Termination' counter to keep track of situations where playback is attempted after pulling the card during playback. Note that while pulling the card effectively stops playback it does not allow the Playback devices to update the timestamp file. Playback devices increment the 'Exception Termination' counter when a "Pull Card Attack" is detected. An SD Memory Card is considered to be in-use if

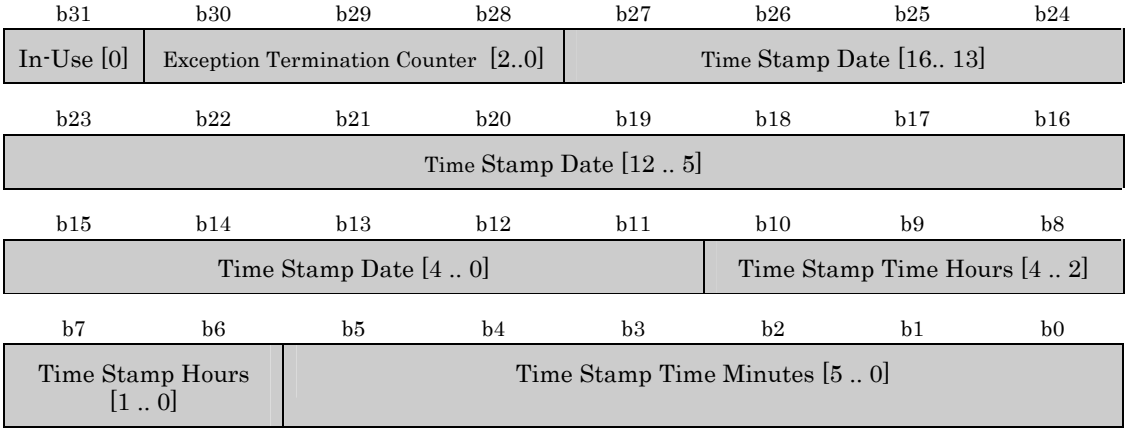
- A device started playing content with time-based usage rules
- A device resumes playback of content with time-based usage rules.

An SD Memory Card is considered not to be in-use if

- Any devices are playing content that does not have time-based usage rules.
- A Mode A device has finished playing content that has time-based usage rules.

Details on how to update the 'In-Use' flag and 'Exception Termination' counter are explained in Section C.8 *Process Definition* of this specification. In the case of the TBUR_A.TS in the \SD_AUDIO\SD_ADPRV directory, this TBUR_A_TS field shall be encrypted according to the process similar to the "Encrypt Title Key and CCI process" described in Section 3.4(4a) of the CPRM *SD Memory Card Book Common Part*.

Notice that the SD Memory Card can distinguish between content that has never been played and content for which the first playback has been performed, that is, 'currently active'. A 'currently active' content is one that is not in the 'period' state but in the 'start' and 'end' state. That is, for active content the Start Date and the End Date have been fixed.



In-Use ... This field describes if the SD Memory Card is being used by a device. That is, playback of content with time-based usage rules has started playing. Playback of content without time-based usage rules should not modify this flag.

0b : the timestamp was last updated: a) after stopping playback , b) after playback has reached the end of the content .

1b : the timestamp was last updated at the start of a playback .

Exception Termination Counter ... This field how many times playback of content has been terminated unexpectedly. Normal termination is defined as either using the STOP control function or playing back until the end of the content is reached. Pulling the card from a device while playing content with date and time usage rules is considered an exception. In contrast, playback of content without date and time usage rules always stops smoothly. That is, pulling the card in this case shall not impact the Exception Termination Counter.

0 (000b)~5 (101b): valid values for this counter. When the number of exception terminations reaches 5, it results on denying playback of currently active content until conditions for compliant playback are met. For details on how to reach such compliant conditions see C.8.2 Preview Process of this specification.

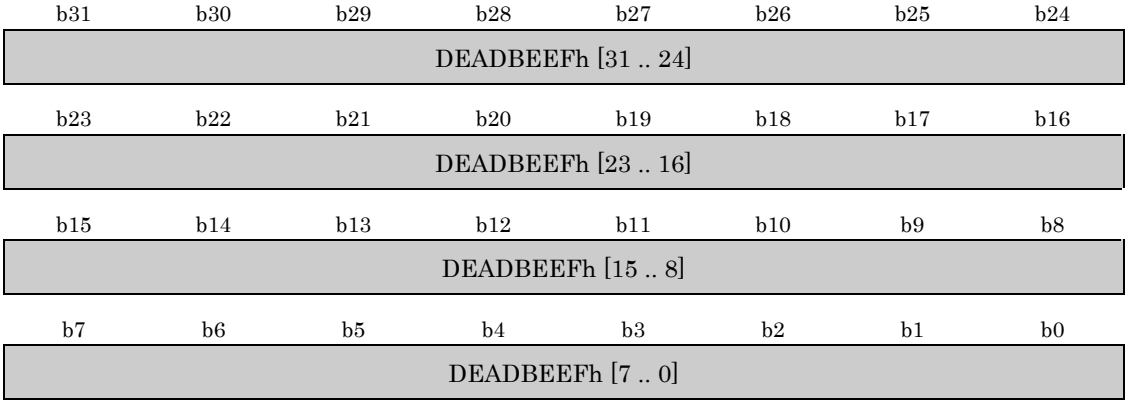
Others: Reserved

TimeStamp Date ... This field describes the current timestamp date in Modified Julian Date format.

TimeStamp Time Hours	...	This field describes the current timestamp by the hour. 0 (00000b) ~23 (10111b): Hours from midnight. others: Reserved.
TimeStamp Time Minutes	...	This field describes the current timestamp by the minutes. 0 (00000b) ~59 (111011b): minutes after the hour stated in TimeStamp Time Hours field. others: Reserved.

(RBP 12 to 15) TS Verification Data

This field stores the 32-bit Verification Data, DEADBEEFh.



Verification Data	...	This field describes the verification data DEADBEEFh

Note: All reserved bits within the TBUR_A.TS shall be set to '0'. Unless otherwise specified, for forward compatibility, devices shall ignore non-zero values in these fields.

If encrypted timestamp file is decrypted successfully, as described below, bytes 12 through 15 contain the value DEADBEEFh, bytes 8 to 11 contain the Time Stamp. Using its current K_{mu} value, the device calculates Time Stamp Data (D_{ts}) as:

$$D_{ts} = C2\_DCBC(K_{mu}, D_{tse}).$$

The device shall not playback CPRM encrypted content with date and time-based usage rules until the following condition is successfully verified:

$$[D_{ts}]_{lsb\_32} = DEADBEEFh$$

C.7.3.2 \SD_AUDIO\SD_ADPRV\TBUR_B.TS

TBUR_B.TS is handled by devices that work in Mode B described in Section C.2. More precisely, to keep the accuracy of the timestamp, TBUR_B.TS shall be updated by only devices that work in Mode B2 when content is recorded. The following table describes TBUR_B.TS.

