Content Protection for Recordable Media Specification

SD Memory Card Book
SD-Binding Part

Intel Corporation

International Business Machines Corporation

Matsushita Electric Industrial Co., Ltd.

Toshiba Corporation

Revision 0.92

December 8, 2005

This page is intentionally left blank.

Preface

Notice

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

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

Intellectual Property

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

Contact Information

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

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

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

This page is intentionally left blank.

Table of Contents

List of Figures

This page is intentionally left blank.

List of Tables

This page is intentionally left blank.

Chapter 1
Introduction

1. Introduction

1.1 Purpose and Scope

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

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

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

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

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

1.2 Document Organization

This specification is organized as follows:

- Chapter 1 provides an introduction.
- Chapter 2 lists abbreviations and acronyms used in this document.
- Chapter 3 describes the use of CPRM to protect SD-Binding 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 for SD-Binding license agreement*

4C Entity, LLC, *CPRM Specification: Introduction and Common Cryptographic Elements, Revision 1.0*

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

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

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

SD Association, *SD Memory Card Specifications, Part 13: Binding Specifications, Version 1.01*

1.4 Notation

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

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

Chapter 2
Abbreviations and Acronyms

2. Abbreviations and Acronyms

The following abbreviations and acronyms are used in this document:

4C	4 Companies (IBM, Intel, MEI, and Toshiba)
AKE	Authentication and Key Exchange
C-CBC	Converted Cipher Block Chaining
C2	Cryptomeria Cipher
CCI	Copy Control Information
CPRM	Content Protection for Recordable Media
ID	Identifier
LLC	Limited Liability Company
MKB	Media Key Block
SD	Secure Digital
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
UR	Usage Rules

Chapter 3
CPRM for SD-Binding

3. CPRM for SD-Binding

3.1 Introduction

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

The SD-Binding 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 1.3). 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-Binding content, the "MKB for SD-Binding" is used. The MKB number for SD-Binding 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-Binding 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 Device Unique Key, which is generated by a Media Unique Key and a Bind ID. Usually, the Bind ID is unique for each set or each user. Note that the CPRM license may include additional requirements regarding the Bind ID. The encryption process of the Title Key and Usage Rules is described in Section 3.11.3 of *SD Memory Card Book Common Part*. 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.

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 four kinds of information:

- "Move Control Information": Usage Rule for controlling the Move operation.
- "Copy Count Control Information": Usage Rule for controlling the Copy operation.
- "Service Defined Area": Any information defined by services or applications. Service providers and device manufacturers who use this area are responsible for defining the format of this area, defining how compliance devices shall behave with respect to this information.
- "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, and detecting whether the device can play back the encrypted content 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-Binding 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~~Figure 3-1~~ illustrates the process for SD-Binding content encryption and decryption on "SD Memory Card."

