Content Protection for Recordable Media Specification

SD Memory Card Book
SD-Video Part

Intel Corporation
International Business Machines Corporation
Panasonic Corporation
Toshiba Corporation

Revision 0.97
December 15, 2011

This page is intentionally left blank.

Preface

Notice

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

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

Intellectual Property

Implementation of this specification requires a license from the 4C Entity, LLC.

Contact Information

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

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

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

This page is intentionally left blank.

Table of Contents

List of Figures

This page is intentionally left blank.

List of Tables

This page is intentionally left blank.

Chapter 1
Introduction

1. Introduction

1.1 Purpose and Scope

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

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

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

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

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

SD-Video has six profiles currently, which are Mobile Video Profile, Personal Video Profile, ISDB-T Mobile Video Profile, H.264 Mobile Video Profile, Entertainment Video Profile and Entertainment Video Recorder Profile. Mobile Video Profile and Personal Video Profile support MPEG-4 contents. ISDB-T Mobile Video Profile and H.264 Mobile Video Profile support H.264 contents. Entertainment Video Profile and Entertainment Video Recorder Profile support MPEG-2 contents. Personal Video Profile is for camera product and they need not to support content protection, then this profile is out of scope of 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-Video content stored on SD Memory Card media.

1.3 References

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

4C Entity, LLC, *CPRM/CPPM License Agreement*

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

4C Entity, LLC, *CPRM Specification: SD Memory Card Book Common Part, Revision 0.97*

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

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

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

SD Association, *SD Memory Card Specifications, Part 8: VIDEO Specifications, Common Book Version 1.30*

SD Association, *SD Memory Card Specifications, Part 8: Mobile Video Profile, Entertainment Video Profile, Entertainment Video Recorder Profile, Personal Video Profile Specification, Addendum to VIDEO Specification, Version 1.10*

SD Association, *SD Memory Card Specifications, Part 8: ISDB-T Mobile Video Profile, Addendum to VIDEO Specification, Version 1.20*

SD Association, *SD Memory Card Specifications, Part 8: H.264 Mobile Video Profile, Addendum to VIDEO Specification, Version 1.0*

1.4 Future Directions

This document currently provides details to using CPRM for the MPEG4 (including H.264) content which is specified by Mobile Video Profile in *SD-Video Part of SD Memory Card Book*. It is anticipated that CPRM technology will also be applied to other formats under future extensions to this specification, e.g. MPEG2 content specified by Entertainment Video Profile, 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. Abbreviations and Acronyms

The following abbreviations and acronyms are used in this document:

AKE	Authentication and Key Exchange
APSTB	Analog Protection System Trigger Bits
AST	Analog Sunset Token
C-CBC	Converted Cipher Block Chaining
C2	Cryptomeria Cipher
CCI	Copy Control Information
CGMS	Copy Generation Management System
CPF	Copy Permission Flag
CPRM	Content Protection for Recordable Media
ID	Identifier
EPN	Encryption Plus Non-assertion
ETS Header	Extended Transport Stream Header
ETS Packet	Extended Transport Stream Packet
LLC	Limited Liability Company
MKB	Media Key Block
MO	Media Object
MOI	Media Object Information
RDI	Real-time Data Information
TBUR	Time-Based Usage Rules
TK	Title Key
TKA	Title Key Area
TKURE	Title Key & Usage Rule Entry
TKURE_SRN	TKURE Search Number
TKURMG	Title Key & Usage Rule Manager
TKURMGI	Title Key & Usage Rule Manager Information
TKURMMG	Title Key & Usage Rule Master Manager
TOD	Transport Stream Object Data
TS	Time Stamp
UR	Usage Rules

Chapter 3
CPRM for SD-Video

3. CPRM for SD-Video

3.1 Introduction

This chapter specifies details for using CPRM to protect SD-Video content stored on SD Memory Card media. This chapter describes details on using CPRM to realize "Move," "Copy," and "Playback" operations for SD-Video content.

The SD-Video and SD Memory Card formats can be licensed from the SD Association, which also publishes specifications describing them in detail (see the corresponding references in Section 1.1). This chapter assumes that readers are familiar with these formats, as defined in their corresponding specifications.

3.2 Device Requirements

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

3.3 CPRM Components

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

3.3.1 System Area

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

3.3.1.1 Media Key Block (MKB)

In order to protect the Title Key and Usage Rules of SD-Video content, the "MKB for SD-Video" is used. The MKB number for SD-Video is described in the Supplementary Note of *SD Memory Card Specifications Part 3: Security Specification*.

3.3.2 Hidden Area

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

3.3.3 Protected Area

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

In the case of SD-Video specifications, the Protected Area contains Encrypted Title Keys and Encrypted Usage Rules. The Title Key and Usage Rules of the content are concatenated and encrypted together by a Media Unique Key, which is unique for each SD Memory Card. The Encrypted Title Key and Usage Rules are stored as a file in the Protected Area. The file system of the Protected Area and the detail format of the Encrypted Title Key and Usage Rules are described in Section 3.7. In addition, the Protected Area may also contain timestamp files. The detail format of timestamp file is described in Section 3.7.1.5.

3.3.3.1 Encrypted Title Key

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

3.3.3.2 Encrypted Usage Rules

Usage Rules (UR) consist of the following information:

- "Move Control Information": Usage Rule for controlling the Move operation.
- "Copy Count Control Information": Usage Rule for controlling the Copy operation.
- "CCIFlags": Usage Rule for controlling Analog Protection System and the status of CCI in the stream.
- "Period Control Information": Usage Rule for controlling the Playback 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 Playback operation. The span information indicates the number of days and hours of permitted playback for content with date and time-based usage rules.
- "Playback Count Control Information": Usage Rule for controlling the Playback operation. It contains information indicating how many times a particular content can be played back. This playback counter constitutes a simple preview counter.
- "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 detailed format of Usage Rules is described in Section 3.7.5.2.

3.3.4 User Data Area

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

3.4 Content Encryption and Decryption Protocol

The SD-Video content, Title Keys and Usage Rules are encrypted/decrypted using almost the same encryption and decryption protocol as defined in Section 3.4 of *SD Memory Card Book Common Part.*

Figure 3-1 illustrates the process for SD-Video content encryption and decryption on "SD Memory Card."

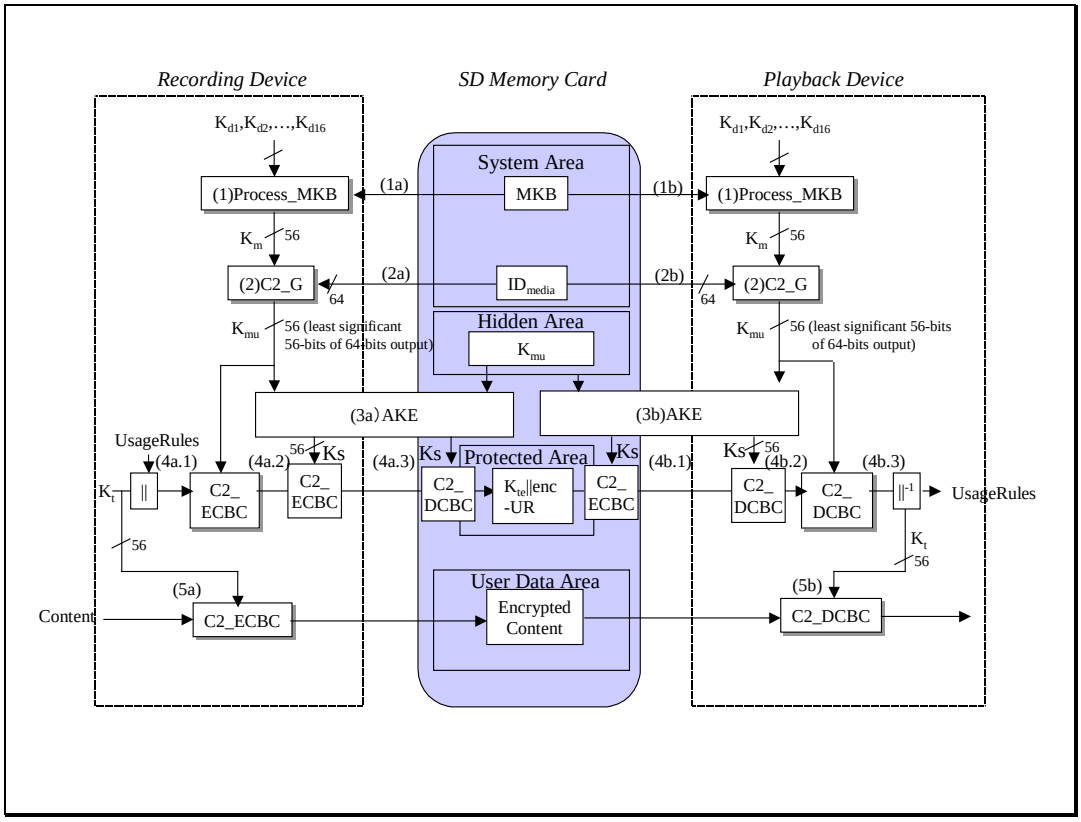


Figure 3-1 Content Encryption and Decryption on SD Memory Card

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 using Device Key for MKB (see the *Introduction and Common Cryptographic Elements* book).

- (2) The accessing device executes the C2_G process

  (2a, 2b) The same procedures defined in Section 3.4 (2) of *SD Memory Card Book Common Part* are used.

- (3) AKE process

  (3a, 3b) The same procedures defined in Section 3.4.1of *SD Memory Card Book Common Part* are used.

-(4a) Title Key and Usage Rule Encryption process.

The following steps (4a.1) through (4a.3) describe the Title Key and Usage Rule Encryption Process.

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

(4a.1) Encrypt the Title Key and Usage Rule Entry by the Media Unique Key associated with MKB.

The Recording Device encrypts the Title Key and Usage Rule Entry (see Table 3-10), as a single 64-byte encryption frame using the Media Unique Key associated with MKB. The encryption algorithm is C2_ECBC (the C2 cipher algorithm in C-CBC mode) which is described in the *Introduction and Common Cryptographic Elements* book.

(4a.2) Encrypt the Title Key and Usage Rule Entry by the Session Key.

The Recording Device further encrypts the entire 64-byte Title Key and Usage Rule Entry using the Session Key K_s, which is shared at step (3a), using C2_ECBC.

The results (the doubly-encrypted Title Key and Usage Rules) are sent to the SD Memory Card.

(4a.3) Decrypt the Title Key and Usage Rule Entry by the Session Key.

In the SD Memory Card, the doubly-encrypted 64-byte Title Key and Usage Rule Entry is decrypted using the Session Key K_s, which is shared at step (3a). The decryption algorithm is C2_DCBC (the C2 cipher algorithm in C-CBC mode) which is described in the *Introduction and Common Cryptographic Elements* book. The result (the encrypted Title Key and Usage Rule Entry) is stored in the Protected Area.

-(4b) Title Key and Usage Rule Decryption process.

The following steps (4b.1) through (4b.3) describe the Title Key and Usage Rule Decryption Process.

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

In the SD Memory Card, the 64-byte Title Key and Usage Rule Entry stored in the Protected Area is encrypted using the Session Key K_s, which is shared at step (3b), using C2_ECBC, and the result (the doubly-encrypted Title Key and Usage Rule Entry) is sent to the Playback Device.

(4b.2) Decrypt the Title Key and Usage Rule Entry by the Session Key.

The Playback Device decrypts the doubly-encrypted 64-byte Title Key and Usage Rule Entry using the Session Key K_s, which is shared at step (3b), using C2_DCBC.

(4b.3) Decrypt the Title Key and Usage Rule Entry by the Media Unique Key associated with MKB.

The Playback Device decrypts the 64-byte Title Key and Usage Rule Entry using the Media Unique Key associated with MKB, using C2_DCBC. Then the Playback Device gets the decrypted Title Key and Usage Rules.

-(5a) Content Encryption process

As for the content encryption process, the same procedures defined in Section 3.4 (5a) of *SD Memory Card Book Common Part* are used.

-(5b) Content Decryption process

As for the content decryption process, the same procedures defined in Section 3.4 (5b) of *SD Memory Card Book Common Part* are used.

3.5 Accessing the Protected Area

Regarding Accessing the Protected Area, refer to Section 3.5 of *SD Memory Card Book Common Part*.

3.6 Content Encryption and Decryption Format

Regarding the General Principle for Content Encryption and Decryption Format, refer to Section 3.6 of *SD Memory Card Book Common Part*.

3.6.1 SD-Video Object Encryption

3.6.1.1 ASF File Encryption

SD-Video application treats the Microsoft's Advanced Systems Format (ASF) file as one of the file format that contains video stream. The ASF file is encrypted by the Title Key as follows:

- The ASF file consists of an ASF Header Section, ASF Data Section Object (fixed to 50 bytes) and multiple ASF Data Packets.

- The ASF Header Section and the ASF Data Section Object are not encrypted.
- Each ASF Data Packet consists of a header part (variable size M: less than or equal to 40 bytes) and a data part (variable size N). Size of Data Packet is less than 2^32 bytes.
- Each ASF Data Packet is encrypted by the corresponding Title Key using C2_ECBC (the C2 cipher algorithm in 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 3-1 and Table 3-2 show the encrypted ASF file Packet format.