Table C-5 \SD_AUDIO\SD_ADPRV\TBUR_B.TS

(Description order)

RBP	Field Name	Contents	Number of bytes
0 to 7	AN	Arbitrary Number	8 bytes
8 to 11	TS	Time Stamp Time	4 bytes
12 to 15	TS Verification Data	Time Stamp Verification Data	4 bytes
Total			16 bytes

The whole \SD_AUDIO\SD_ADPRV\TBUR_B.TS file is encrypted using C2_ECBC by the Media Unique Key (K_{mu}) associated with MKB for Usage Rule (MKB-U) described in Section A.3.1.1. This encryption is performed with the same media unique key as the one used to encrypt TKE-EXT, that is, the media unique key calculated by processing both the base MKB and the MKB extension. (as described in Section 3.9 of *SD Memory Card Book Common Part.)*

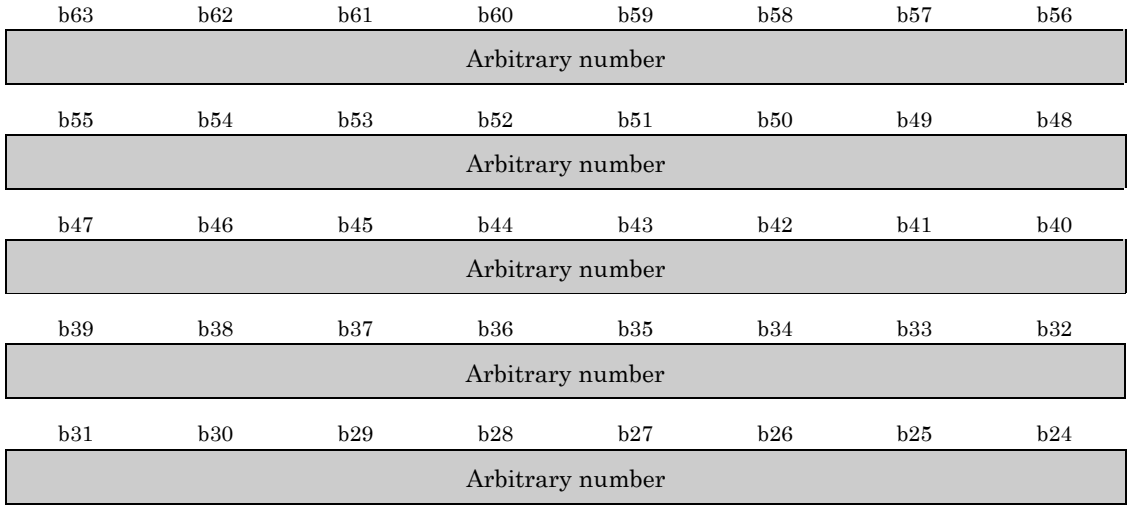
Namely, \SD_AUDIO\SD_ADPRV\TBUR_B.TS contains Encrypted Time Stamp Data (D_{tse}) as:

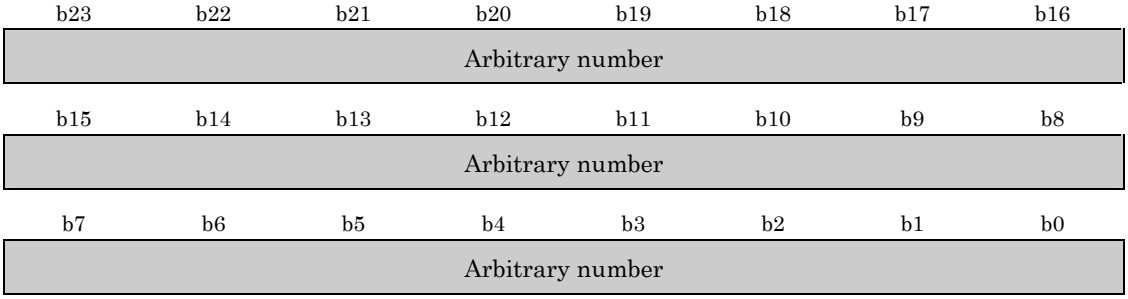
$$D_{tse} = C2\_ECBC(K_{mu}, D_{ts}),$$

where $D_{ts} = \{AN||TS||TS\ Verification\ Data\}$

(RBP 0 to 7) AN

This field stores the 64-bit arbitrary number. For example, a random number may be stored in this field.

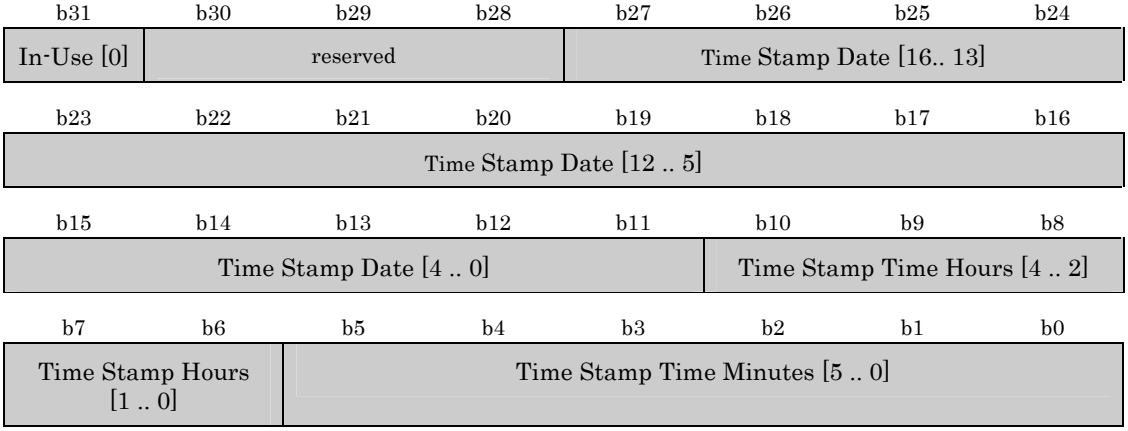




Arbitrary Number ... This field describes the 64-bit arbitrary number

(RBP 8 to 11) TS

This field describes the a timestamp indicating the date and time of the last time any content with time-based usage rules was recorded by the devices that works in Mode B and 'In-Use'.



In-Use ... This field describes if the timestamp in TBUR_B.TS file has been used to set Clock B1 by a device that works in Mode B1..