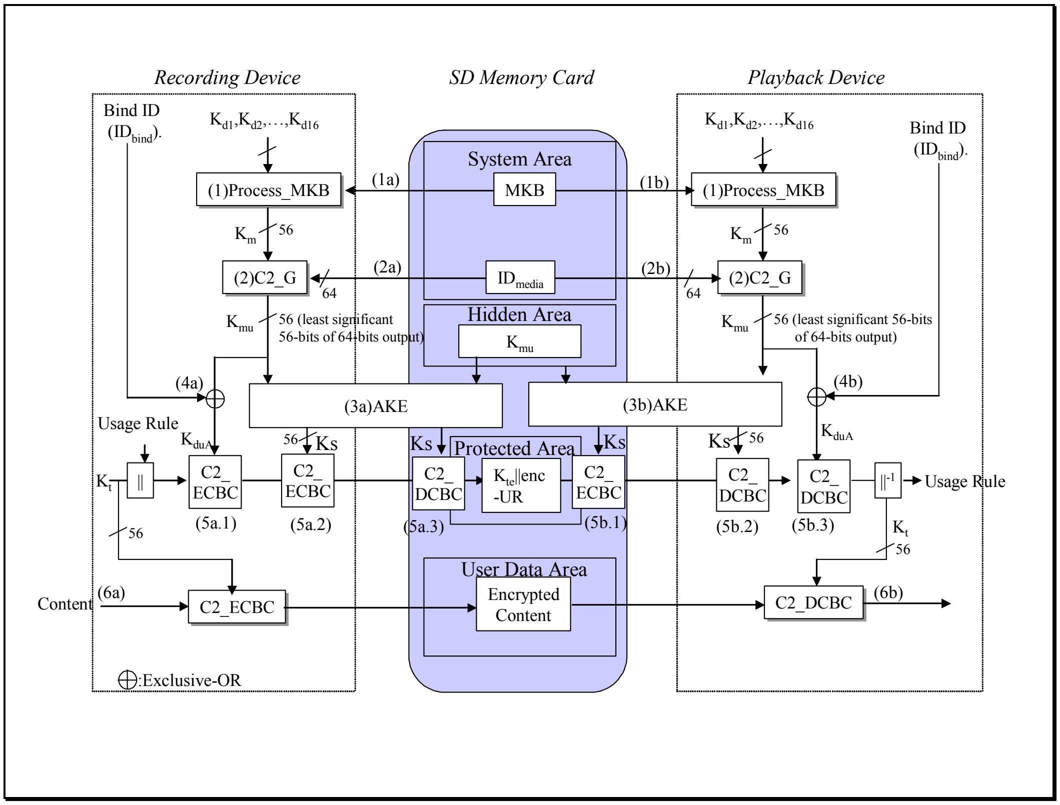

Figure 3-1 Content Encryption and Decryption on SD Memory Card

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.

-(4) Device Unique Key Generation process

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

Device Unique Key (K_{du}) = Media Unique Key (K_{mu}) ⊕ Bind ID (ID_{bind})

-(5a) Title Key and Usage Rule Encryption process.

The following steps (5a.1) through (5a.3) describe the Title Key and Usage Rule Encryption Process.

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

(5a.1) Encrypt the Title Key and Usage Rule Entry by the Device Unique Key.

The Recording Device encrypts the Title Key and Usage Rule Entry, (see Table 3-10~~Table 3-10~~), as a single 64-byte encryption frame using the Device Unique Key. 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.

(5a.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.

(5a.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.

-(5b) Title Key and Usage Rule Decryption process.

The following steps (5b.1) through (5b.3) describe the Title Key and Usage Rule Decryption Process.

(5b.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 Device.

(5b.2) Decrypt the Title Key and Usage Rule Entry by the Session Key.

The 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.

(5b.3) Decrypt the Title Key and Usage Rule Entry by the Device Unique Key.

The Device decrypts the 64-byte Title Key and Usage Rule Entry using the Device Unique Key using C2_DCBC. Then the Device gets the decrypted Title Key and Usage Rules.

-(6a) Content Encryption process

As for the content encryption process, the same procedures defined in Section 3.4 (6a) of *SD Memory Card Book Common Part* are used.

-(6b) Content Decryption process

As for the content decryption process, the same procedures defined in Section 3.4 (6b) 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-Binding Object Encryption

Each SD-Binding object is encrypted using a Title Key as follows:

- The encrypted SD-Binding object file (variable size N=1, …, 2^{31}-1) consists of one optional unencrypted header and multiple encryption blocks.
- The size X of each encryption block other than last encryption block is calculated by the following formula referring to the Encryption Block Size Factor E.