Table 3-1 Encrypted ASF Data Packet format without residual block (M+N=8*n)

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 (Encrypted)							
41								
M+N-1								

Table 3-2 Encrypted ASF Data Packet format with residual block (M+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)							
M+N-1								

3.6.1.2 MP4 File Encryption

SD-Video application treats MP4 file which is designed to contain the media information of an ISO/IEC 14496 presentation as one of the file format that contains video content stream. The MP4 file is encrypted by the Title Key as follows:

- The MP4 file consists of Movie Box (moov), Movie Fragment Box (moof), Media Data Box (mdat), and other miscellaneous boxes. Movie Box (moov) contains Sample To Chunk Box (stsc) and Movie Fragment Box (moof) contains Track Fragment Run Box (trun).
- Each Media Data Box (mdat) consists of a header part (8 or 16 bytes) and data part (variable size), and data part of Media Data Box (mdat) consists of some Chunks (variable size). Chunk is continuous set of samples for one track indicated by Sample To Chunk Box (stsc) in Movie Box (moov) or Track Fragment Run Box (trun) in Movie Fragment Box (moof).
- Encryption of an MP4 file is done using C2_ECBC (the C2 cipher algorithm in C-CBC mode) with the corresponding Title Key as the encryption key.
- Movie Box (moov), Movie Fragment Box (moof) and other miscellaneous boxes are not encrypted.
- Each Chunk is encrypted and starts a new C-CBC mode cipher chain. But if Chunk size is larger than 2048 bytes, the cipher chain is reset every 2048 bytes offset.
- The last residual blocks of encryption parts, if they are less than 8 bytes, are not encrypted.

Table 3-3 and Table 3-4 show the encrypted Chunk.

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

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

Table 3-4 Encrypted Chunk with residual block (N=8*n+m, m<8)

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

If Chunk size is larger than 2048 bytes, cipher chain in Chunk is reset every 2048 bytes as shown in Table 3-5. Each Encryption Block starts a new C-CBC mode cipher chain.

Table 3-5 Encrypted Chunk (N > 2048, N=8*n+m, m<8, N=2048*p+q, q<2048)

Bit / Byte	7	6	5	4	3	2	1	0
0	Encryption block (Encrypted)							
1								
2047								
2048	Encryption block (Encrypted)							
4095								
:								
2048p	Encryption block (Encrypted)							
8n-1								
8n	Residual block (Non-Encrypted)							
N-1								

3.6.1.3 TOD File Encryption

SD-Video application treats TOD file as one of the file format that contains video content stream. TOD file is constructed from an integer number of Packet Sequences. One Packet Sequence consists of plural ETS Packets. The number of ETS Packets that compose one Packet Sequence is stored in PacketSeqPacketNum field of MOI in User Data Area. In the case of last Packet Sequence the number of ETS Packets may be less than or equal to PacketSeqPacketNum. Figure 3-2 shows the relationship between Packet Sequence and ETS Packet.

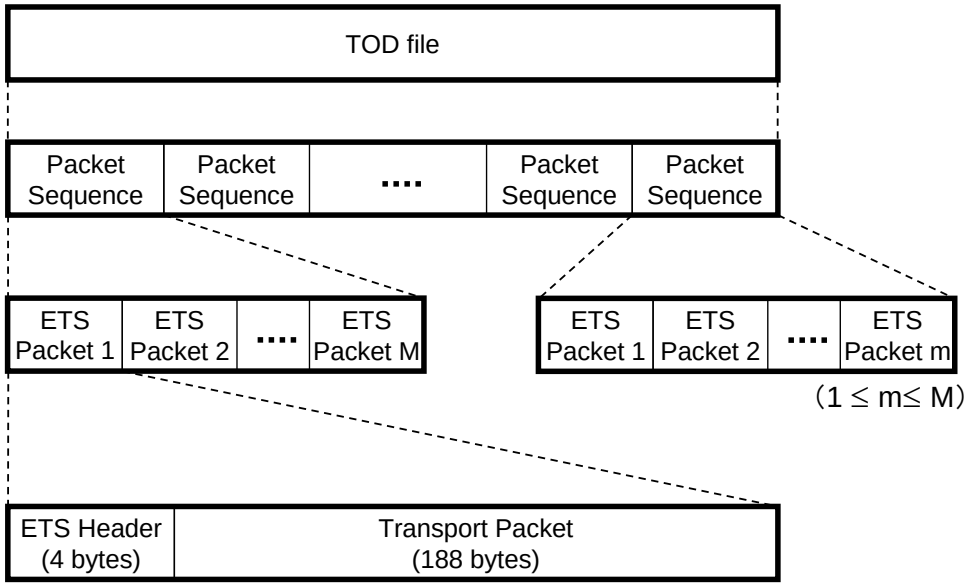


Figure 3-2 Encrypted Packet Sequence

The first ETS Packet in the Packet Sequence shall be Real-time Data Information (RDI) Packet if the Packet Sequence is encrypted. RDI Packet is used to carry various types of information including copyright information about the stream.

An ETS Packet is composed of a 4-byte ETS Header and a 188-byte MPEG-2 Transport Packet. An ETS header contains 32-bit reserved field. Transport packets shall comply with ISO/IEC 13818-1.

TOD file is encrypted by Title Key as follows.

- Encryption of TOD file is done using C2-ECBC (the C2 cipher algorithm in C-CBC mode) with the corresponding Title Key as the encryption key.
- Each Packet Sequence starts a new C-CBC cipher chain.
- 160 bytes from the top of each Packet Sequence is not encrypted and the residual part is encrypted.
- Encrypted Packet Sequences and un-encrypted Packet Sequences may coexist in one TOD file.

3.6.1.3.1 Encryption of Packet Sequence

Table 3-6 shows the encrypted Packet Sequence.

Table 3-6 Encrypted Packet Sequence (N=192*M)

	Bit / Byte	7	6	5	4	3	2	1	0	
RDI Packet	0	(Data defined in SD Memory Card Specification, Part 8)								
	1									
	:									
	11									
	12	CPF		APSTB						CCI_byte
	13	(Data defined in SD Memory Card Specification, Part 8)								
	:									
	159									
	160	E_CPF		E_APSTB						E_CCI_byte
	161	(Data defined in SD Memory Card Specification, Part 8)								
	:									
	183									
	184	RDI_CHECK								
	:									
	191									
	192	Second ETS Packet								
	193									
	:									
	383									
	:									
	(M-1)*192	M'th ETS Packet (if present)								
	:									
	M*192-1									

The data field values in a given RDI Packet apply to subsequent ETS Packet in the Packet Sequence. The data field of each Packet Sequence may distinct from each other. In RDI Packet, there are CCI_byte field and E_CCI_byte field including the Copy Permission Field (CPF) field and the APSTB field. CCI_byte field and E_CCI_byte field shall have the same value, but CCI_byte field is not encrypted and E_CCI_byte field is encrypted. Encrypted CPF and APSTB are named as E_CPF and E_APSTB, respectively.

The APSTB field indicates the analog protection status of corresponding ETS Packet, with encodings defined in the SD Memory Card Specification, Part 8. The CPF field indicates the copy control status of corresponding ETS Packet as shown in Table 3-7.

Table 3-7 Indication of copy control status

CPF/E_CPF	Encryption of Packet Sequence	CGMS	EPN
00b	Off	Copy freely	Unasserted
01b	Reserved		
10b	On	Copy freely	Asserted
11b	On	No more copies	Don't care

The RDI_CHECK field stores 64-bit check value, it shall be equal to '0123456789ABCDEFh' if CPF field and E_CPF field are equal to '10b' or '11b.'

3.7 File System of the Protected Area

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

3.7.1 File System of the Protected Area for SD-Video

This section describes the file system of the Protected Area in which the encrypted Title Key (TK) and encrypted Usage Rules (UR) for SD-Video content are stored.

In SD-Video Specification, there are two ways of encryption for the contents. One is Program Encryption and another is MO (Media Object) Encryption. If all MOs in a Program can be managed by a single Title Key & Usage Rule, Program Encryption is used. In this case all MOs in a Program are encrypted with the same Title Key and have the same Usage Rule. If each MO in Program should be managed by its own Title Key & Usage Rule, then MO Encryption is used. In this case each MO in a Program is encrypted with the Title Key assigned individually to such MO and has its own Usage Rule.

3.7.1.1 Title Key & Usage Rule Master Manager (TKURMMG) for Programs

A single master manager file for Programs manages all the Title Key & Usage Rule Manager (TKURMG) files for Programs for SD-Video content in the Protected Area. The file is called Title Key & Usage Rule Master Manager (TKURMMG) file for Programs.

3.7.1.2 Title Key & Usage Rule Manager (TKURMG) for Programs

In the case of Program Encryption, the Title Key and the Usage Rules for Programs for SD-Video content are encrypted by the Media Unique Key and stored in one file of the Protected Area. This file is called Title Key & Usage Rule Manager (TKURMG) file for Programs. In the Protected Area, there can be only one TKURMG files for Programs.

3.7.1.3 Title Key & Usage Rule Master Manager (TKURMMG) for MOs

A single master manager file for MOs manages all the Title Key & Usage Rule Manager files for MOs for SD-Video content in the Protected Area. The file is called Title Key & Usage Rule Master Manager (TKURMMG) file for MOs.

3.7.1.4 Title Key & Usage Rule Manager (TKURMG) for MOs

Similar to Program Encryption, the Title Key and the Usage Rules for SD-Video content are encrypted by the Media Unique Key and stored in a file of the Protected Area in case of MO Encryption. The file is called Title Key & Usage Rule Manager (TKURMG) file for MOs. In the Protected Area, there can be plurality of TKURMG files for MOs.

3.7.1.5 SD Applications and Timestamp Files (TBUR.TS)

We denote 'date and time-based usage rules' to comprise usage rules that are based on date, time and playback counter. In order to assist devices to enforce date and time-based usage rules, SD-Video applications may store a timestamp in the Protected Area of the SD Memory Card. In the case where the video content in the SD Memory Card includes date and time-based usage conditions, at most two timestamp files, denoted TBUR.TS, will appear in the Protected Area. A TBUR.TS file contains a timestamp, an in-use flag and a counter necessary to enforce time-based usage rules. The first TBUR.TS file has the following properties

- plain text.

- written with mode bit = 0, that is, accessible to all SD applications.
- shall appear in the Root directory (\TBUR.TS).

The second TBUR.TS file has the following characteristics

- encrypted,
- written with mode bit = 1, that is, accessible only to SD-Video application.
- shall appear in the SD_VIDEO directory (\SD_VIDEO\TBUR.TS).

Both timestamp files have the same format (See Section 3.7.6 in this specification). These files are used by any SD-Video content with date and time-based usage conditions. That is, it can be used by Program Encrypted content as well as Media Object Encrypted content. The TBUR.TS file in the SD_VIDEO directory is encrypted according to the process similar to the "Encrypt Title Key and CCI process" described in Section 3.4 (4a) of SD Memory Card Book Common Part, i.e., using the Kmu for SD-Video.

3.7.1.6 Directory and File Configuration in Protected Area

Figure 3-3 shows two sample directories and file configurations of the Protected Area for the SD-Video specifications. Figure 3-3 (a) shows a Program Encryption example (with files SD_VIDEO.MMG and VIDEO001.KEY) and a Media Object Encryption example (with single master manager file MO.MMG and at least two Media Object files: MO0001.KEY and MO002.KEY). The Program Encryption and Media Objects in this example do not have time and based usage conditions.

Figure 3-3 (b) shows an example where the video content has calendar usage conditions. In this case, a timestamp is required to enforce date and time usage conditions. File TBUR.TS contains a timestamp. This example shows the two instances of file TBUR.TS, one in the Root directory, and another in the SD_VIDEO directory. Details on how to update this file are described in Section 3.7.6.

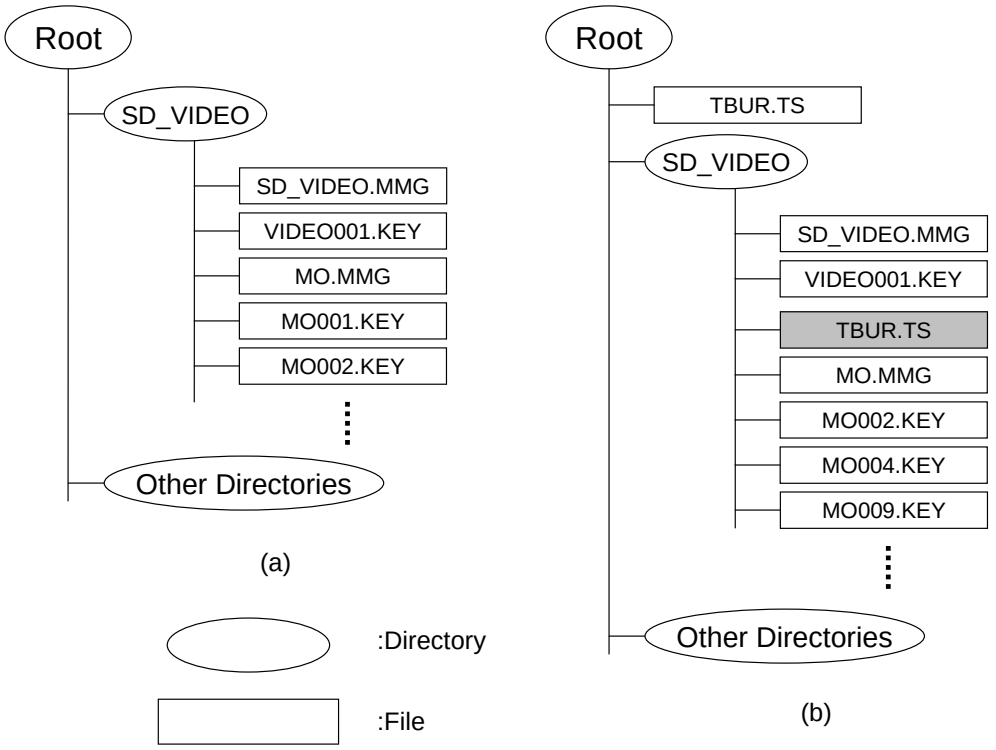


Figure 3-3 Directory and File Configuration of the Protected Area

The name of the TKURMMG file for Programs shall be “SD_VIDEO.MMG.”