0b : the device that works in Mode B1may use the timestamp in TBUR_B.TS to ser Clock B1 when this flag = "0b".

1b : the device that works in Mode B1 shall not use the timestamp in TBUR_B.TS to set Clock B1 when this flag = "1b".

Note: The definition of "In-Use" in TBUR_B.TS is different from "In-Use" in TBUR_A.TS .

TimeStamp Date ... This field describes the current timestamp date in Modified Julian Date format.

TimeStamp Time Hours ... This field describes the current timestamp by the hour.

0 (00000b) ~23 (10111b): Hours from midnight.

others: Reserved.

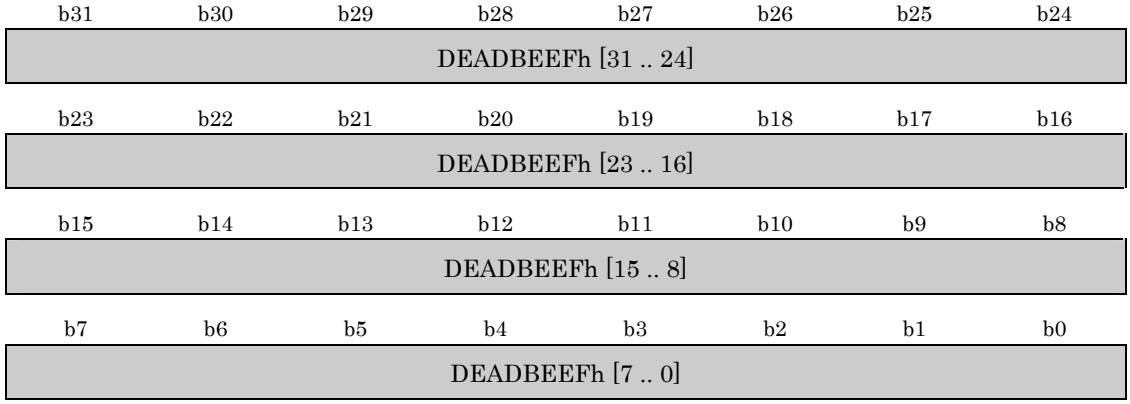
TimeStamp Time Minutes ... This field describes the current timestamp by the minutes.

0 (00000b) ~59 (111011b): minutes after the hour stated in TimeStamp Time Hours field.

others: Reserved.

(RBP 12 to 15) TS Verification Data

This field stores the 32-bit Verification Data, DEADBEEFh.



Verification Data ... This field describes the verification data DEADBEEFh

Note: All reserved bits within the TBUR_A.TS shall be set to '0'. Unless otherwise specified, for forward compatibility, devices shall ignore non-zero values in these fields.

If encrypted timestamp file is decrypted successfully, as described below, bytes 12 through 15 contain the value DEADBEEFh, bytes 8 to 11 contain the Time Stamp. Using its current K_{mu} value, the device calculates Time Stamp Data (D_{ts}) as:

$$D_{ts} = C2\_DCBC(K_{mu}, D_{tse}).$$

The device shall not playback CPRM encrypted content with date and time-based usage rules until the following condition is successfully verified:

$$[D_{ts}]_{lsb\_32} = DEADBEEFh$$

C.7.3.3 \TBUR.TS

TBUR.TS is handled by any SD Applications. More precisely, it is optional, but recommended, for devices that work in Mode A or Mode B to update TBUR.TS. The following table describes TBUR.TS.

Table C-6 \TBUR.TS

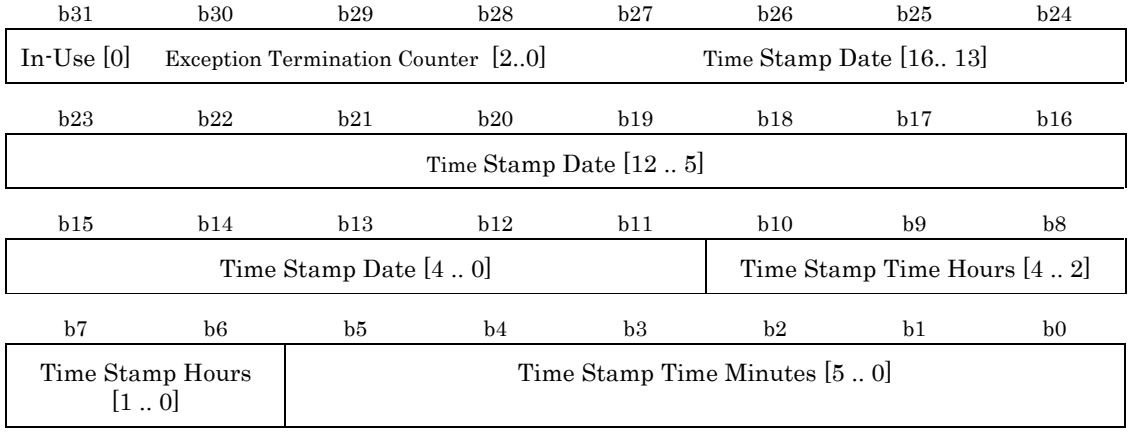
(Description order)

RBP	Field Name	Contents	Number of bytes
0 to 3	TS	Time Stamp Time	4 bytes
4 to 7	Reserved	Reserved	4 bytes
Total			8 bytes

This \TBUR.TS file does not contain an Arbitrary Number and a Verification Data because the file is not encrypted.

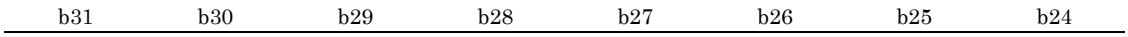
(RBP 0 to 3) TS

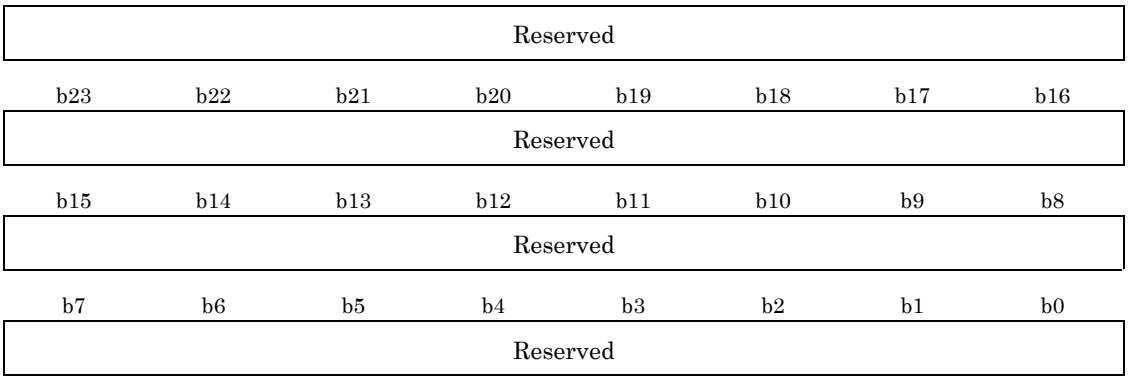
This field describes a timestamp field indicating the date and time of the last time any content was played or recorded by a compliant device, a card 'In-Use' flag, and a counter to keep track of how many times unexpected termination of playback has occurred while playing content with date and time-based usage rules.