  $X=64*2^{E}$ (bytes), E=0, …, 5

  The size of the last encryption block is equal to X or less.
- The Encryption Block Size Factor (E) is specified in the corresponding Title Key & Usage Rule Entry of the encrypted object file.
- Each encryption block of an SD-Binding object file is encrypted by the Title Key.
- Each encryption block starts a new C-CBC mode cipher chain.
- If the size of an SD-Binding object file is less than or equal to X, the entire object file is encrypted using a single C-CBC mode cipher chain.
- The last encryption block is encrypted as follows:

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

  -If the object file is 7 bytes or less (N=1, …, 7), no encryption is performed
- If the header part exists, the Unencrypted Header Size Factor H of the optional unencrypted header shall be specified in the corresponding Title Key & Usage Rule Entry of the encrypted object file and shall be used to decrypt the encrypted SD-Binding object file. The size Y of the optional unencrypted header is calculated by the following formula:

  $Y= 64*2^{(H-1)}$ (bytes), H=1, …, 13

  When H=0, the corresponding object file does not have an unencrypted header.
- The equivalent information of the size Y may be specified in any file in the User Data Area. The file name and format can be dependent on each service.

Table 3-1~~Table 3-1~~ through Table 3-4~~Table 3-4~~ shows the encrypted SD-Binding object file without the optional unencrypted header. While Table 3-5~~Table 3-5~~ trough Table 3-7~~Table 3-7~~ shows the encrypted SD-Binding object file with the optional unencrypted header.

Table 3-1 Encrypted object file without residual encryption block (N=X*n)

Bit Byte	7	6	5	4	3	2	1	0
0	Encryption Block (Encrypted by C2-ECBC)							
1								
:								
X-1								
X	Encryption Block (Encrypted by C2-ECBC)							
X+1								
:								
2X-1								
	:							
	:							

X*(n-1)	Encryption Block (Encrypted by C2-ECBC)							
X*(n-1)+1								
:								
nX-1								

Table 3-2 Encrypted object file with residual encryption block (N=X*n+m, m<X, m=8*p)

Bit Byte	7	6	5	4	3	2	1	0
0	Encryption Block (Encrypted by C2-ECBC)							
1								
:								
X-1								
X	Encryption Block (Encrypted by C2-ECBC)							
X+1								
:								
2X-1								
	:							
	:							
nX	Encryption Block (Encrypted by C2-ECBC)							
nX+1								
:								
nX+m-1								

Table 3-3 Encrypted object file with residual data block (N=X*n+m+q, m<X, m=8*p, q<8)

Bit Byte	7	6	5	4	3	2	1	0
0	Encryption Block (Encrypted by C2-ECBC)							
1								
:								
X-1								
X	Encryption Block (Encrypted by C2-ECBC)							
X+1								
:								
2X-1								
	:							
	:							

nX	Encryption Block (Encrypted by C2-ECBC)
nX+1	
nX+m-1	
nX+m	Non-Encrypted
nX+m+1	
:	
nX+m+q-1	

Table 3-4 Object file less than 8 bytes (N<8)

Bit Byte	7	6	5	4	3	2	1	0
0	Non-Encrypted							
1								
:								
N								

Table 3-5 Encrypted object file (with unencrypted header) without residual encryption block (N=X*n)

Bit Byte	7	6	5	4	3	2	1	0
0	Non-Encrypted							
1								
:								
Y-1								
Y	Encryption Block (Encrypted by C2-ECBC)							
Y+1								
:								
Y+X-1								
Y+X	Encryption Block (Encrypted by C2-ECBC)							
Y+X+1								
:								
Y+2X-1								
	: :							
Y+X*(n-1)	Encryption Block (Encrypted by C2-ECBC)							
Y+X*(n-1)+1								
:								
Y+nX-1								

Table 3-6 Encrypted object file (with unencrypted header) with residual encryption block (N=X*n+m, m<X, m=8*p)

Bit Byte	7	6	5	4	3	2	1	0
0	Non-Encrypted							
1								
:								
Y-1								
Y	Encryption Block (Encrypted by C2-ECBC)							
Y+1								
:								
Y+X-1								
Y+X	Encryption Block (Encrypted by C2-ECBC)							
Y+X+1								
:								
Y+2X-1								
	: :							
Y+nX	Encryption Block (Encrypted by C2-ECBC)							
Y+nX+1								
:								
Y+nX+m-1								

Table 3-7 Encrypted object file (with unencrypted header) with residual data block (N=X*n+m+q, m<X, m=8*p, q<8)