The size of a TKURMG file for Programs is fixed. It contains 250 Title Key & Usage Rule Entries (TKUREs) for Programs. In the TKURMG file for Programs, only up to 99 entries are used, because the maximum number of Program that should be protected is 99. In this case, TKURE numbers from 100 to 250 are not used.

The name of the TKURMG files for Programs shall be VIDEO001.KEY.

The name of TKURMMG file for MOs shall be “MO.MMG.”

The size of a TKURMG file for MOs is fixed. It contains 250 Title Key & Usage Rule Entries (TKUREs) for MOs. In this case any of the 250 TKUREs can be use.

There can be at most 9 TKURMG files for MOs in the SD_VIDEO directory of Protected Area, because the maximum number of MOs that can be protected is 2047, 2047 entries can be stored into 9 TKURMG files which have 250 entries.

The name of TKURMG file for MOs shall be:

MOxxx.KEY

where xxx is a serial number (001~009) assigned to each of the TKURMG files for MOs in the SD_VIDEO directory.

The TKURE Search Number (TKURE_SRN) for Programs is a serial number uniquely associated with each TKURE of all the TKURMG files for Programs in SD_VIDEO directory. In other words, TKURE #1 to TKURE #99 in the VIDEO001.KEY file are associated with TKURE_SRN 1 to 99.

Each encrypted content file in the User Data Area is associated with the corresponding TKURE for Programs in the Protected Area through its TKURE_SRN for Programs in case of Program Encryption.

The TKURE Search Number (TKURE_SRN) for MOs is a serial number uniquely associated with each TKURE of all the TKURMG files for MOs in SD_VIDEO directory. The directory contains at most 9 TKURMG files for MOs, each of which has 250 TKUREs, and the maximum number of TKURE_SRN for MOs is 2047. For example, TKURE #1 through TKURE #250 in the MO001.KEY file are associated with TKURE_SRN 1 through 250, TKURE #1 through TKURE #250 in the MO002.KEY file are associated with TKURE_SRN 251 through 500, and so forth.

Each encrypted file in the User Data Area is associated with the corresponding TKURE for MOs in the Protected Area through its TKURE_SRN for MOs in case of MO Encryption.

Actually, the TKURE_SRN for Programs of the corresponding TKURE for Programs is stored in TkureIndex fields of the PRG_ATTR (Program Attribute) and PRG_INFO (Program Information) in the User Data Area., and TKURE_SRN for MOs of the corresponding TKURE for MOs is stored in MOTkureIndex field of MoInfoTbl of PRG_INFO in the User Data Area. The two TkureIndex fields of PRG_ATTR and PRG_INFO shall have same value. Regarding the structure and the file names in the User Data Area, refer to *SD Memory Card Specifications, Part 8: Video Specifications*.

If a content file in the User Data Area is not encrypted, the TkureIndex field and MOTkureIndex field in the corresponding PRG_INFO and PRG_INFO shall be set to 0. If a content file is encrypted with Program Encryption, TkureIndex field shall be TKURE_SRN for Programs and MOTkureIndex field shall be set to 0. If a content file is encrypted with MO Encryption, TkureIndex field shall be set to 0 and MOTkureIndex shall be TKURE_SRN for MOs. Both of TkureIndex field and MOTkureIndex field shall not be nonzero. When TkureIndex field or MOTkureIndex field are set to nonzero, they shall be unique in the SD_VIDEO directory in each number space.

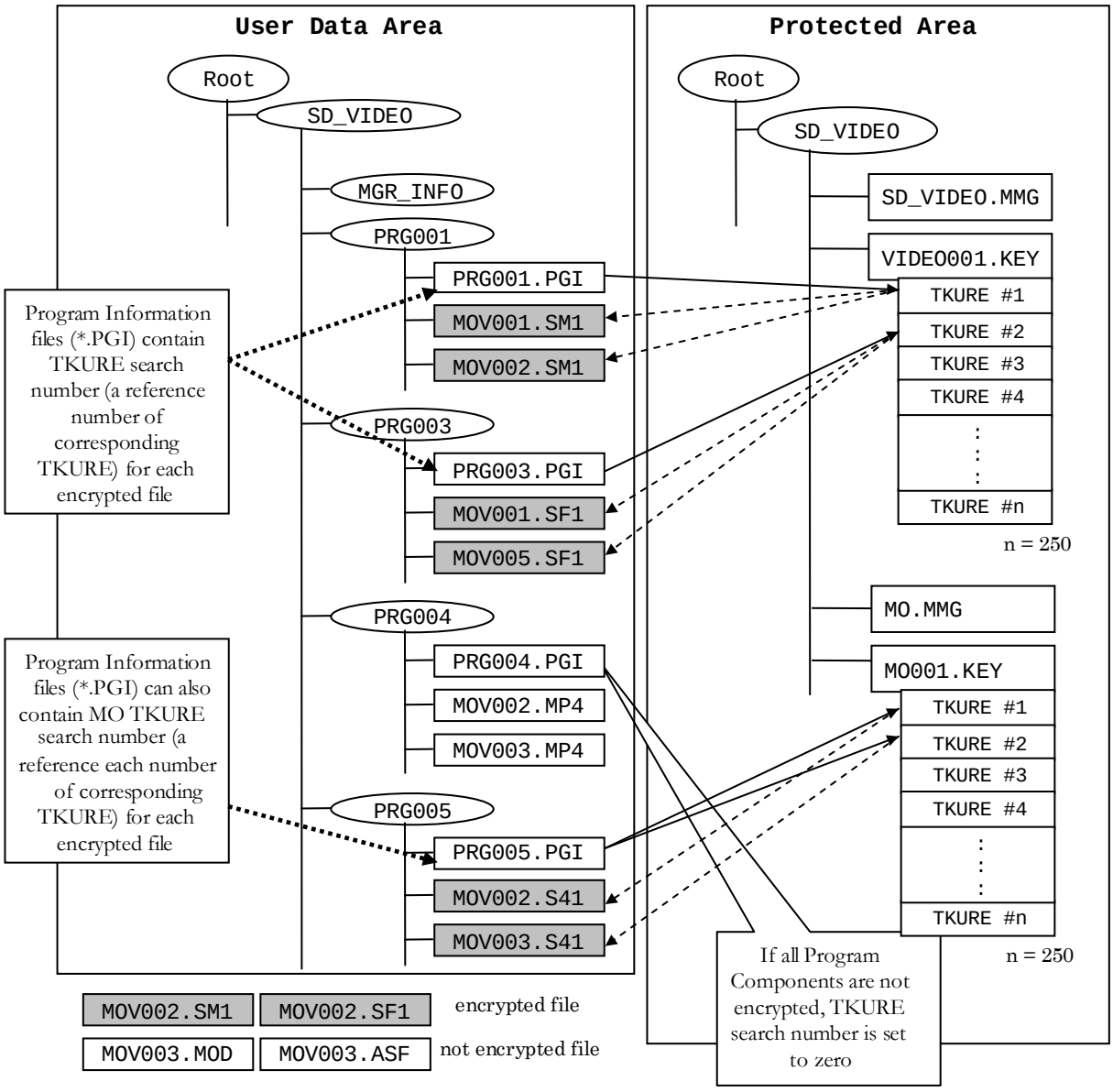


Figure 3-4 Relationship between Directory and Filename

3.7.2 Structure of Title Key & Usage Rule Master Manager

As shown in Table 3-8, the TKURMMG consists of Version number, Application ID of TKURMG, and Used flag of each TKURMG. The same structure of TKURMMG is used between TKURMMG for Programs and MOs.

Table 3-8 TKURMMG

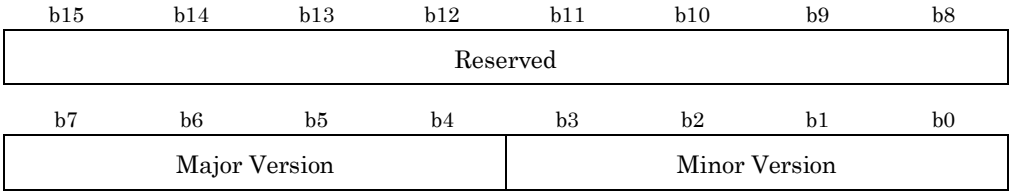
(Description order)

RBP	Field Name	Contents	Number of bytes
0 to 1	VERN	Version number	2 bytes
2 to 3	TKURMG_AP_ID	Application ID of TKURMG	2 bytes
4 to 31	Reserved	Reserved	28 bytes
32 to 33	TKURMG_USED	TKURMG Used flag	2 bytes
34 to 63	Reserved	Reserved	30 bytes
Total			64 bytes

All reserved bits shall be set to '0.'

(RBP 0 to 1) VERN

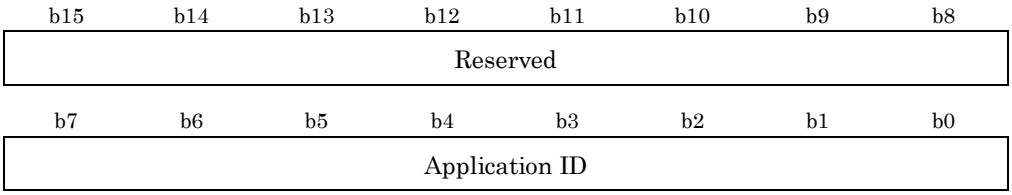
This field describes the version of SD-Video data structure. Regarding the version of SD-Video data structure, refer to Section 4.2.2 of *SD Specifications, Part 8: VIDEO Specifications, Common Book Version 1.30.* The version number in this field is as same as the version of MGR_DATA in the User Data Area. Regarding MGR_DATA, refer to Section 4.3 of *SD Specifications, Part 8: VIDEO Specifications, Common Book Version 1.30.*



Major Version	Minor Version	
0001b	0100b	Version 1.4 (in the case of Mobile Video Profile version 1.1 and H.264 Mobile Video Profile version 1.0)
0001b	0011b	Version 1.3 (in the case of ISDB-T Mobile Video Profile version 1.0)
0001b	0010b	Version 1.2
0001b	0001b	Version 1.1
Others		Reserved.

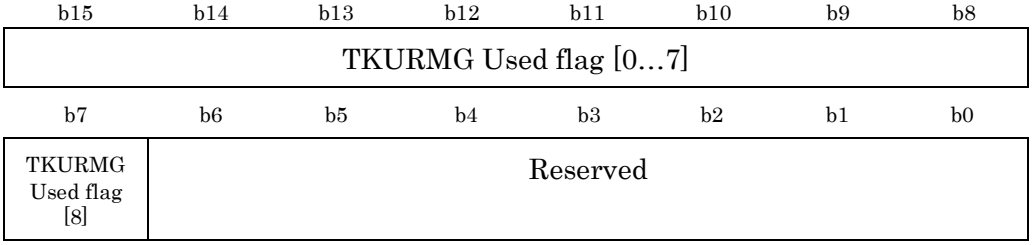
(RBP 2 to 3) TKURMG_AP_ID

This field describes the Application ID of TKURMG. This value must be 4.



(RBP 32) TKURMG_USED

This field describes whether each TKURMG has unused TKUREs or not.



In case of TKURMMG for Programs,

TKURMG Used flag[0] ... 1b: "VIDEO001 .KEY" exists and all the TKUREs of "VIDEO001 .KEY" are used.

0b: Either "VIDEO001 .KEY" does not exist, or

"VIDEO001 .KEY" exists and has some unused TKUREs.

This flag shall be always 0.

TKURMG Used flag[1] .. [8] … Reserved

In case of TKURMMG for MOs,

TKURMG Used flag [*j*-1] ... 1b: "MO*j* .KEY" exists and all the TKUREs of "MO*j* .KEY" are used.

0b: Either "MO*j* .KEY" does not exist, or

"MO*j* .KEY" exists and has some unused TKUREs.

3.7.3 Structure of Title Key & Usage Rule Manager

Figure 3-5 shows the structure of a Title Key & Usage Rule Manager (TKURMG). The same structure of TKURMG is used between TKURMG for Programs and MOs.

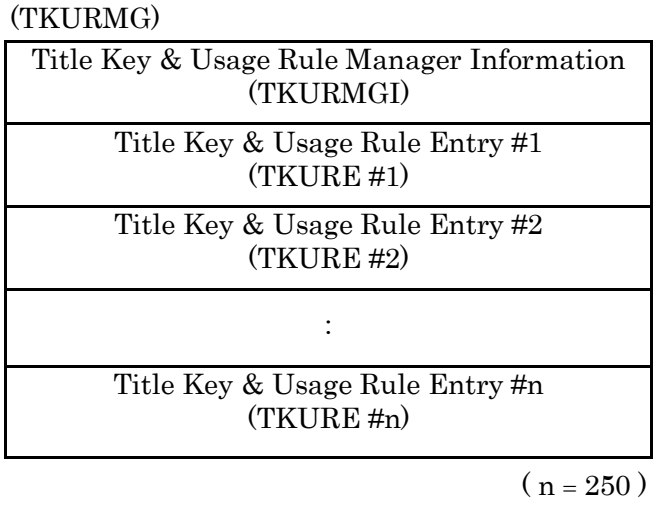


Figure 3-5 Title Key & Usage Rule Manager (TKURMG)

A TKURMG file starts with a Title Key & Usage Rule Manager Information (TKURMGI), followed by a set of Title Key & Usage Rule Entries (TKUREs). TKURE number is from 1 to 250, but TKURE numbers from 100 to 250 are not used in case of TKURE for Programs.