Fields in TS describing the Time Stamp have the same meaning as in the \SD_AUDIO\SD_ADPRV\TBUR_A.TS file, except that they are not encrypted.

(RBP 4 to 7) Reserved





C.7.3.4 Processing the timestamp files in Mode A

The process of recording and updating the timestamp files (TBUR_A.TS and TBUR.TS) by the device that works in Mode A is described as follows:

- When recording the downloaded content with time-based usage rules, the device that works in Mode A shall record a timestamp in the TBUR_A.TS in the SD_AUDIO\SD_ADPRV directory and may record a timestamp in the TBUR.TS in the Root directory.
- When playing the content with time-based usage rules, the device that works in Mode A shall update the timestamp in the TBUR_A.TS in the SD_AUDIO\SD_ADPRV directory and may update the timestamp in the TBUR.TS in the Root directory.

All devices are allowed to update the timestamp in the TBUR.TS file located in the Root directory. Devices that do not have clock functions described in C.2 shall not play content with time-based usage rules; hence they shall ignore the timestamp files. Details on the procedures to update timestamp files are described in Section C.8*Process Description* of this specification. For instance, one fundamental rule is that the timestamp can only be updated to a later time. A device with time-based usage capabilities

- The device shall choose one of the following rules to calculate the reference time: 1) compare the two timestamps (\TBUR.TS and \SD_AUDIO\SD_ADPRV\TBUR_A.TS) and set the reference time to be the timestamp with the later date and, time or 2) set the reference time to the timestamp in the \SD_AUDIO \SD_ADPRV directory.
- If the time derived from the device is later than the reference time stamp, the reference time shall be set to the time derived from the device.
- Shall update the time stamp TBUR_A.TS in the SD_AUDIO\SD_ADPRV directory (\SD_AUDIO\SD_ADPRV\TBUR_A.TS) to the reference time.
- It is optional for a device to update the TBUR.TS in Root directory (\TBUR.TS).

The devices that work in Mode A are required to update the timestamp when they begin playback, stop playback (using STOP control function), or end playback (reach the end of the content). The TBUR_A.TS in the SD_AUDIO\SD_ADPRV directory records the last time that devices that work in Mode A used the SD Memory Card. Analogously, the TBUR.TS in the Root directory is intended to record the last time any compliant application used the card.

Updating the TBUR.TS file in the Root directory by compliant applications, is not mandatory. However, it is strongly recommended that such update be performed by all applications since it results in a more up-to-date time stamp. Devices that work in Mode A shall update the timestamp files in the SD_AUDIO\SD_ADPRV directory and may update the timestamp files in the Root directory with the same data. If there is no timestamp

file when the SD Memory Card gets content with time-based usage rules, the file shall be created. Details on the initial content for this file are described in Recording Process, Section C.8.1of this specification.

Response to the existence of date and time-based usage rules is required in devices subject to this Specification. Such response may be in the form of not playing content marked with such rules or in the form of supporting the following:

- Before conrtent is played or recorded the device that work in Mode A must read the timestamp in the SD Memory Card. The device shall read the timestamp in the TBUR_A.TS file in the SD_AUDIO\SD_ADPRV directory. and may read the timestamp in the TBUR.TS file in the Root Directory in the Protected Area. The device shall choose the later of the two timestamp as the reference timestamp, if it reads the timestamp in the TBUR.TS file in the Root Directory. If the timestamp in the SD Memory Card is later than Clock A, the device must refuse to play or record such content
- Every time a device plays or records content with time-based usage rules, the device is required to write the current time to the SD Memory Card. The time is stored in timestamp files in the Protected Area: the TBUR_A.TS file in the SD_AUDIO\SD_ADPRV directory, and the TBUR.TS file in the root directory. The device shall not write a date that is earlier than the reference timestamp in the SD Memory Card.
- The device is required to write the current time to the TBUR_A.TS timestamp file in the SD_AUDIO\SD_ADPRV directory at least at the following times:
    - before it starts playing the content.
    - after it finishes playing the content.
    - every time playback is stopped smoothly, i.e. using the STOP function. Pulling the card stops the playback of the content; however, it is consider an unexpected termination. Pulling the card can eventually affect the rental.
- Devices are required to set the ‘In-Use’ flag to ‘1b’ when it starts playing content with time-based usage rules, and to set the In-Use’ flag to ‘0b’ when it stops playback smoothly.
- Devices are required to update the ‘Exception Termination Count’ when it plays the content and the ‘in-use’ flag is ‘1b’, that is, playback was not stopped smoothly.

C.7.3.5 Processing the timestamp files in Mode B

The process of recording and updating the timestamp file by the device that works in Mode B is described as follows:

- To keep the accuracy of the timestamp, when recording the downloaded content with time-based usage rules, only devices that work in Mode B2 shall record the timestamp in the TBUR_B.TS file in the SD_AUDIO\SD_ADPRV directory and devices that work in Mode B1shall not record the timestamp in the TBUR_B.TS file in the SD_AUDIO\SD_ADPRV directory.
- When playing the content with time-based usage rules, devices that work in Mode B (i.e. Mode B1 or Mode B2) do not need to update the timestamp in the TBUR_B.TS file in the SD_AUDIO\SD_ADPRV directory.
- It is optional for the devices that work in Mode B to record or update the TBUR.TS in the Root directory.

Details on the procedures to update timestamp files are described in Section C.8 *Process Description* of this specification.

Moreover, the process of adjusting Clock B1 by devices that work in Mode B1 is described as follows

- When an SD Memory Card is inserted, or when an application starts or when device turns on, devices that work in Mode B1shall read the timestamp in the TBUR_B.TS file in the SD_AUDIO\SD_ADPRV directory.
- When the timestamp in TBUR_B.TS is later than Clock B1, the devices that work in Mode B1 shall adjust the Clock B1 identically to the timestamp in TBUR_B.TS and set 'In-use' in TBUR_B.TS to '1b'.
- When Clock B1 is later than the timestamp in TBUR_B.TS and 'In-use' in TBUR_B.TS is '0b', the devices that work in Mode B1 shall adjust Clock B1 identically to the timestamp in TBUR_B.TS and set the 'In-use' to '1b'.