Bit Byte	7	6	5	4	3	2	1	0
0	Non-Encrypted							
1								
:								
Y-1								
Y	Encryption Block (Encrypted by C2-ECBC)							
Y+1								
:								
Y+X-1								
Y+X	Encryption Block (Encrypted by C2-ECBC)							
Y+X+1								
:								
Y+2X-1								

	: :
Y+nX	Encryption Block (Encrypted by C2-ECBC)
Y+nX+1	
Y+nX+m-1	
Y+nX+m	Non-Encrypted
Y+nX+m+1	
:	
Y+nX+m+q-1	

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-Binding

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

3.7.1.1 Title Key & Usage Rule Master Manager (TKURMMG)

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

3.7.1.2 Title Key & Usage Rule Manager (TKURMG)

The Title Key and the Usage Rules for SD-Binding content are encrypted by a Device Unique Key, which is generated by a Media Unique Key and a Bind ID. Usually, the Bind ID is unique for each set or each user. The Encrypted Title Key and Usage Rules are stored as a file of the Protected Area. The file is called Title Key & Usage Rule Manager (TKURMG) file. In the Protected Area, there can be plurality of TKURMG files.

3.7.1.3 Directory and File Configuration in Protected Area

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

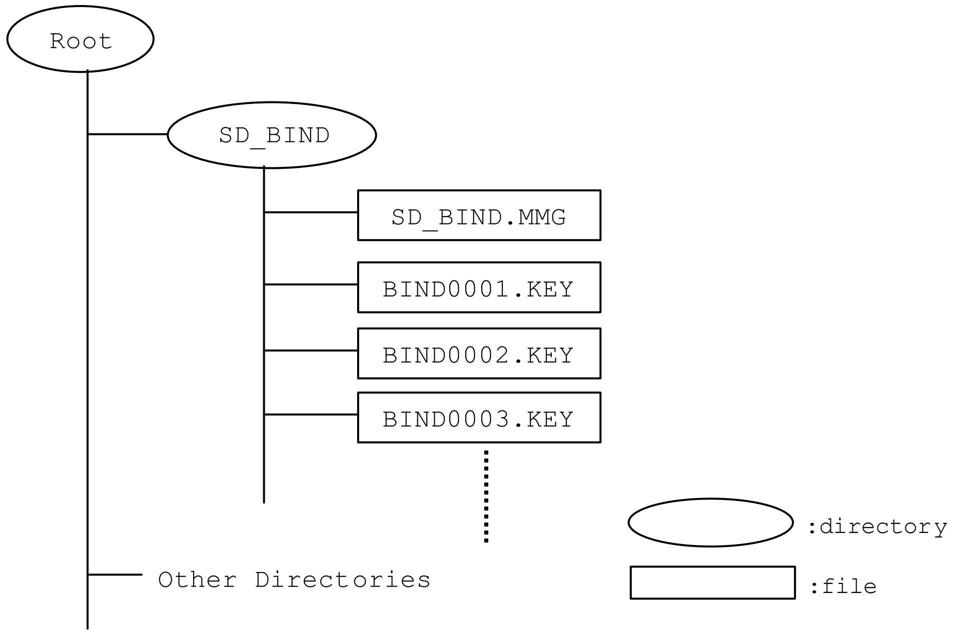

Figure 3-2 Directory and File Configuration

- The name of the TKURMMG file shall be "SD_BIND.MMG."

- The size of a TKURMG file is fixed. It contains 250 Title Key & Usage Rule Entries (TKUREs).

- There can be at most 256 TKURMG files in the SD_BIND directory of the Protected Area.

- The name of a TKURMG file shall be:

  BINDxxxx.KEY,

  where xxxx is a serial number (0001, …, 0256) assigned to each of the TKURMG files in the SD_BIND directory.