3.7.4 Title Key & Usage Rule Manager Information (TKURMGI)

As shown in Table 3-9, the TKURMGI consists of Used flag of each TKURE in the TKURMG. The same structure of TKURE is used between TKURE for Programs and MOs.

Table 3-9 TKURMGI

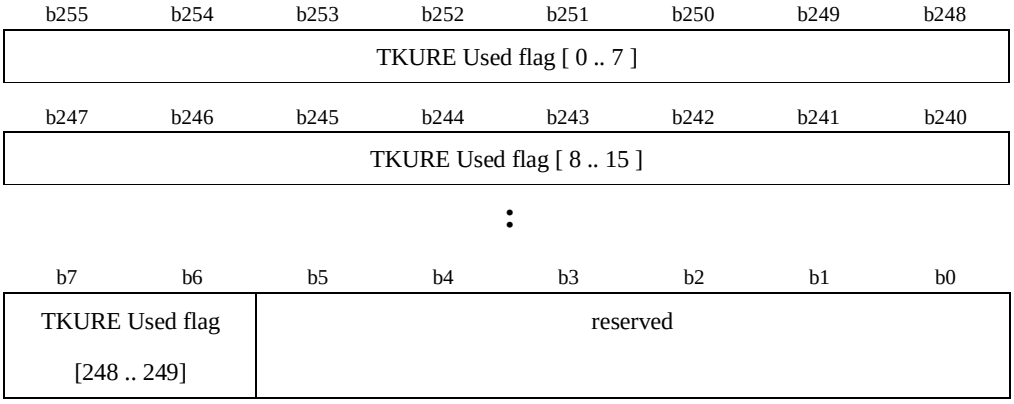
(Description order)

RBP	Field Name	Contents	Number of bytes
0 to 31	TKURE_USED	TKURE Used flag	32 bytes
32 to 383	Reserved	Reserved	352 bytes
Total			384 bytes

All reserved bits shall be set to '0.'

(RBP 0 to 31) TKURE_USED

This field describes whether each TKURE in this TKURMG is used or not.



TKURE Used flag [*j*] ... 0b: TKURE # *j+1* in this TKURMG is not used.

(TKURE # *j+1* is vacant.)

1b: TKURE # *j+1* in this TKURMG is used.

(TKURE # *j+1* is not vacant.)

In case of TKURE for Programs, because TKURE numbers from 100 to 250 are not used, TKURE Used flag from 99 to 249 shall be always 0.

3.7.5 Title Key & Usage Rule Entry (TKURE)

As shown in Table 3-10, a TKURE field contains Title Key Area (TKA) and Usage Rules (UR) of the corresponding encrypted content. The whole TKURE is encrypted using C2_ECBC (both fields are concatenated and then encrypted using C2_ECBC).

Table 3-10 TKURE

(Description order)

RBP	Field Name	Contents	Number of bytes
0 to 7	TKA	Title Key Area	8 bytes
8 to 63	UR	Usage Rules	56 bytes
Total			64 bytes

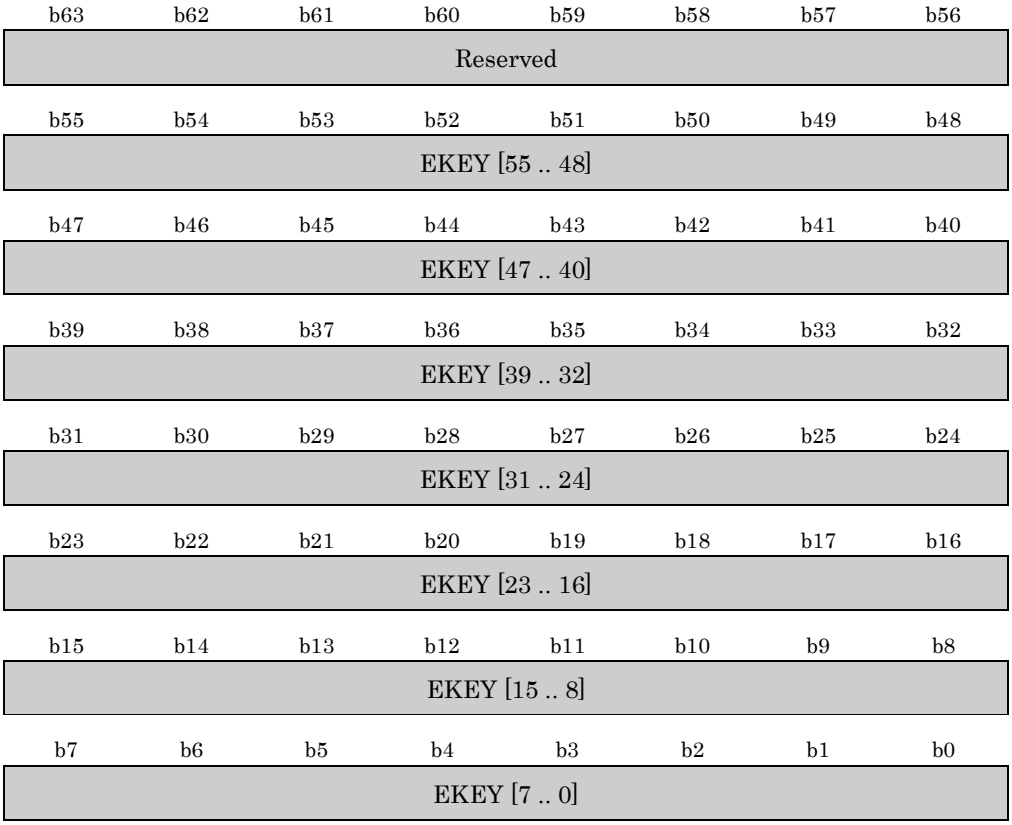
3.7.5.1 Title Key Area (TKA)

As shown in Table 3-9, TKA contains EKEY field. This field describes the Title Key of the corresponding encrypted content.

Table 3-11 TKA

(Description order)

RBP	Field Name	Contents	Number of bytes
0	Reserved	Reserved	1 byte
1 to 7	EKEY	Title Key	7 bytes
Total			8 bytes



EKEY ... Stores the Title Key.

All reserved bits (from b56 to b63) shall be set to '0.' For forward compatibility, devices shall ignore non-zero values in these reserved fields.

3.7.5.2 Usage Rules (UR)

As follows, Table 3-12 shows the scope of the Usage Rules. Specifically Usage Rules (UR) consists of Trigger Bit Information, Initial Move Control Information, Current Move Control Information, Copy Count Control Information, CCI Flags Control Information (i.e. Analog Protection System Control Information), Current Start Date of Playback Period, Current End Date of Playback Period, Current Playback Counter, Initial Start Date of

Playback Period, Initial End Date of Playback Period, Initial Playback Counter, Playback Span, and Check Value.

Table 3-12 UR

(Description order)

RBP	Field Name	Contents	Number of bytes
0	UR_TRIGGER	Trigger Bit Information	1 byte
1	UR_MCCNTRL	Initial Move Control Information / Current Move Control Information / Copy Count Control Information	1 byte
2	UR_CCIFLAGS	CCI Flags	1 byte
3 to 5	UR_C_STRTDATE	Current Start Date of Playback Period	3 bytes
6 to 8	UR_C_ENDDATE	Current End Date of Playback Period	3 bytes
9 to 10	UR_C_P_CNT	Current Playback Counter	2 bytes
11 to 16	Reserved	Reserved	6 bytes
17 to 19	UR_I_STRTDATE	Initial Start Date of Playback Period	3 bytes
20 to 22	UR_I_ENDDATE	Initial End Date of Playback Period	3 bytes
23 to 24	UR_I_P_CNT	Initial Playback Counter	2 bytes
25 to 30	Reserved	Reserved	6 bytes
31 to 33	UR_ SPAN	Playback Span	3 bytes
34 to 47	Reserved	Reserved	14 bytes
48 to 55	UR_CHECK	Check Value	8 bytes
Total			56 bytes

All reserved bits shall be set to ‘0.’ For forward compatibility, devices shall ignore non-zero values in these reserved fields, unless otherwise specified.

In the following definition of Usage Rule fields, the assigned values are effective only when the TKURE is used. When the TKURE is not used, no specific value is assigned to each Usage Rule field.

(RBP 0) UR_TRIGGER

This field describes Trigger Bit Information.

b7	b6	b5	b4	b3	b2	b1	b0
Trigger bit		Reserved					

Trigger bit ... 0Xb : Devices shall ignore bytes 3 through 33., that is, they shall ignore fields containing date and time-based usage rules, where X is an arbitrary bit.

10b: Devices shall process bytes 3 through 33, that is, they shall process fields containing date and time-based usage rules.

11b : Accessing devices conforming to this specification shall not be permitted the Move/Copy/Playback processes.

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 Usage Rules may be expanded, or other information for controlling these processes may be added. Accessing devices of the future version shall process the new information for controlling these processes correctly when these bits are set to '11b.'

(RBP 1) UR_MCCNTRL

This field describes the Initial Move Control Information, Current Move Control Information, and Copy Count Control Information.

b7	b6	b5	b4	b3	b2	b1	b0
Initial Move Control Information		Current Move Control Information		Copy Count Control Information			

Initial Move Control Information ... 00b : Move is never permitted.

01b : Move is permitted once.

11b : Move is permitted unlimited times.

		others : Reserved. The Initial Move Control Information is set when the corresponding content is distributed. It never changes even when the content is moved. This field is inherited to a replicated content when copying.
Current Move Control Information	...	00b : Move is never permitted. 01b : Move is permitted once. 11b : Move is permitted unlimited times. others : Reserved. The Current Move Control Information changes when the corresponding content is moved. As for the details how conforming devices shall change this field, refer to the Move process described in Section 3.8 *Process Description* of this specification.
Copy Count Control Information	...	0000b : Copy is never permitted. 0001b~1110b : Copy is permitted specified times.

1111b : Copy is permitted unlimited times and this value is regarded as EPN (Encryption plus Non-assertion) asserted.

The Copy Count Control Information changes when the corresponding content is copied. When copying is executed, this field of an originated content shall be decremented, and that of a replicated content shall be set to '0000b.' As for the details how conforming devices shall change this field, refer to the Copy process described in Section 3.8 *Process Description* of this specification.

When this content is output, CGMS and EPN are set as follows;

Copy Count Control Information	CGMS	EPN
0000b	No more copies	Unasserted
0001b~1110b	No more copies	Unasserted
1111b	Copy freely	Asserted

(RBP 2) UR_CCIFLAGS

This field describes StrmCCI, AST and APSTB.

b7	b6	b5 b4	b3 b2 b1 b0
StrmCCI	AST	APSTB	Reserved

StrmCCI … In the case that the contents file format is not TOD file,

This field shall be set to '0b.'

Copy control is performed by Copy Count Control Information in UR_MCCNTRL and APSTB in UR_CCIFLAGS.

In the case that the contents file format is TOD file,

This field shall be set to '1b.'

Copy control is performed by E_CPF and E_APSTB field in RDI Packet. In this case Copy Count Control Information in UR_MCCNTRL shall be set to '0000b' and APSTB in UR_CCIFLAGS shall be set to '00b.'

AST … 0b: Analog Sunset is not applied.

1b: Analog Sunset is applied to Decrypted CPRM Video Content in accordance with the *CPRM/CPPM License Agreement.*

APSTB ... 00b : APS is Off

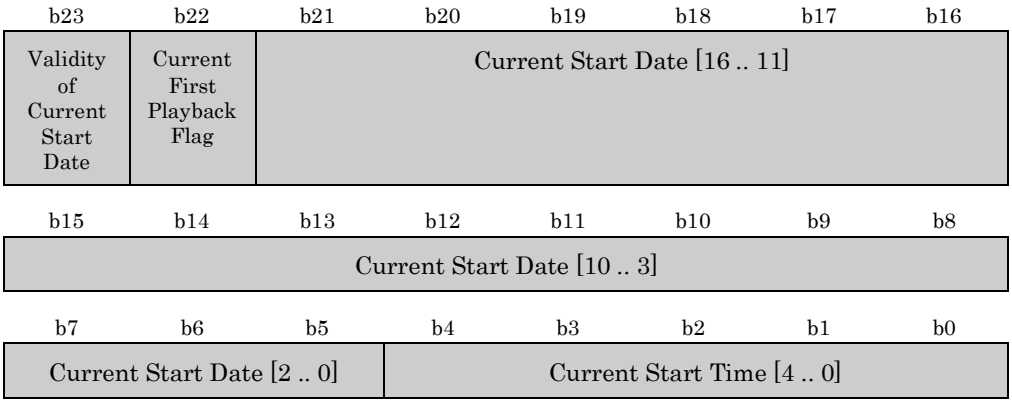
01b: Type 1 of APS is On

10b: Type 2 of APS is On

11b: Type 3 of APS is On

(RBP 3 to 5) UR_C_STRTDATE

This field describes the current start date and time of permitted playback period.



Validity of Current Start Date ... 0b : The current start date of permitted playback period is not specified.

1b : The current start date of permitted playback period is specified.

Current 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 Current Start Date and the Current End Date have already been fixed.

Current Start Date ... This field describes the current start date in Modified Julian Date format.