C.8 Recording and Preview

This section describes the Recording and Preview processes:

- Section C.8.1 describes the Recording Process for devices that work in Mode A
- Section C.8.2 describes the Recording Process for devices that work in Mode B
- Section C.8.3 describes the Preview processes for devices that work in Mode A
- Section C.8.4 describes the Preview processes for devices that work in Mode B.

Regarding the definition of Mode A devices/Mode B devices, see section C.2.

In the following protocols, regarding the Secure Read Process, the Secure Write Process, the Secure Title Key Delete Process and the AKE Process, refer to Sections 3.5.1, 3.5.2, 3.5.3 and 3.4.1 of the *Common Part* of the *CPRM SD Memory Card Book* and regarding the Secure Title Key and Usage Rule Delete Process, refer to Section C.5.

C.8.1 Recording Process in Mode A

This section describes the Recording Process for devices that work in Mode A. The Recording Device securely holds information associated with SD-Audio Content for Preview. The information includes and Usage Rules given by the Content Provider and a secret unpredictable Title Key (e.g., given by the Content Provider or selected at random). In the case of recording the content with time-based Usage Rule, Recording Devices that work in Mode A shall update the timestamp in TBUR_A.TS file and may update the timestamp in TBUR.TS in step (4).In the case of recording the content without time-based Usage Rule, step (4) is skipped.

(1) Read the Extended Title Key Manager (TKMG-EXT) file from the SD Memory Card

The Recording Device securely reads the Extended Title key Manager (TKMG-EXT) file, P_AOBSA1.KEY, from the SD Memory Card using the Secure Read Process after the AKE Process using the Media Unique Key associated with MKB-U.

(2) Update the Extended Title Key Entry (TKE-EXT) in the TKMG-EXT file

The Recording Device finds a TKE-EXT that is not in use, and updates the Content ID field with the number that has not been currently assigned in the TKMG-EXT file on this SD Memory Card. It also updates the EKEY field, CCI field, and the Usage Rule field (the Trigger bit field, Preview Counter field, Preview Threshold field, Period control field, and Span control field and Check Value field) and the Availability flag field of the TKE-EXT.

(3) Write updated TKMG-EXT file to the SD Memory Card

The Recording Device securely writes the TKMG-EXT file including the updated TKE-EXT as the new TKMG-EXT file to the SD Memory Card using the Secure Write Process after the AKE process using Media Unique Key associated with MKB-U.

(4) Update or create Timestamp File

The Recoding Device records SD-Audio content onto the SD Memory Card. The Recoding Device shall update the timestamp to the current time only if the timestamp already on the SD Memory Card has a time no later than the current time. That is, the Recoding Device shall not overwrite or update a timestamp indicating the future time. The Recoding Device is allowed to record content when the timestamp is indicating the future time (a compliant playback device shall refuse to play such content until the timestamp catches up with the current time). A Recording Device shall perform the following steps:

- If the \SD_AUDIO\SD_ADPRV\TBUR_A.TS exists, the Recording Device that works in Mode A shall check the verification of the 'DEADBEEFh' hexadecimal value in this timestamp file. If this check fails, this process shall be aborted.
    - The Recording Device that works in Mode A shall read the timestamp from this timestamp file and set the reference time to the timestamp.
    - If the reference time is in the past, the Recording Device that works in Mode A shall write the current time to this timestamp file and set In-Use = '0b' and ETC = '0h' on this timestamp file.
    - If the reference time is in the future, the Recording Device that works in Mode A shall write the reference time to this timestamp file and set In-Use = '0b', and ETC unchanged on this timestamp file.
- If the \SD_AUDIO\SD_ADPRV\TBUR_A.TS does not exist, the Recording Device that works in Mode A shall create \SD_AUDIO\SD_ADPRV\TBUR_A.TS, and shall write the current time to this timestamp file and set In-Use = '0b' and ETC = '0h' on this timestamp file..
- For Recording Devices that work in Mode A, it is optional to update or create the \TRUR.TS file. The Recording Device that works in Mode A may execute the following steps:
    - If \TBUR.TS does not exist, the Recording Device that works in Mode A may create \TBUR.TS file and write the current time to \TBUR.TS and set In-Use = '0b' and ETC = '0h' on\TBUR.TS.
    - If \TBUR.TS exists and the timestamp in \TBUR.TS is in the past, the Recording Device that works in Mode A may write the current time to \TBUR.TS and set In-Use = '0b' and ETC = '0h' on\TBUR.TS.

To protect against the "Pull Card Attack", the Recording Device must assume that Recording process has been completely done, when any error occur in step (3) and step (4).

C.8.2 Recording Process in Mode B

This section describes the Recording Process for devices that work in Mode B. The Recording Device securely holds information associated with SD-Audio Content for Preview. The information includes and Usage Rules given by the Content Provider and a secret unpredictable Title Key (e.g., given by the Content Provider or selected at random).

In the case of recording the content with time-based Usage Rule, to keep the accuracy of the timestamp, only Recording Devices that work in Mode B2 shall update the timestamp in TBUR_B.TS file in the SD_AUDIO\SD_ADPRV directory in step (4) and Recording Devices that work in Mode B1 shall not update the timestamp in TBUR_B.TS file. It is optional for devices that work in Mode B to update the timestamp in TRUR.TS file in the root directory.

In the case of recording the content without time-based Usage Rule, step (4) is skipped.

(1) Read the Extended Title Key Manager (TKMG-EXT) file from the SD Memory Card

The Recording Device securely reads the Extended Title key Manager (TKMG-EXT) file, P_AOBSA1.KEY, from the SD Memory Card using the Secure Read Process after the AKE Process using the Media Unique Key associated with MKB-U.

(2) Update the Extended Title Key Entry (TKE-EXT) in the TKMG-EXT file

The Recording Device finds a TKE-EXT that is not in use, and updates the Content ID field with the number that has not been currently assigned in the TKMG-EXT file on this SD Memory Card. It also updates the EKEY field, CCI field, and the Usage Rule field (the Trigger bit field, Preview Counter field, Preview Threshold field, Period control field, Span control field and Check Value field) and the Availability flag field of the TKE-EXT.

(3) Write updated TKMG-EXT file to the SD Memory Card

The Recording Device securely writes the TKMG-EXT file including the updated TKE-EXT as the new TKMG-EXT file to the SD Memory Card using the Secure Write Process after the AKE process using Media Unique Key associated with MKB-U.