- The TKURE Search Number (TKURE_SRN) is a serial number uniquely associated with each TKURE of all the TKURMG files in SD_BIND directory. The directory contains at most 256 TKURMG files, each of which has 250 TKUREs, and the maximum number of TKURE_SRN is 64,000(250 x 256)[1]. For example, TKURE #1 through TKURE #250 in the BIND0001.KEY file are associated with TKURE_SRN 1 through 250, TKURE #1 through TKURE #250 in the BIND0002.KEY file are associated with TKURE_SRN 251 through 500, and so forth.

- Each encrypted content file in the User Data Area is associated with the corresponding TKURE in the Protected Area through its TKURE_SRN.

- The TKURE_SRN of the corresponding TKURE is stored in the Title Key Information (TKI) of the Title Key Manager file (TKMG) in the User Data Area. Regarding the structure and the file names in the User Data Area, refer to *SD Memory Card Specifications, Part 13: Binding Specifications*.

[1] Note that *SD Memory Card Specifications, Part 13: Binding Specifications V1.0* has described that maximum number of TKURE_SRN is 4,194,304,000 which is no longer a valid number. It shall be corrected on later version of *SD Memory Card Specifications, Part 13: Binding Specifications.*

- If a content file in the User Data Area is not encrypted, the TKURE_SRN field in the corresponding TKI shall be set to 0. Otherwise, the TKURE_SRN field has TKURE_SRN, which shall be unique in the SD_BIND directory.