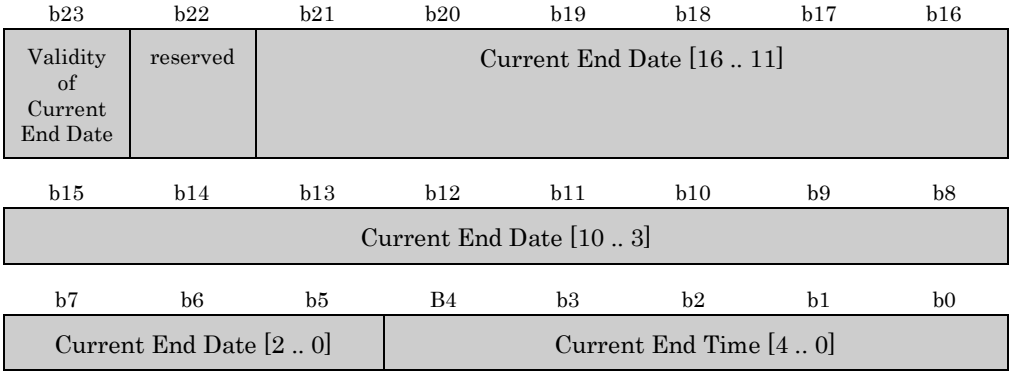
Current Start Time ... This field describes the current start time by the hour.

0~23: Hours from midnight.

others: Reserved.

(RBP 6 to 8) UR_C_ENDDATE

This field describes the current end date and time of permitted playback period.



Validity of Current End Date ... 0b : The current end date of permitted playback period is not specified.

1b : The current end date of permitted playback period is specified.

Current End Date ... This field describes the current end date in Modified Julian Date format.

Current End Time ... This field describes the current end time by the hour.

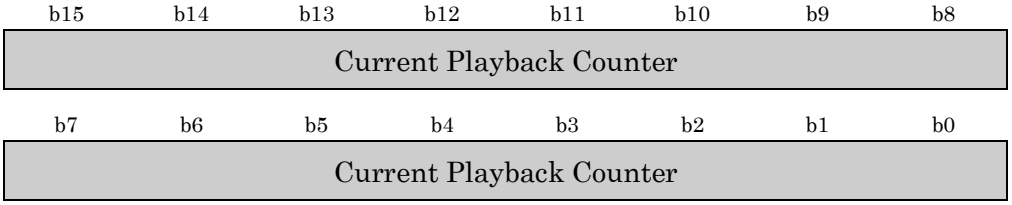
0~23: Hours from midnight.

others: Reserved.

UR_C_STRTDATE is set to the same value as that of UR_I_STRTDATE and UR_C_ENDDATE is set to the same value as that of UR_I_ENDDATE when the corresponding content is distributed. When the corresponding content is played for the first time, these fields may change according to the validity of the playback span. These fields shall not be inherited to a replicated content when copying. For details how conforming devices shall change these fields, refer to the Playback process described in Section 3.8 *Process Description* of this specification.

(RBP 9 to 10) UR_C_P_CNT

This field describes the current permitted playback count.



Current Playback Counter ... 0000h : Playback is never permitted.

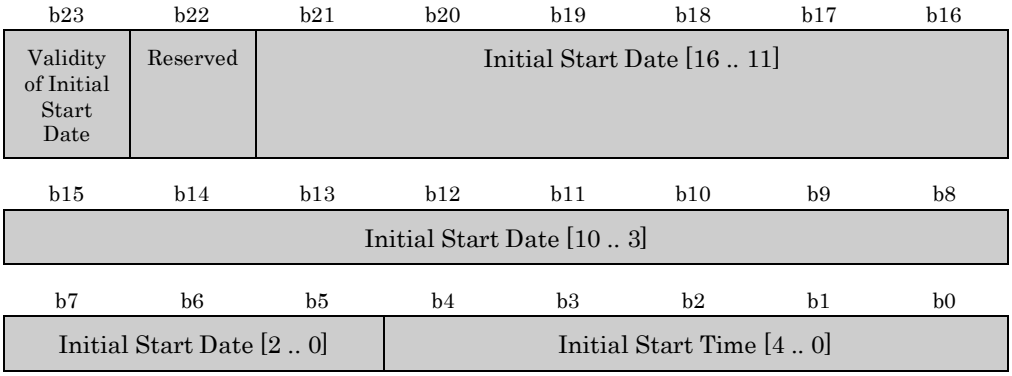
... 0001h~FFFEh : Playback is permitted specified times.

... FFFFh : Playback is permitted unlimited times.

This field may change when the corresponding content is played. This field shall not be inherited to a replicated content when copying. For details on how conforming devices shall change this field, refer to the Playback process described in Section 3.8 *Process Description* of this specification.

(RBP 17 to 19) UR_I_STRTDATE

This field describes the initial start date and time of permitted playback period.



Validity of Initial Start Date ... 0b : The initial start date of permitted playback period is not specified.

1b : The initial start date of permitted playback period is specified.

Initial Start Date ... This field describes the initial start date in Modified Julian Date format.

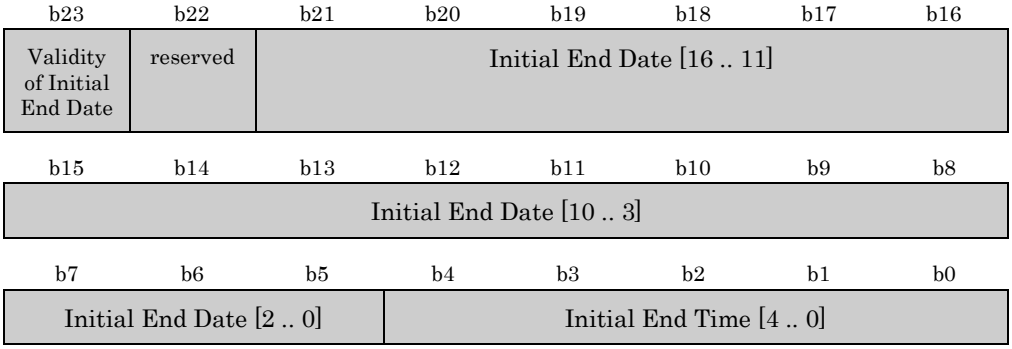
Initial Start Time ... This field describes the initial start time by the hour.

0~23: Hours from midnight.

others: Reserved.

(RBP 20 to 22) UR_I_ENDDATE

This field describes the initial end date and time of permitted playback period.



Validity of Initial End Date ... 0b : The initial end date of permitted playback period is not specified.

1b : The initial end date of permitted playback period is specified.

Initial End Date ... This field describes the initial end date in Modified Julian Date format.

Initial End Time ... This field describes the initial end time by the hour.

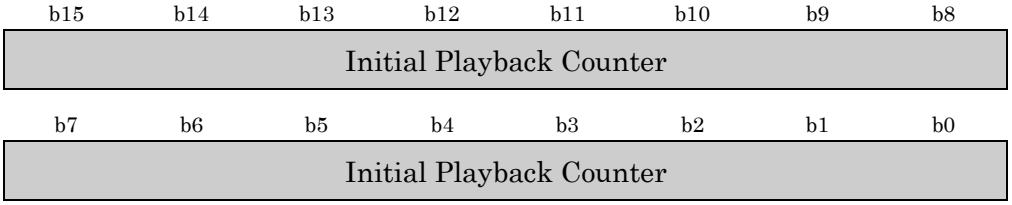
0~23: Hours from midnight.

others: Reserved.

UR_I_STRTDATE and UR_I_ENDDATE are set when the corresponding content is distributed and shall not be changed. These fields shall be inherited to a replicated content when copying.

(RBP 23 to 24) UR_I_P_CNT

This field describes the initial permitted playback count.



Initial Playback Counter ... 0000h : Playback is never permitted.

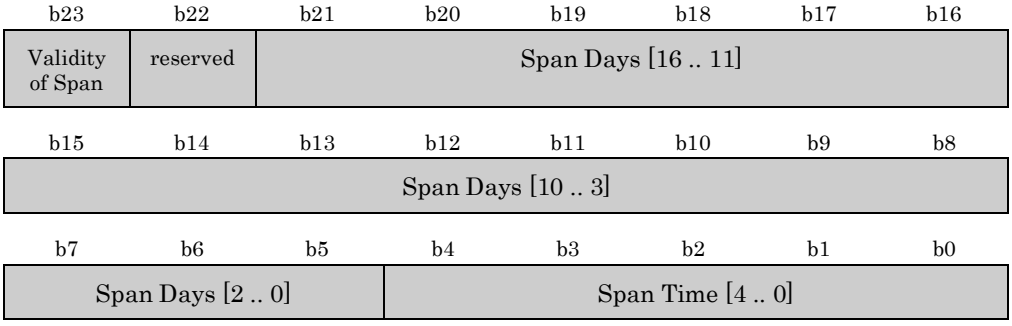
... 0001h~FFFEh : Playback is permitted specified times.

... FFFFh : Playback is permitted unlimited times.

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

(RBP 31 to 33) UR_SPAN

This field describes the permitted playback span.



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.

0~23: Valid hours.

others: Reserved.

This field is set when the corresponding content is distributed and shall not be changed. This field shall be inherited to a replicated content when copying.

(RBP 48 to 55) UR_CHECK

This field stores the 64-bit check value, '0123456789ABCDEFh.'

3.7.6 Time Based Usage Rules Time Stamp (TBUR.TS)

There are two timestamp files, one in the Root Directory and another in the SD_VIDEO Directory. The latter is encrypted and consists of 64-bit fields: Arbitrary Number field and two 32-bit fields: the Time Stamp field and the Verification Data field. The timestamp file in the Root Directory is in the clear and consists of two 32-bit fields; The Time Stamp field and the reserved field. Namely, the Time Stamp field has the same format (except from being encrypted).

3.7.6.1 \SD_VIDEO\TBUR.TS

The following table describes the timestamp file in the SD_VIDEO directory (i.e. the encrypted timestamp file)

Table 3-13 \SD_VIDEO\TBUR.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_VIDEO\TBUR.TS file is encrypted using C2_ECBC. This encryption is performed with the same media unique key as the one used to encrypt TKURE files, 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.)*

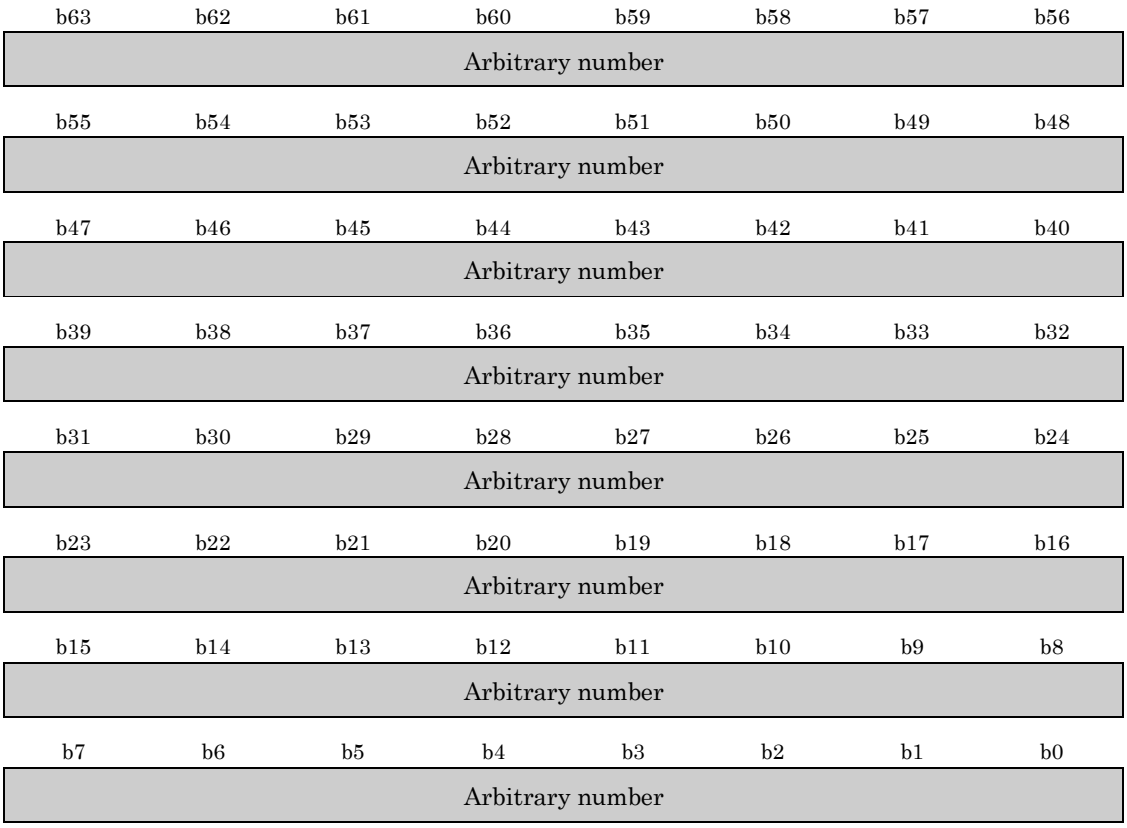
Namely, \SD_VIDEO\TBUR.TS contains Encrypted Time Stamp Data (D_{tse}) as:

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

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

(RBP 0 to 15) 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 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.

Devices 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 player 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.