(4)Update and write Timestamp File

The Recoding Device records SD-Audio content onto the SD Memory Card. The Recoding Device shall update the timestamp to the current time only if the timestamp already on the SD Memory Card has a time no later than the current time. That is, the Recoding Device shall not overwrite or update a timestamp indicating the future time. The Recoding Device is allowed to record content when the timestamp is indicating the future time (a compliant playback device shall refuse to play such content until the timestamp catches up with the current time). A Recording Device shall perform the following steps:

- If the \SD_AUDIO\SD_ADPRV\TBUR_B.TS exists, the Recording Device that works in Mode B2 shall check the verification of the 'DEADBEEFh' hexadecimal value in this timestamp file. If this check fails, this process shall be aborted.
    - The Recording Device that works in Mode B2 shall read the timestamp from this timestamp file and set the reference time to the timestamp.
    - If the reference time is in the past, the Recording Device that work in Mode B2 shall write the current time to this timestamp file.
    - If the reference time is in the future, the Recording Device that work in Mode B2 shall write the reference time to this timestamp file.
- If the \SD_AUDIO\SD_ADPRV\TBUR_B.TS does not exist, the Recording Device that works in Mode B2 shall create \SD_AUDIO\SD_ADPRV\TBUR_B.TS, and shall write the current time to this timestamp file.
- The Recording Device that works in Mode B1 shall not update nor create \SD_AUDIO\SD_ADPRV\TBUR_B.TS.
- For Recording Devices that work in Mode B (Mode B1 and Mode B2), it is optional to update or write the \TRUR.TS file. The Recording Device that works in Mode B may execute the following steps:
    - If \TBUR.TS does not exist, the Recording Device that works in Mode B may create \TBUR.TS file and write the current time to \TBUR.TS and set In-Use = '0b' and ETC = '0h' on\TBUR.TS.
    - If \TBUR.TS exists and the timestamp in \TBUR.TS is in the past, the Recording Device that works in Mode B may write the current time to \TBUR.TS and set In-Use = '0b' and ETC = '0h' on\TBUR.TS.

To protect against the "Pull Card Attack", the Recording Device must assume that Recording process has been completely done, when any error occur in step (3) and step (4).

C.8.3 Preview Process in Mode A

This section describes the Preview Process for devices tha work in Mode A. In the case of playback the content without time-based Usage Rule, step (6) (7), (11) are skipped.

(1) Read the Extended Title Key Entry (TKE-EXT) from the SD Memory Card

The Playback Device securely reads the Extended Title Key Entry (TKE-EXT) associated with the SD-Audio content for Preview in the Extended Title Key Manager (TKMG-EXT) file, P_AOBSA1.KEY, from the SD Memory Card using Secure Read Process after the AKE Process using the Media Unique Key associated with MKB-U.

(2) Check the Usage Rules (Phase1)

The Playback Device checks the Extended Title Key Entry (TKE-EXT)

- If the Check Value is not '0123456789ABCDEFh,' then the process shall be aborted.
- If Trigger bit fields are "11b", playback is not allowed, hence the process shall be aborted.
- If Clock Usage Flag is equal to '1Xb' or '01b', then the process shall be aborted.
- The Playback Device checks the Preview Counter field and judges whether the content is allowed to be previewed or not. If the Preview Counter is equal to zero, the process is aborted.
- If the Playback Device does not have clock functions described in section C.2, the process shall be aborted.
- If the Trigger bit fields are '00b,' or '01b', content does not have time-based usage rules (i.e. Period Control, Span Control), go to step (9) .That is, any Playback Device shall ignore time-based rules and proceed to playback content

The Playback Device checks the Validity of Start Date field, the Validity of End Date field, and the Validity of Span field. When all the above fields are equal to '0b,' that is, all fields have not been set, go to step (6).

(3) Obtain current date and time.

The Playback Device obtains the current date and time by referring to its internal clock (Clock A). If the Playback Device cannot obtain the current date and time, then the process shall be aborted.

(4) Update the TKE-EXT

The Playback Device checks the First Playback Flag field and the Validity of Span field. When the First Playback Flag field is equal to '1b' or the Validity of Span field is equal to '0b,' go to step (5).

(4.1) Update the Start Date of Playback Period.

a) When the Validity of Start Date field is equal to '0b,' the Playback Device sets the Start Date of Playback Period field to the current date and time and sets the Validity of Start Date field to '1b.'

b) When the Validity of Start Date field is equal to '1b,' the Playback Device compares the current date and time with the date and time of the Start Date of Playback Period field.

- If the current date and time precedes the Start Date of Playback Period, then the process shall be aborted.
- If the current date and time does not precede the Start Date of Playback Period, then the Playback Device sets the Start Date of Playback Period field to the current date and time.

(4.2) Update the End Date of Playback Period.

a) When the Validity of End Date field is equal to '0b,' the Playback Device calculates the end date and time by adding the value specified in the Playback Span field to the current date and time, sets

the End Date of Playback Period field to the calculated end date and time, and sets the Validity of End Date field to '1b.'

b) When the Validity of End Date field is equal to '1b,' the Playback Device compares the current date and time with the date and time of the End Date of Playback Period field.

- If the current date and time does not precede the End Date of Playback Period, then the process shall be aborted.
- If the current date and time precedes the End Date of Playback Period, then the Playback Device calculates the end date and time by adding the value specified in the Playback Span field to the current date and time. If the calculated end date and time precedes the End Date of Playback Period field, the Playback Device sets the End Date of Playback Period field to the calculated end date and time.

(4.3) The Playback Device sets the First Playback Flag field to '1b.' Then go to step (6).

(5) Check the Usage Rules (Phase 2).

(5.1) If the Validity of Start Date field is equal to '1b' and the current date and time precedes the Start Date of Playback Period field, then the process shall be aborted.

(5.2) If the Validity of End Date field is equal to '1b' and the current date and time does not precede the End Date of Playback Period field, then the process shall be aborted.

(6) Calculate a reference timestamp.

The Playback Device shall perform the following steps:

- If there is no SD_AUDIO\SD_ADPRV\TBUR_A.TS file, the process shall be aborted.
- Read the timestamp file in the SD_AUDIO\SD_ADPRV directory. If the verification of the DEADBEEFh hexadecimal value fails, the Playback Device shall abort this process. Otherwise, the Playback Device shall set the reference time to the timestamp in the SD_AUDIO\SD_ADPRV directory.
- If the timestamp file in the Root directory exists, the Playback Device may read the timestamp file in the Root directory. If the verification of the DEADBEEFh hexadecimal value in the timestamp file succeeds, set the reference time to the later of the two timestamp. If there is no timestamp in the Root directory or if the verification of the DEADBEEFh hexadecimal value fails, the Playback Device shall set the reference time to the timestamp in the SD_AUDIO\SD_ADPRV directory.