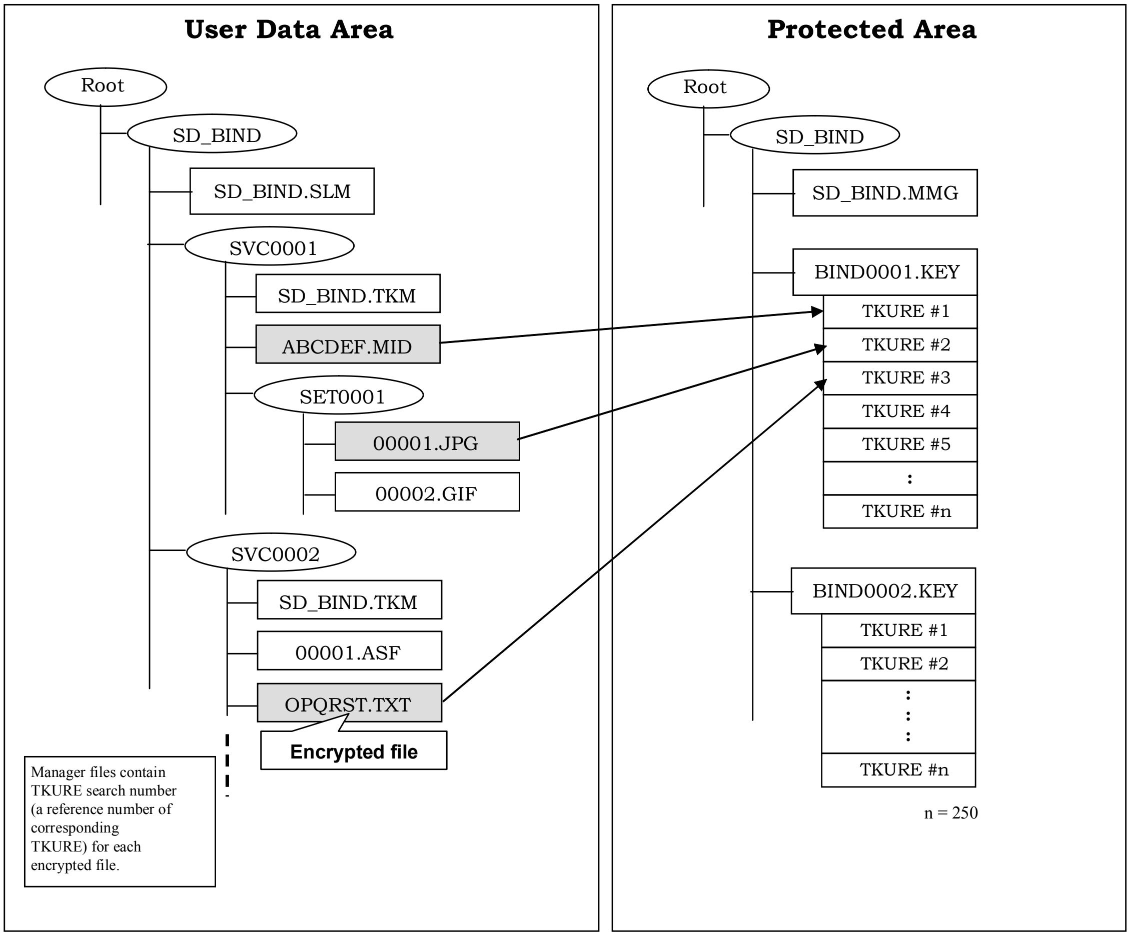

Figure 3-3 Relationship between Directory and Filename

3.7.2 Structure of Title Key & Usage Rule Master Manager

As shown in Table 3-8~~Table 3-8~~, the TKURMMG consists of Version number, Application ID of TKURMG, and Used flag of each TKURMG.

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 63	TKURMG_USED	TKURMG Used flag	32 bytes
Total			64 bytes

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

(RBP 0 to 1) VERN

This field describes the Version number of the SD-Binding specification.

b15	b14	b13	b12	b11	b10	b9	b8
Reserved							

b7	b6	b5	b4	b3	b2	b1	b0
Book part version							

Book part version ... 10h : version 1.0

Others : reserved

(RBP 2 to 3) TKURMG_AP_ID

This field describes the Application ID of TKURMG. This value must be '10'.

b15	b14	b13	b12	b11	b10	b9	b8
Reserved							

b7	b6	b5	b4	b3	b2	b1	b0
Application ID							

Application ID ... 0Ah : SD-Binding

(RBP 32 to 63) TKURMG_USED

This field describes whether each TKURMG has unused TKUREs or not. Notwithstanding bit ordering in Section 1.4, bit positions within TKURMG Used flag are numbered such that the most significant bit is numbered 0 and the least significant bit is numbered 255. Therefore, for example, TKURMG Used flag[0] is stored at b255.

b255	b254	b253	b252	b251	b250	b249	b248
TKURMG Used flag [0 .. 7]							

:

:

b7	b6	b5	b4	b3	b2	b1	b0
TKURMG Used flag [248 .. 255]							

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

0b: Either "BIND*j* .KEY" does not exist, or
"BIND*j* .KEY" exists and has some unused TKUREs.

3.7.3 Structure of Title Key & Usage Rule Manager

Figure 3-4~~Figure 3-4~~ shows the structure of a Title Key & Usage Rule Manager (TKURMG).

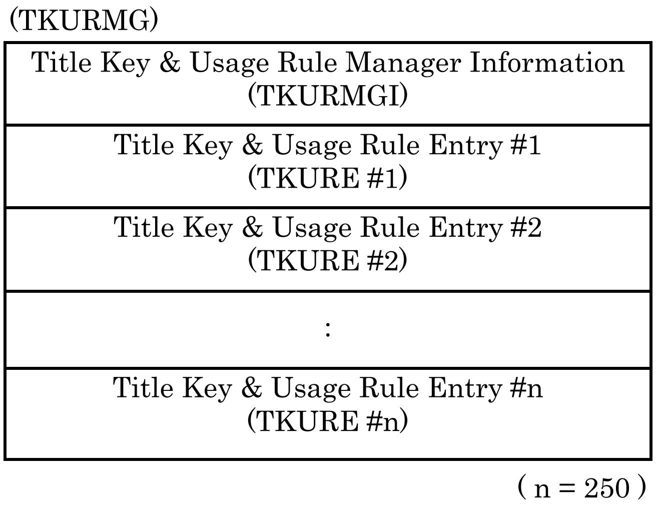
(TKURMG)
Title Key & Usage Rule Manager Information (TKURMGI)
Title Key & Usage Rule Entry #1 (TKURE #1)
Title Key & Usage Rule Entry #2 (TKURE #2)
:
Title Key & Usage Rule Entry #n (TKURE #n)
(n = 250)

Figure 3-4 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.