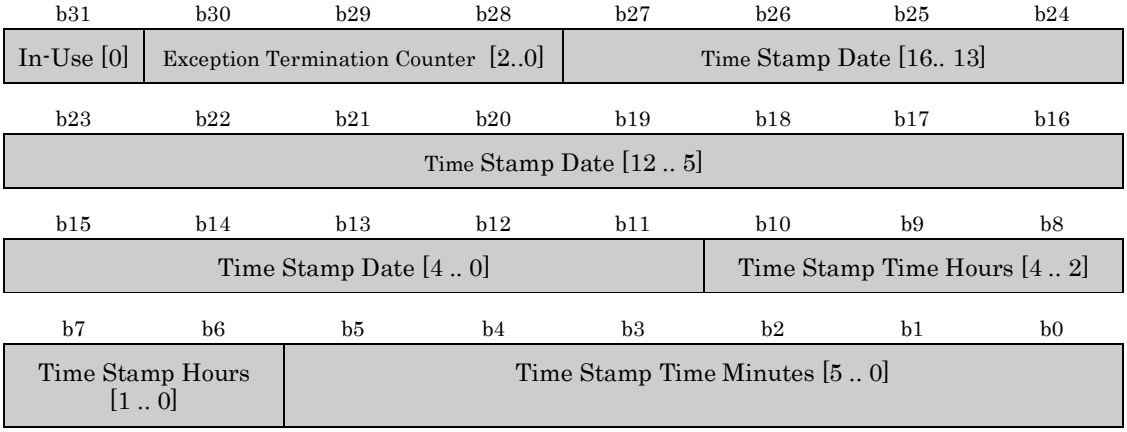
An SD Memory Card is considered not to be in-use if

- Any Playback Device is playing content that does not have date and time-based usage conditions.
- A device has finished playing content that has date and time-based usage rules.

Details on how to update the in-use flag and counter are explained in Section 3.8 *Process Definition* of this specification. In the case of the TBUS.TS in the SD_VIDEO directory, this TBUS_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 Current Start Date and the Current 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-based usage rules is considered an exception. In contrast, playback of content without date and time usage conditions always stops smoothly. That is, pulling the card in this case shall not impact the Exception Termination Counter. 0~5: 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 3.8.7 Playback Process of this specification. Others: Reserved
Time Stamp Date	...	This field describes the current time stamp date in Modified Julian Date format.
Time Stamp Time Hours	...	This field describes the current time stamp by the hour. 0~23: Hours from midnight. others: Reserved.
Time Stamp Time Minutes	...	This field describes the current timestamp by the minutes. 0~59: minutes after the hour stated in Time Stamp Time Hours field. others: Reserved.

(RBP 12 to 15) TS Verification Data

This field stores the 32-bit Verification Data, $DEADBEEF_{16}$.

b31	b30	b29	b28	b27	b26	b25	b24
$DEADBEEF_{16}$ [31 .. 24]							
b23	b22	b21	b20	b19	b18	b17	b16
$DEADBEEF_{16}$ [23 .. 16]							
b15	b14	b13	b12	b11	b10	b9	b8
$DEADBEEF_{16}$ [15 .. 8]							

Verification Data ... This field describes the verification data DEADBEEF$_{16}$

If encrypted timestamp file is decrypted successfully, as described below, bytes 12 through 15 contain the value DEADBEEF$_{16}$, 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:

$$[D_{ts}]_{lsb\_32} = DEADBEEF_{16}$$

3.7.6.2 \TBUR.TS

The following table describes the timestamp file in the root directory, that is, the timestamp file in the clear.

Table 3-14 \TBUR.TS

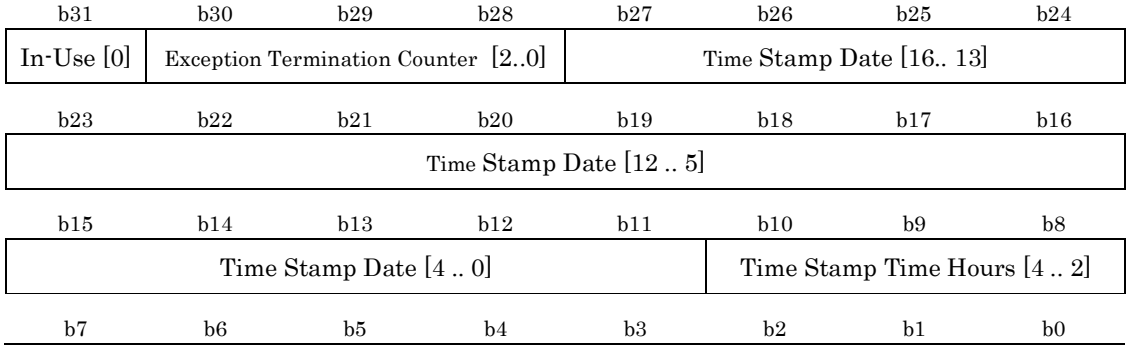
(Description order)

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.



Time Stamp Hours [1 .. 0]	Time Stamp Time Minutes [5 .. 0]

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

(RBP 4 to 7) 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							
b7	b6	b5	b4	b3	b2	b1	b0
Reserved							

3.7.6.3 Processing the timestamp file (TBUR.TS)

The process of recording and updating the timestamp file (TBUR.TS) is described as follows:

- When recording the downloaded content with date and time-based usage rules, all SD-Video compliant devices shall record a timestamp in the TBUR.TS file in the Protected Area of the SD Memory Card.
- When playing the content with date and time-based usage rules,
  - SD-Video compliant devices shall update the timestamp in the TBUR.TS file in the Protected Area of the SD Memory Card,

All devices are allowed to update the timestamp in the TBUR.TS file located in the Root directory. Devices that do not have time-based usage capabilities shall not play content with time-based usage rules; hence they shall ignore the TBUR.TS in the SD_VIDEO directory. Details on the procedures to update timestamp files are described in Section 3.8 *Process Description* of this specification. For instance, one fundamental rule is that the timestamp in a TBUR.TS file can only be updated to a later time. A device with time-based usage capabilities shall

- update the TBUR.TS in the SD_VIDEO directory (\SD_VIDEO\TBUR.TS).
- update the TBUR.TS in Root directory (\TBUR.TS).
- in the case that both TBUR.TS files exist (\TBUR.TS and \SD_VIDEO\TBUR.TS), set the reference time as that defined by the timestamp with a later date and time.

SD-Video applications 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 timestamp in the SD_VIDEO directory records the last time that an SD-Video application used the SD Memory Card. Analogously, the timestamp 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, other than SD-Video, 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. SD-Video applications shall update both timestamp files, in the Root directory and in the SD_VIDEO directory with the same data. If there is no TBUR.TS file when the SD Memory Card gets content with date and time-based usage rules, the file shall be created. Details on the initial content for this file are described in Recording Process, Section 3.8.1of 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 a title is played or recorded the device must read the timestamp in the SD Memory Card. The device shall read the timestamp in the TBUR.TS file in the SD_VIDEO directory and 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 the timestamp in the SD Memory Card is later than device's clock, the device must refuse to play or record such content
- Every time a device plays or records a title with calendar usage conditions, the device is required to write the current time to the SD Memory Card. The time is stored in both files in the Protected Area: the TBUR.TS file in the SD_VIDEO 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.TS timestamp file in the SD_VIDEO 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 date and 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.

3.8 Process Description

This section describes Recording, Erasing, Copy, Move and Playback processes.

- Recording Process

  Specifies how a Recording Device (e.g. Kiosk) writes CPRM protected SD-Video content to an SD Memory Card.

- Erasing Process

  Specifies how an Erasing Device erases CPRM protected SD-Video content from an SD Memory Card.

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

  Specifies how CPRM protected SD-Video content on an SD Memory Card is copied securely to a Destination Device (e.g. personal computer).

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

  Specifies how CPRM protected SD-Video content on a Source Device is copied securely to an SD Memory Card.

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

  Specifies how CPRM protected SD-Video content on an SD Memory Card is copied securely to a Destination Device (e.g. personal computer) and how it is made permanently unusable on the SD Memory Card.

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

  Specifies how CPRM protected SD-Video content on a Source Device is copied securely to an SD Memory Card and how it is made permanently unusable on the Source Device.

- Playback Process

  Specifies how CPRM protected SD-Video content on an SD Memory Card is played back by a Playback Device in conformance with the content's Usage Rules.

When aborting or terminating each process, the processing device shall delete all the temporary images of TKURE/TKURMG/TKURMMG, which are either read from the SD Memory Card or created on the device.

In this section, 'Initial Field Group,' 'Current Field Group,' and 'Fixed Field Group' are used to represent groups of the Usage Rule fields defined as follows:

- 'Initial Field Group' consists of the Initial Start Date of Playback Period field, the Initial End Date of Playback Period field, and the Initial Playback Counter field. Notice that 'Initial Field Group' information has the following characteristics: a) shall be set when the corresponding content is distributed, b) shall not be change even when the content is moved, and c) shall be inherited to a replicated content when copying.
- 'Current Field Group' consists of the Current Start Date of Playback Period field, the Current End Date of Playback Period field, and the Current Playback Counter field.
- 'Fixed Field Group' consists of the Playback Span field.

In addition, following sub-processes are used in each process described in this section. As for the details for these processes, see the corresponding references.

- 'Secure Read Process' is described in *SD Memory Card Book Common Part* Section 3.5.
- 'Secure Write Process' is described in *SD Memory Card Book Common Part* Section 3.5.
- ' TKURE Encryption Process (Title Key & Usage Rule Encryption Process)' is described in Section 3.4 (step (4a.1)) of this specification.
- ' TKURE Decryption Process (Title Key & Usage Rule Decryption Process)' is described in Section 3.4 (step (4b.3)) of this specification.

When TKURMMG, TKURMG and TKURE are used without distinction between Programs and MOs in this section., these descriptions mean they are applied to both cases in the same manner

3.8.1 Recording Process

The Recording Device securely holds information associated with SD-Video content to be recorded. The information includes the Usage Rules given by a Content Provider and a Title Key that has a secret unpredictable value (e.g. given by the Content Provider or selected at random). If the information does not include the field which indicates Move is not permitted, it is treated as Move is permitted unlimited times.

In the case of recording the content without date and time-based usage rules, step (5) is skipped.

(1) Read the TKURMMG file from the SD Memory Card.

The Recording Device securely reads the TKURMMG file from the SD Memory Card using the Secure Read Process and holds it as the temporary TKURMMG image.

(2) Read or create a TKURMG.

(2.1) Select a TKURMG file that has at least one unused TKURE.

The Recording Device checks the TKURMG Used flag (TKURMG_USED) field in the temporary TKURMMG image. The Recording Device selects the first TKURMG file whose TKURMG Used flag is equal to '0b.' If all the TKURMG Used flags are equal to '1b,' the process shall be aborted.

(2.2) Read the selected TKURMG file from the SD Memory Card or create a temporary TKURMG image on the Recording Device.

The Recording Device checks whether the selected TKURMG file exists or not.

(a) When the selected TKURMG file exists, the Recording Device securely reads the selected TKURMG file from the SD Memory Card using the Secure Read Process and holds it as the temporary TKURMG image.

(b) When the selected TKURMG file does not exist, the Recording Device creates a new TKURMG image on the Recording Device.

(3) Update the temporary TKURMG and TKURMMG image.

(3.1) Update the TKURE in the temporary TKURMG image.

The Recording Device checks the TKURE Used flag (TKURE_USED) in the temporary TKURMG image, and finds the first unused TKURE.

The Recording Device updates the unused TKURE in the temporary TKURMG image as follows:

- The Initial Move Control Information and Copy Count Control Information, Initial Field Group and Fixed Field Group of the TKURE are set to the value specified by the Content Provider.
- When there is an indication that Analog Sunset in accordance with the *CPRM/CPPM License Agreement* is required, the AST shall be set to 1b.
- The CCIFlags of the TKURE is set to the value specified by the Content Provider.
  - If StrmCCI in CCIFlags is equal to '1b,' CCI_byte and E_CCI_byte in RDI Packet in the content is set to the value specified by the Content Provider and RDI_CHECK in RDI Packet in the content is set to '0123456789ABCDEFh.'
- The Current Move Control Information is set to the same value as that of the Initial Move Control Information specified by the Content Provider.
- The Trigger bit is set to '0Xb' or '10' as appropriate. That is, '0X' should be used in the case where devices shall ignore fields containing date and time-based usage rules, and '10' should be use in the case where the devices must process fields that contain date and time-based usage rules.

- The Check Value is set to '0123456789ABCDEFh.'

After all the fields in the unused TKURE are set as above, the Recording Device encrypts the TKURE in the temporary TKURMG image using the TKURE Encryption process.

(3.2) Set the TKURE_USED in the temporary TKURMG image and the TKURMG_USED in the temporary TKURMMG image.

The Recording Device sets the TKURE Used flag associated with the updated TKURE in the temporary TKURMG image to '1b.'

In addition, when all the TKURE Used flags are equal to '1b' (all the TKUREs in the temporary TKURMG image have been used), the TKURMG Used flag associated with the selected TKURMG file in the temporary TKURMMG image shall be set to '1b.'

(4) Write the updated temporary TKURMG and TKURMMG image to the SD Memory Card.

The Recording Device securely writes the updated temporary TKURMG image held in the Recording Device as the updated TKURMG file to the SD Memory Card using the Secure Write Process. When a new TKURMG image was created in step (2.2), the updated temporary TKURMG image is written as a new TKURMG file using the Secure Write Process.

In addition, if the temporary TKURMMG image is updated in step (3.2), the Recording Device securely writes the updated temporary TKURMMG image held in the Recording Device as the updated TKURMMG file to the SD Memory Card using the Secure Write Process.