(7) Update Timestamp.

Playback Device shall update the timestamp in \SD_AUDIO\SD_ADPRV\TBUR_A.TS file and may update the timestamp in \TBUR.TS file as following:

- Read 'In-Use' flag and ETC counter from the \SD_AUDIO\SD_ADPRV\TBUR_A.TS file.
- If 'In-Use' = '0b', ETC = '0h', and the reference time is in the past, Playback Device shall write the current time to \SD_AUDIO\SD_ADPRV\TBUR_A.TS file, with 'In-Use = '1b' and ETC = '0h' and may write the same to \TBUR.TS file. Go to step (8).
- If the reference time is in the future, and any of the following conditions below hold, the Playback device shall refuse to play the content, i.e. this process shall be aborted.
    - In-Use = '0b', and ETC = '0h'
    - In-Use = '0b', and ETC = '5h'
    - In-Use = '1b', and ETC = '5h'
- If In-Use = '0b', '0h' < ETC < '5h', and the reference time is in the past, Playback Device shall write the current time to \SD_AUDIO\SD_ADPRV\TBUR_A.TS file, with In-Use = '1b, and ETC unchanged and may write the same to \TBUR.TS file.

- If In-Use = ‘0b’, ‘0h’ < ETC < ‘5h’, and the reference time is in the future,
  - If the content is active, set In-Use = ‘1b’, Playback Device shall leave ETC unchanged and write the reference time to \SD_AUDIO\SD_ADPRV\TBUR_A.TS file and may write the same to \TBUR.TS file.
  - If the content is non-active, this process shall be aborted. Non-active content cannot be played until the latest timestamp catches up with the current time.
- If In-Use = ‘1b’, ETC = ‘5h’ and the reference time is in the past, Playback Device shall reset ETC = ‘0h’, and write the current time to \SD_AUDIO\SD_ADPRV\TBUR_A.TS file and may write the same to \TBUR.TS file. This is the case where the reference time caught up with the current time.
- If In-Use = ‘1b’, and ETC < ‘5h’, increment ETC by one, Playback Device shall leave In-Use flag unchanged, and write the later of the reference time and the current time plus the duration of the content. It is recommended that the device displays a warning message alerting the user. The message should indicate that pulling of the SD Memory Card has been detected and further occurrences of this event could affect the terms of the rental and/or prevent playback of date and time-based content.

(8) Write the TKE-EXT to the SD Memory Card.

If the TKE-EXT has not been updated either in step (4), then go to step (9).

the Playback Device securely writes the updated TKE-EXT as the new TKE-EXT to the SD Memory Card using the Secure Write Process after the AKE Process using the Media Unique Key associated with MKB-U, securely reads the updated TKE-EXT from the SD Memory Card using the Secure Read Process after the AKE Process using the Media Unique Key associated with MKB-U, and verifies that the update has completed successfully.

If the verification of the TKE-EXT fails, the Playback Device shall abort this process.

(9) Start Playback

The Playback Device starts to playback the SD-Audio content.

If the Preview counter is not equal to zero, then the Playback Device shall execute the following process before elapsed playback time reaches the time specified in the Preview Threshold field.

(10) Update or invalidate TKE-EXT on the SD Memory Card

If the Preview Counter is equal to “11111111b”, skip this step (10).

The Playback Device decrements the Preview Counter and holds the decremented Preview Counter. Then,

a) If the (decremented) Preview Counter is greater than zero, the Playback Device updates the Preview Counter field of the TKE-EXT as follows:

- The Preview Counter field is updated with the decremented Preview Counter.

Then the Playback Device securely writes the updated TKE-EXT as the new TKE-EXT to the SD Memory Card using the Secure Write Process after the AKE Process using the Media Unique Key associated with MKB-U, securely reads the updated TKE-EXT from the SD Memory Card using the Secure Read Process after the AKE Process using the Media Unique Key associated with MKB-U, and verifies that the update has completed successfully.

b) If the (decremented) Preview Counter is equal to zero, the Playback Device securely overwrites “the value for delete (random number)” to the encrypted field (the first 8 bytes (including Title Key) and last 48 bytes (including Usage Rule)) of the TKE-EXT in the TKMG-EXT file on the SD Memory Card using the Secure Title Key and Usage Rule Delete protocol after the AKE Process using the Media Unique Key associated with MKB-U.

In addition, the Availability flag and the Content ID field are set to ‘0’.

(11) Stop Function or End Playback

The Playback Device has stopped playback of content after the stop control function has been used or the Playback Device has reached the end of the content.

- Read the timestamp file in the SD_AUDIO\SD_ADPRV directory. If the verification of the DEADBEEFh hexadecimal value fails, the Playback Device shall abort this process.
- If the timestamp file in the Root directory exists, Playback Device may read the timestamp file in the Root directory, and if the verification of the DEADBEEFh hexadecimal value succeeds, set the reference time to the later of the two timestamp. If there is no timestamp in the Root directory, or If the verification of the DEADBEEFh hexadecimal value fails, set the reference time to the timestamp in the SD_AUDIO\SD_ADPRV directory.
- Read 'In-Use' flag and ETC from the file in the SD_AUDIO\SD_ADPRV directory.
- If the reference time is in the past, Playback Device shall write TBUR_A.TS file with the current time, In-Use = '0b' and ETC ='0h'and may write TBUR.TS file with the same. If the reference time is in the future, Playback Device shall write the reference time to TBUR_A.TS file with In-Use = '0b' and ETC unchanged and may the same to TBUR.TS..

If the above Secure Write Process or the above Secure Title Key and Usage rule Delete protocol does not succeed, the Playback Device shall stop playing the content.

Note: If the Playback Device executes step (10) in advance and playback is stopped before elapsed time reaches the Preview Threshold time, it should restore the TKE-EXT on the SD Memory Card to the state before executing step (10). (E.g. when the Playback Device starts playback, it may save the Preview Counter, decrement it and write the decremented Preview Counter to the SD Memory Card. If the playback is stopped before the elapsed time reaches the Preview Threshold time, the Playback Device should restore the Preview Counter field to the saved Preview Counter.)

C.8.4 Preview Process in Mode B

This section describes the Preview Process of Mode B devices. In the case of playback the content without time-based Usage Rule, step (6), (7) and (11) are skipped.

(1) Read the Extended Title Key Entry (TKE-EXT) from the SD Memory Card

The Playback Device securely reads the Extended Title Key Entry (TKE-EXT) associated with the SD-Audio content for Preview in the Extended Title Key Manager (TKMG-EXT) file, P_AOBSA1.KEY, from the SD Memory Card using Secure Read Process after the AKE Process using the Media Unique Key associated with MKB-U.