(5) Update Timestamp File

The Recording Device records SD-Video content onto the SD Memory Card. The Recording 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 Recording Device shall not overwrite a timestamp in the future. The Recording Device is allowed to record content when the timestamp is in the future (a compliant playback device shall refuse to play such content until the timestamp catches up with the current time). A Recording Device must perform the following steps:

- If only the \SD_VIDEO\TBUR.TS exists, check the verification of the 'DEADBEEFh' hexadecimal value in this file. If this check fails, this process shall be aborted.
- If both timestamp files exist (i.e. the \SD_VIDEO\TBUR.TS and \TBUR.TS) check the verification of the 'DEADBEEFh' hexadecimal value in the \SD_VIDEO\TBUR.TS. If this check fails, this process shall be aborted.
- If only the \SD_VIDEO\TBUR.TS exists, set the reference time to that in that file. If both timestamp files exists (i.e. SD_VIDEO\TBUR.TS and \TBUR.TS) choose the latest timestamp to be the reference time
- Read 'In-Use' flag and ETC from the file in the SD_VIDEO directory.
- If only the \SD_VIDEO\TBUR.TS exists and the reference time is in the past, write both timestamp files with the current time, In-Use = '0b' and ETC = '0h.' Otherwise, write the reference time to both timestamp files with In-Use = '0b' and ETC unchanged.
- If neither the \TBUR.TS nor the \SD_VIDEO\TBUR.TS exist, the recorder must create both files (in the clear and encrypted, respectively) with the timestamp set to the current time, 'In-Use' = '0b.' and ETC = '0h.'
- If only the \TBUR.TS exists, create \SD_VIDEO\TBUR.TS file. Set flag In-Use = '0b.' and counter ETC = '0h' on both TBUR.TS files. If the timestamp is in the future, leave timestamp unchanged in \TBUR.TS and write such timestamp to \SD_VIDEO\TBUR.TS file. If the timestamp is in the past, write current time to both TBUR.TS files.

To protect against the "Pull Card Attack," the Recording Device must assume that the Recording Process has been completely done, even if errors occur in step (4).

3.8.2 Erasing Process

(1) Determine the TKURMG file and TKURE associated with the content to be erased.

(1.1) Obtain TKURE_SRN.

The Erasing Device obtains the TKURE_SRN ***s*** associated with the content to be erased.

(1.2) Determine the TKURMG file and TKURE associated with the content to be erased.

The Erasing Device determines the TKURMG filename and the TKURE using the following formula:

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

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

For example, when the TKURE_SRN is 1010, the TKURE shall be in the fifth TKURMG file ("MO005.KEY" in the case of TKURE for MOs) and the TKURE shall be tenth entry in the file. But the TKURE for Programs shall be always in the first TKURMG file ("VIDEO001.KEY") because TKURE_SRN for Programs is less than or equal to 99.

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

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

Then, the Erasing Device checks the ***m***th TKURE Used flag in the temporary TKURMG image. If it is equal to '0b,' the process shall be aborted.

Otherwise, the Erasing Device obtains the ***m***th TKURE in the temporary TKURMG image.

(3) Update the temporary TKURMG and TKURMMG image.

The Erasing Device overwrites this TKURE in the temporary TKURMG image with "the value for delete (random number)."

The Erasing Device shall set the TKURE Used flag associated with the TKURE in the temporary TKURMG image to '0b.'

In addition, the Erasing Device checks all the TKURE Used flags in the temporary TKURMG image.

(a) When all the TKURE Used flags are equal to '0b,' the Erasing Device deletes the selected TKURMG file from the Protected Area of the SD Memory Card, and then considers this process to be successfully terminated.

(b) When all the TKURE Used flags other than the one associated with the overwritten TKURE are equal to '1b,' the Erasing Device securely reads the TKURMMG file from the SD Memory Card using Secure Read Process and holds it as the temporary TKURMMG image. Then the Erasing Device sets the ***n***th TKURMG Used flag in the temporary TKURMMG image to '0b.'

(4) Write the updated temporary TKURMG and TKURMMG image to the SD Memory Card.

The Erasing Device securely writes the updated temporary TKURMG image as the updated TKURMG file to the SD Memory Card using the Secure Write Process. Then the Erasing Device securely reads the updated TKURMG file from the SD Memory Card using the Secure Read Process and verifies that the value of the ***m***th TKURE in the TKURMG file is equal to "the value for delete (random number)" used in step (3). If the verification of the TKURMG file fails, the Erasing Device shall abort this process.

In addition, if the temporary TKURMMG image was updated in step (3b), the Erasing Device securely writes the updated temporary TKURMMG image as the updated TKURMMG file to the SD Memory Card using the Secure Write Process.

3.8.3 Copy Process I (from SD Memory Card to Host)

(1) Determine the TKURMG file and TKURE associated with the content to be copied.

(1.1) Obtain TKURE_SRN.

The Destination Device obtains the TKURE_SRN ***s*** associated with the content to be copied.

(1.2) Determine the TKURMG file and TKURE associated with the content to be copied.

The Destination Device determines the TKURMG filename and the TKURE using the following formula:

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

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

For example, when the TKURE_SRN is 1010, the TKURE shall be in the fifth TKURMG file ("MO005.KEY" in the case of TKURE for MOs) and the TKURE shall be tenth entry in the file. But the TKURE for Programs shall be always in the first TKURMG file ("VIDEO001.KEY") because TKURE_SRN for Programs is less than or equal to 99.

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

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

Then, the Destination Device checks the ***m***th TKURE Used flag in the temporary TKURMG image. If it is equal to '0b,' the process shall be aborted.

Otherwise, the Destination Device obtains the ***m***th TKURE in the temporary TKURMG image.

(3) Check the TKURE in the temporary TKURMG image.

The Destination Device decrypts the TKURE using the Title Key and Usage Rule Decryption process described in Section 3.4 of this specification, and securely holds it as the decrypted TKURE image. The Destination Device checks this decrypted TKURE image.

- If the Check Value is not '0123456789ABCDEFh,' the process shall be aborted.
- If the Trigger bit is '11b,' the process shall be aborted.
- If StrmCCI is equal to '1b.' copy permission of the Packet Sequence is controlled by the corresponding RDI Packet.
    - For each Packet Sequence, following processes are executed;
        - The Destination Device reads the corresponding RDI Packet from the SD Memory Card.
        - If the RDI_CHECK field in the RDI Packet is not equal to '0123456789ABCDEFh,' the process shall be aborted.
        - If the E_CPF field in the RDI Packet is equal to '11b,' the process continues for next Packet Sequence.
        - If the E_CPF field in the RDI Packet is equal to '10b,' the Destination Device reads the Packet Sequence and holds it, and then continues for next Packet Sequence.
    - If all the E_CPF fields in RDI Packet in the processed Packet Sequences have '11b' value, the process shall be aborted. Otherwise, go to step (6).
- If the Copy Count Control Information is equal to '0000b,' the process shall be aborted.
- If the Copy Count Control Information is equal to '1111b,' then go to step (6).

(4) Update the decrypted TKURE image.

The Destination Device decrements the value of Copy Count Control Information of the decrypted TKURE image. Then the Destination Device encrypts this decrypted TKURE image using the TKURE Encryption process, and sets the ***m***th TKURE in the temporary TKURMG image to the resulting value.

(5) Write the updated temporary TKURMG image to the SD Memory Card.

The Destination Device securely writes the updated temporary TKURMG image as the updated TKURMG file to the SD Memory Card using the Secure Write Process. Then the Destination Device securely reads the updated TKURMG file from the SD Memory Card using the Secure Read Process and verifies that the update of the ***m***th TKURE in the TKURMG file has completed successfully.

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

(6) Update the Usage Rules on the Destination Device.

The Destination Device temporarily holds the decrypted TKURE image as the associated Title Key and Usage Rules for the copied content on the Destination Device.

The Destination Device updates those Usage Rule fields as follows:

- If the Copy Count Control Information is not equal to '1111b,' the Copy Count Control Information is set to '0000b.'
- The Current Move Control Information field is set to the same value as that of the Initial Move Control Information field.
- Each field in the Current Field Group is set to the same value as that of each corresponding field in the Initial Field Group. (Here, the Current First Playback Flag in the Current Start Date of Playback Period is set to be '0b.')

When all of the above steps are executed successfully, the Destination Device securely holds the Title Key and the updated Usage Rules as the associated Title Key and Usage Rules for the copied content. In step (3), if StrmCCI is equal to '1b,' the Destination Device shall execute following step.

- Generate a new Title Key that has a secret unpredictable value.
- Decrypt the copied Packet Sequence with the associated Title Key and encrypt it with the new Title Key.
- Securely hold the new Title Key for the copied Packet Sequence instead of the original Title Key.

3.8.4 Copy Process II (from Host to SD Memory Card)

The Source Device securely holds information associated with SD-Video content to be copied. The information includes the Usage Rules and a secret unpredictable Title Key. When the following steps are executed, if necessary, the Source Device appropriately converts the Usage Rules securely held in it into the Usage Rules specified by this specification (e.g. Copy Count Control Information, StrmCCI).

(1) Check the Usage Rules on the Source Device.

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

- When there is an indication that Analog Sunset in accordance with the CPRM/CPPM License Agreement is required, the AST shall be set to 1b.
- If StrmCCI is equal to '0b' and the Copy Count Control Information is equal to '0000b,' then the process shall be aborted.
- If StrmCCI is equal to '1b,' copy permission of the Packet Sequence is controlled by the corresponding RDI Packet.
    - For each Packet Sequence, following processes are executed;
        - The Source Device checks the corresponding RDI Packet held in it.

- If the RDI_CHECK field in the RDI Packet is not equal to '0123456789ABCDEFh,' the process shall be aborted.
- If the E_CPF field in the RDI Packet is equal to '11b,' the process continues for next Packet Sequence.
- If the E_CPF field in the RDI Packet is equal to '10b,' the Source Device writes the Packet Sequence to SD Memory Card, and then continues for next Packet Sequence.

- If all the E_CPF fields in RDI Packet in the processed Packet Sequences have '11b' value, the process shall be aborted.

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

The Source Device securely reads the TKURMMG file from the SD Memory Card using the Secure Read Process and holds it as the temporary TKURMMG image.

(3) Read or create a TKURMG.

(3.1) Select a TKURMG file that has at least one unused TKURE.

The Source Device checks the TKURMG Used flag (TKURMG_USED) field in the temporary TKURMMG image. The Source Device selects the first TKURMG file whose TKURMG Used flag is equal to '0b.' If all the TKURMG Used flags are equal to '1b,' the process shall be aborted.

(3.2) Read the selected TKURMG file from the SD Memory Card or create a temporary TKURMG image on the Source Device.

The Source Device checks whether the selected TKURMG file exists or not.

(a) When the selected TKURMG file exists, the Source Device securely reads the selected TKURMG file from the SD Memory Card using the Secure Read Process and holds it as the temporary TKURMG image.

(b) When the selected TKURMG file does not exist, the Source Device creates a new TKURMG image on the Source Device.

(4) Update the temporary TKURMG and TKURMMG image.

(4.1) Update the TKURE in the temporary TKURMG image.

The Source Device checks the TKURE Used flag (TKURE_USED) in the temporary TKURMG image, and finds the first unused TKURE.

The Source Device updates the unused TKURE in the temporary TKURMG image as follows:

- If the Copy Count Control Information field of the Usage Rules held in the Source Device is equal to '1111b,' the Copy Count Control Information of the TKURE is set to '1111b.' Otherwise, the Copy Count Control Information of the TKURE is set to '0000b.'
- The Initial Move Control Information field of the TKURE is set to the same value as that of the Initial Move Control Information field of the Usage Rules held in the Source Device. The Current Move Control Information field of the TKURE is set to the same value as that of the Initial Move Control Information field of the Usage Rules held in the Source Device.
- The CCIFlags field of the TKURE is set to the same value as that of the CCIFlags field of the Usage Rules held in the Source Device.
- Each field in the Initial Field Group of the TKURE is set to the same value as that of each corresponding field in the Initial Field Group of the Usage Rules held in the Source Device.
- Each field in the Current Field Group of the TKURE is set to the same value as that of each corresponding field in the Initial Field Group of the Usage Rules held in the Source Device. (Here, the Current First Playback Flag in the Current Start Date of Playback Period of the TKURE is set to be '0b.')

- Each field in the Fixed Field Group of the TKURE is set to the same value as that of each corresponding field in the Fixed Field Group of the Usage Rules held in the Source Device.
- The Trigger bit of the TKURE is set to '0Xb' or '10b' as appropriate.
- The Check Value of the TKURE is set to '0123456789ABCDEFh.'

After all the fields in the unused TKURE are set as above, the Source Device encrypts the TKURE in the temporary TKURMG image using the TKURE Encryption process.

(4.2) Set the TKURE_USED in the temporary TKURMG image and the TKURMG_USED in the temporary TKURMMG image.

The Source Device sets the TKURE Used flag associated with the updated TKURE in the temporary TKURMG image to '1b.'

In addition, when all the TKURE Used flags are equal to '1b' (all the TKUREs in the temporary TKURMG image have been used), the TKURMG Used flag associated with the selected TKURMG file in the temporary TKURMMG image shall be set to '1b.'

(5) Update the Usage Rules on the Source Device

If the Copy Count Control Information held in the Source Device is not equal to '1111b,' the Source Device decrements the value of the Copy Count Control Information held in it.

(6) Write the updated temporary TKURMG and the TKURMMG image to the SD Memory Card.

The Source Device securely writes the updated temporary TKURMG image held in the Source Device as the updated TKURMG file to the SD Memory Card using the Secure Write Process. When a new TKURMG image was created in step (3.2), the updated temporary TKURMG image is written as a new TKURMG file using the Secure Write Process.

In addition, if the TKURMMG image was updated in step (4.2), the Source Device securely writes the updated temporary TKURMMG image held in the Source Device as the updated TKURMMG file to the SD Memory Card using the Secure Write Process.

To protect against the "Pull Card Attack," the Source Device must assume that the Copy Process II has been completely done, even if errors occur in step (6).

In step (1), if StrmCCI is equal to '1b,' the Source Device shall execute following step.

- Generate a new Title Key that has a secret unpredictable value.
- Decrypt the copied Packet Sequence with the associated Title Key and encrypt it with the new Title Key.
- Securely write the new Title Key for the copied Packet Sequence to SD Memory Card.

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

(1) Determine the TKURMG file and TKURE associated with the content to be moved.

(1.1) Obtain TKURE_SRN.