(2) Check the Usage Rules (Phase1)

The Playback Device checks the Extended Title Key Entry (TKE-EXT)

- If the Check Value is not '0123456789ABCDEFh,' then the process shall be aborted.
- If Trigger bit fields are "11b", playback is not allowed, hence the process shall be aborted.
- If Clock Usage Flag is equal to '01b', then the process shall be aborted.
- The Playback Device checks the Preview Counter field and judges whether the content is allowed to be previewed or not. If the Preview Counter is equal to zero, the process is aborted.
- If the Playback Device does not support clock function described in section C.2 the process shall be aborted.
- If the Trigger bit fields are '00b,' or '01b', content does not have date and time-based usage rules, go to step (9) .That is, any Playback Device shall ignore date and time-based rules and proceed to playback content

The Playback Device checks the Validity of Start Date field, the Validity of End Date field and the Validity of Span field. When all the above fields are equal to ‘0b,’ that is, all fields have not been set, go to step (6).

(3) Obtain current date and time.

The Playback Device that works in Mode B obtains the current date and time by referring to its internal tamper resistant clock (Clock B).

If the Playback Device that works in Mode B2 cannot obtain the current date and time, and if Clock Usage Flag is equal to ‘11b’, then the process shall be aborted.

If the Playback Device that works in Mode B2 cannot obtain the current date and time, and if Clock Usage Flag is equal to ‘10b’, then the Playback Device can switch to Mode B1.

(4) Update the TKE-EXT

The Playback Device checks the First Playback Flag field and the Validity of Span field. When the First Playback Flag field is equal to ‘1b’ or the Validity of Span field is equal to ‘0b,’ go to step (5).

(4.1) Update the Start Date of Playback Period.

a) When the Validity of Start Date field is equal to ‘0b,’ the Playback Device sets the Start Date of Playback Period field to the current date and time and sets the Validity of Start Date field to ‘1b.’

b) When the Validity of Start Date field is equal to ‘1b,’ the Playback Device compares the current date and time with the date and time of the Start Date of Playback Period field.

- If the current date and time precedes the Start Date of Playback Period, then the process shall be aborted.
- If the current date and time does not precede the Start Date of Playback Period, then the Playback Device sets the Start Date of Playback Period field to the current date and time.

(4.2) Update the End Date of Playback Period.

a) When the Validity of End Date field is equal to ‘0b,’ the Playback Device calculates the end date and time by adding the value specified in the Playback Span field to the current date and time, sets the End Date of Playback Period field to the calculated end date and time, and sets the Validity of End Date field to ‘1b.’

b) When the Validity of End Date field is equal to ‘1b,’ the Playback Device compares the current date and time with the date and time of the End Date of Playback Period field.

- If the current date and time does not precede the End Date of Playback Period, then the process shall be aborted.
- If the current date and time precedes the End Date of Playback Period, then the Playback Device calculates the end date and time by adding the value specified in the Playback Span field to the current date and time. If the calculated end date and time precedes the End Date of Playback Period field, the Playback Device sets the End Date of Playback Period field to the calculated end date and time.

(4.3) The Playback Device sets the First Playback Flag field to ‘1b.’ Then go to step (6).

(5) Check the Usage Rules (Phase 2).

(5.1) If the Validity of Start Date field is equal to ‘1b’ and the current date and time precedes the Start Date of Playback Period field, then the process shall be aborted.

(5.2) If the Validity of End Date field is equal to ‘1b’ and the current date and time does not precede the End Date of Playback Period field, then the process shall be aborted.

(6) Write the TKE-EXT to the SD Memory Card.

If the TKE-EXT has not been updated either in step (4), then go to step (7).

The Playback Device securely writes the updated TKE-EXT as the new TKE-EXT to the SD Memory Card using the Secure Write Process after the AKE Process using the Media Unique Key associated with MKB-U, securely reads the updated TKE-EXT from the SD Memory Card using the Secure Read Process after the AKE Process using the Media Unique Key associated with MKB-U, and verifies that the update has completed successfully.

If the verification of the TKE-EXT fails, the Playback Device shall abort this process.

(7) Start Playback

The Playback Device starts to playback the SD-Audio content.

If Preview counter not equal to zero, then, the Playback Device shall execute the following process before elapsed playback time reaches the time specified in the Preview Threshold field.

(8) Update or invalidate TKE-EXT on the SD Memory Card

If the Preview Counter is equal to “11111111b”, skip this step (8).

The Playback Device decrements the Preview Counter and holds the decremented Preview Counter. Then,

a) If the (decremented) Preview Counter is greater than zero, the Playback Device updates the Preview Counter field of the TKE-EXT as follows:

- The Preview Counter field is updated with the decremented Preview Counter.

Then the Playback Device securely writes the updated TKE-EXT as the new TKE-EXT to the SD Memory Card using the Secure Write Process after the AKE Process using the Media Unique Key associated with MKB-U, securely reads the updated TKE-EXT from the SD Memory Card using the Secure Read Process after the AKE Process using the Media Unique Key associated with MKB-U, and verifies that the update has completed successfully.

b) If the (decremented) Preview Counter is equal to zero, the Playback Device securely overwrites “the value for delete (random number)” to the encrypted field (the first 8 bytes (including Title Key) and last 48 bytes (including Usage Rule)) of the TKE-EXT in the TKMG-EXT file on the SD Memory Card using the Secure Title Key and Usage Rule Delete protocol after the AKE Process using the Media Unique Key associated with MKB-U.

In addition, the Availability flag and the Content ID field are set to ‘0’.

If the above Secure Write Process or the above Secure Title Key and Usage rule Delete protocol does not succeed, the Playback Device shall stop playing the content.

Note: If the Playback Device executes step (8) in advance and playback is stopped before elapsed time reaches the Preview Threshold time, it should restore the TKE-EXT on the SD Memory Card to the state before executing step (8). (E.g. when the Playback Device starts playback, it may save the Preview Counter, decrement it and write the decremented Preview Counter to the SD Memory Card. If the playback is stopped before the elapsed time reaches the Preview Threshold time, the Playback Device should restore the Preview Counter field to the saved Preview Counter.)

C.9 MKB Extension

This section describes the MKB Extension file configuration for MKB-U (“MKB for Usage Rules”) on the SD Memory Card. MKB Extensions are described in the *Introduction and Common Cryptographic Elements* book of this specification.

In the case of SD-Audio extension for Preview, the directory name is SD_AUDIO and the file name of the MKB Extension file for MKB-U is SD_ADEX8.MKB.

Recording and Playback devices must recognize SD_ADEX8.MKB file and process it if it is present on the SD Memory Card.

This MKB Extension file is shared by Move Extension described in Appendix A.