The Destination Device obtains the TKURE_SRN ***s*** associated with the content to be moved.

(1.2) Determine the TKURMG file and TKURE associated with the content to be moved.

The Destination Device determines the TKURMG filename and the TKURE using the following formula:

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

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

For example, when the TKURE_SRN is 1010, the TKURE shall be in the fifth TKURMG file ("MO005.KEY" in the case of TKURE for MOs) and the TKURE shall be tenth entry in the file. But the TKURE for Programs shall be always in the first TKURMG file ("VIDEO001.KEY") because TKURE_SRN for Programs is less than or equal to 99.

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

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

Then, the Destination Device checks the ***m***th TKURE Used flag in the temporary TKURMG image. If it is equal to '0b,' the process shall be aborted.

Otherwise, the Destination Device obtains the ***m***th TKURE in the temporary TKURMG image.

(3) Check the TKURE in the temporary TKURMG image.

The Destination Device decrypts the TKURE using the TKURE Decryption process and securely holds it as the decrypted TKURE image. The Destination Device checks this decrypted TKURE image.

- If the Check Value is not '0123456789ABCDEFh,' the process shall be aborted.
- If the Trigger bit is '11b,' the process shall be aborted.
- If the Current Move Control Information is equal to '00b,' the process shall be aborted.

(4) Update the temporary TKURMG and TKURMMG image.

The Destination Device securely overwrites the TKURE in the temporary TKURMG image with "the value for delete (random number)."

The Destination Device shall set the TKURE Used flag associated with the TKURE in the temporary TKURMG image to '0b.'

In addition, the Destination Device checks all the TKURE Used flags in the temporary TKURMG image.

(a) When all the TKURE Used flags are equal to '0b,' the Destination Device deletes the selected TKURMG file from the Protected Area of the SD Memory Card. Then go to step (6).

(b) When all the TKURE Used flags other than the one associated with the overwritten TKURE are equal to '1b,' the Destination Device securely reads the TKURMMG file from the SD Memory Card using Secure Read Process and holds it as the temporary TKURMMG image. Then the Destination Device sets the ***n***th TKURMG Used flag in the temporary TKURMMG image to '0b.'

(5) Write the updated temporary TKURMG and TKURMMG image to the SD Memory Card.

The Destination Device securely writes the updated temporary TKURMG image as the updated TKURMG file to the SD Memory Card using the Secure Write Process. Then the Destination Device securely reads the updated TKURMG file from the SD Memory Card using the Secure Read Process and verifies that the value of the ***m***th TKURE in the TKURMG file is equal to "the value for delete (random number)" used in step (4). If the verification of the TKURMG file fails, the Destination Device shall abort this process.

In addition, if the temporary TKURMMG image was updated in step (4b), the Destination Device securely writes the updated temporary TKURMMG image as the updated TKURMMG file to the SD Memory Card using the Secure Write Process.

(6) Update the Usage Rules on the Destination Device.

The Destination Device temporarily holds the decrypted TKURE image as the associated Title Key and Usage Rules for the moved content on the Destination Device.

- When the Current Move Control Information in the decrypted TKURE image is equal to '01b,' the Destination Device sets the value of the Current Move Control Information field to '00b.'

When all of the above steps are executed successfully, the Destination Device securely holds the Title Key and Usage Rules as the associated Title Key and Usage Rules for the moved content.

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

The Source Device securely holds information associated with SD-Video content to be moved. The information includes the Usage Rules and a secret unpredictable Title Key. When the following steps are executed, if necessary, the Source Device appropriately converts the Usage Rules securely held in it into the Usage Rules specified by this specification (e.g. Current Move Control Information).

(1) Check the Usage Rules on the Source Device.

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

- If the Current Move Control Information is equal to '00b,' then the process shall be aborted.
- When there is an indication that Analog Sunset in accordance with the CPRM/CPPM License Agreement is required, the AST shall be set to 1b.

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

The Source Device securely reads the TKURMMG file from the SD Memory Card using the Secure Read Process and holds it as the temporary TKURMMG image.

(3) Read or create a TKURMG.

(3.1) Select a TKURMG file that has at least one unused TKURE.

The Source Device checks the TKURMG Used flag (TKURMG_USED) field of the temporary TKURMMG image. The Source Device selects the first TKURMG file whose TKURMG Used flag is equal to '0b.' If all the TKURMG Used flags are equal to '1b,' the process shall be aborted.

(3.2) Read the selected TKURMG file from the SD Memory Card or create a temporary TKURMG image on the Source Device.

The Source Device checks whether the selected TKURMG file exists or not.

(a) When the selected TKURMG exists, the Source Device securely reads the selected TKURMG file from the SD Memory Card using the Secure Read Process and holds it as the temporary TKURMG image.

(b) When the selected TKURMG does not exist, the Source Device creates a new TKURMG image on the Source Device.

(4) Update the temporary TKURMG and TKURMMG image.(4.1) Update the TKURE in the temporary TKURMG image.

The source device checks the TKURE Used flag (TKURE_USED) in the temporary TKURMG image, and finds the first unused TKURE.

The Source Device updates the unused TKURE in the temporary TKURMG image as follows:

- The Copy Count Control Information of the TKURE is set to the same value as that of the Copy Count Control Information of the Usage Rules held in the Source Device.
- The Initial Move Control Information field of the TKURE is set to the same value as that of the Initial Move Control Information field of the Usage Rules held in the Source Device. The Current Move Control Information field of the TKURE is set to the same value as that of the Current Move Control Information field of the Usage Rules held in the Source Device.
- The CCIFlags field of the TKURE is set to the same value as that of the CCIFlags field of the Usage Rules held in the Source Device.
- Each field in the Initial Field Group of the TKURE is set to the same value as that of each corresponding field in the Initial Field Group of the Usage Rules held in the Source Device.
- Each field in the Current Field Group of the TKURE is set to the same value as that of each corresponding field in the Current Field Group of the Usage Rules held in the Source Device.

- Each field in the Fixed Field Group of the TKURE is set to the same value as that of each corresponding field in the Fixed Field Group of the Usage Rules held in the Source Device.
- The Trigger bit of the TKURE is set to '0Xb.' or '10b' as appropriate.
- The Check Value of the TKURE is set to '0123456789ABCDEFh.'

After all the fields in the unused TKURE are set as above, the Source Device encrypts the TKURE in the temporary TKURMG image using the TKURE Encryption process.

(4.2) Set the TKURE_USED in the temporary TKURMG image and the TKURMG_USED in the temporary TKURMMG image.

The Source Device sets the TKURE Used flag associated with the updated TKURE in the temporary TKURMG image to '1b.'

In addition, when all the TKURE Used flags are equal to '1b' (all the TKUREs in the temporary TKURMG image have been used), the TKURMG Used flag associated with the selected TKURMG file in the temporary TKURMMG image shall be set to '1b.'

(5) Make the original content held in the Source Device unusable.

The Source Device makes the original SD-Video content held in it permanently unusable.

(6) Write the updated temporary TKURMG image and the TKURMMG image to the SD Memory Card.

The Source Device securely writes the updated temporary TKURMG image held in the Source Device as the updated TKURMG file to the SD Memory Card using the Secure Write Process. When a new TKURMG image was created in step (3.2), the updated temporary TKURMG image is written as a new TKURMG file using the Secure Write Process.

In addition, if the TKURMMG image was updated in step (4.2), the Source Device securely writes the updated temporary TKURMMG image held in the Source Device as the updated TKURMMG file to the SD Memory Card using the Secure Write Process.

To protect against the "Pull Card Attack," the Source Device must assume that the Move Process II has been completely done, even if errors occur in step (6).

3.8.7 Playback Process

This section describes the playback process taking into account a) if the Playback Device supports date and time-based usage rules and b) if the content to be played has date and time-based usage conditions. A Playback Device that does not support date and time-based usage rules shall deny playback of content with such usage rules.

In the case of playback the content without date and time-based usage rules, steps (8) , (9) and (12) are skipped.

(1) Determine the TKURMG file and TKURE associated with the content to be played back.

(1.1) Obtain TKURE_SRN.

The Playback Device obtains the TKURE_SRN ***s*** associated with the content to be played back.

(1.2) Determine the TKURMG file and TKURE associated with the content to be played back.

The Playback Device determines the TKURMG filename and the TKURE using the following formula:

$\boldsymbol{s} = (\boldsymbol{n} - 1) * 250 + \boldsymbol{m}$ (***n***: TKURMG file number, ***m***: TKURE number in a TKURMG)

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

For example, when the TKURE_SRN is 1010, the TKURE shall be in the fifth TKURMG file ("MO005.KEY" in the case of TKURE for MOs) and the TKURE shall be tenth entry in the file. But

the TKURE for Programs shall be always in the first TKURMG file ("VIDEO001.KEY") because TKURE_SRN for Programs is less than or equal to 99.

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

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

Then, the Playback Device checks the ***m***th TKURE Used flag in the temporary TKURMG image. If it is equal to '0b,' the process shall be aborted.

Otherwise, the Playback Device obtains the ***m***th TKURE in the temporary TKURMG image.

(3) Check the TKURE (Phase I).

The Playback Device decrypts the TKURE using the TKURE Decryption process and securely holds it as the decrypted TKURE image. The Playback Device checks the decrypted TKURE image.

- If the Check Value is not '0123456789ABCDEFh,' then the process shall be aborted.
- If the Trigger bit fields are '11b,' playback is not allowed, hence 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 (11) .That is, any Playback Device shall ignore date and time-based rules and proceed to playback content
- If the Playback Device does not support date and time-based usage rules, the process shall be aborted.
- If the Current Playback Counter is equal to '0000h,' then the process shall be aborted.
- If the Analog Sunset Token is equal to '1b,' Analog Sunset shall be applied to the Decrypted CPRM Video Content in accordance with the CPRM/CPPM License Agreement.

The Playback Device checks the Validity of Current Start Date field, the Validity of Current 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 (7).

(4) Obtain current date and time.

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

(5) Update the decrypted TKURE image.

The Playback Device checks the Current First Playback Flag field and the Validity of Span field. When the Current First Playback Flag field is equal to '1b' or the Validity of Span field is equal to '0b,' go to step (6).

(5.1) Update the Current Start Date of Playback Period.

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

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

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

(5.2) Update the Current End Date of Playback Period.

a) When the Validity of Current 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 Current End Date of Playback Period field of the decrypted TKURE image to the calculated end date and time, and sets the Validity of Current End Date field to '1b.'

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

- If the current date and time does not precede the Current End Date of Playback Period, then the process shall be aborted.
- If the current date and time precedes the Current 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 Current End Date of Playback Period field of the decrypted TKURE image, the Playback Device sets the Current End Date of Playback Period field of the decrypted TKURE image to the calculated end date and time.

(5.3) The Playback Device sets the Current First Playback Flag field to '1b.' Then go to step (7).

(6) Check the TKURE (Phase 2).

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

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

(7) Decrement the Current Playback Counter.

If the Current Playback Counter of the decrypted TKURE image is not equal to 'FFFFh,' the Playback Device decrements the value of the Current Playback Counter.

(8) Calculate Reference Timestamp.

The Playback Device must perform the following steps:

- If there is no \SD_VIDEO\TBUR.TS file, this process shall be aborted.
- Read the timestamp file in the SD_VIDEO 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, read the timestamp file in the Root directory, and set the reference time to the later of the two timestamp. If there is no timestamp in the Root directory, the Playback Device shall set the reference time to the timestamp in the SD_VIDEO directory.

(9) Update Timestamp.

- Read 'In-Use' flag and ETC counter from the \SD_VIDEO\TBUR.TS file.
- If 'In-Use' = '0b,' ETC = '0h,' and the reference time is in the past, write the current time to both timestamp files, with 'In-Use = '1b' and ETC = '0h.' Go to step (10).
- If the reference time is in the future and any of the following conditions below hold, the 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, write the current time to both timestamp files, with In-Use = '1b, and ETC unchanged.
- If In-Use = '0b,' '0h' < ETC < '5h' and the reference time is in the future,

- If the content is active set In-Use = ‘1b,’ leave ETC unchanged and write the reference time to both TBUR.TS files.
- 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, reset counter, ETC = ‘0h,’ and write the current time to both TBUR.TS files. 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, leave In-Use flag unchanged, and write the later of the reference time and the current time plus the duration of the movie. It is recommended that the device display 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.

(10) Write the temporary TKURMG image to the SD Memory Card.

If the decrypted TKURE image has not been updated either in step (5) or (7), then go to step (11).

The Playback Device encrypts this decrypted TKURE image using the TKURE Encryption process, and sets the ***m***th TKURE in the temporary TKURMG image to the resulting value.

The Playback Device securely writes the updated temporary TKURMG image as the updated TKURMG file to the SD Memory Card using the Secure Write Process. Then the Playback device securely reads the updated TKURMG file from the SD Memory Card using the Secure Read Process and verifies that the update of the ***m***th TKURE in the TKURMG file has completed successfully.

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

(11) Start Playback

The Playback Device starts to play the SD-Video content.

(12) 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_VIDEO 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, read the timestamp file in the Root directory, and set the reference time to the later of the two timestamp. If there is no timestamp in the Root directory set the reference time to the timestamp in the SD_VIDEO directory.
- Read ‘In-Use’ flag and ETC from the file in the SD_VIDEO directory.
- If the reference time is in the past, write both timestamp files with the current time, In-Use = ‘0b’ and ETC =’0h.’ If the reference time is in the future, write the reference time to both timestamp files with In-Use = ‘0b’ and ETC unchanged.

3.9 MKB Extensions for SD-Video

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

The directory name in which the MKB Extension file is located is "SD_VIDEO," and the name of the MKB Extension file is "SD_VIDEO.MKB."