3.7.4 Title Key & Usage Rule Manager Information (TKURMGI)

As shown in Table 3-9~~Table 3-9~~, the TKURMGI consists of Used flag of each TKURE in the TKURMG.

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. Notwithstanding bit ordering in Section 1.4, bit positions within TKURE Used flag are numbered such that the most significant bit is numbered 0 and the least significant bit is numbered 249. Therefore, for example, TKURE Used flag[0] is stored at b255.

b255	b254	b253	b252	b251	b250	b249	b248
TKURE Used flag [0 .. 7]							

:

:

b7	b6	b5	b4	b3	b2	b1	b0
TKURE Used flag [248 .. 249]		Reserved					

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.)

3.7.5 Title Key & Usage Rule Entry (TKURE)

As shown in Table 3-10~~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 3-11~~Table 3-11~~, 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

b63	b62	b61	b60	b59	b58	b57	b56
Reserved							
b55	b54	b53	b52	b51	b50	b49	b48
EKEY [55 .. 48]							
b47	b46	b45	b44	b43	b42	b41	b40
EKEY [47 .. 40]							
b39	b38	b37	b36	b35	b34	b33	b32
EKEY [39 .. 32]							
b31	b30	b29	b28	b27	b26	b25	b24
EKEY [31 .. 24]							
b23	b22	b21	b20	b19	b18	b17	b16
EKEY [23 .. 16]							
b15	b14	b13	b12	b11	b10	b9	b8

EKEY [15 .. 8]							
b7	b6	b5	b4	b3	b2	b1	b0
EKEY [7 .. 0]							

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 fields.

3.7.5.2 Usage Rules (UR)

As shown in Table 3-12~~Table 3-12~~, Usage Rules (UR) consists of Trigger Bit Information, Encryption Block Size Factor, Initial Move Control Information, Current Move Control Information, Copy Count Control Information, Unencrypted Header Size Factor, Service Defined Area, and Check Value.

Table 3-12 UR

(Description order)

RBP	Field Name	Contents	Number of bytes
0	UR_TRIGGER	Trigger Bit Information / Encryption Block Size Factor	1 byte
1	UR_MCCNTRL	Initial Move Control Information / Current Move Control Information / Copy Count Control Information	1 byte
2 to 14	Reserved	Reserved	13 bytes
15	HDRSZ_FACTOR	Unencrypted Header Size Factor	1 byte
16 to 47	SV_AREA	Service Defined Area	32 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, and Encryption Block Size Factor.

b7	b6	b5	b4	b3	b2	b1	b0
Trigger bit	reserved		Encryption Block Size Factor				

Trigger bit ... 0b : Accessing devices conforming to this specification can control the Move/Copy/Playback processes.

1b : 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 ‘0b’ 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 this bit is set to ‘1b.’

Encryption Block Size Factor ... This field describes the Encryption Block Size Factor (E) of corresponding content file.

0,…,15: The Encryption Block Size Factor E.

The encryption block size X is calculated by following formula:

$$X = 64 * 2^E \text{ (bytes)}$$

11111b: The entire content file is encrypted using a single C-CBC chain

(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.

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.

(RBP 15) HDRSZ_FACTOR

This field describes the Unencrypted Header Size Factor of the corresponding content file.

b7	b6	b5	b4	b3	b2	b1	b0
Reserved				Unencrypted Header Size Factor			

Unencrypted Header Size Factor ... 0: The corresponding file do not have unencrypted header.

1,…,13: The Unencrypted Header Size Factor H.

The unencrypted header size Y is calculated by following formula:

$$Y=64*2^{(H-1)} \text{ (bytes)}$$

others: Reserved.

(RBP 16 to 47) SV_AREA

This field stores any information that will be defined by particular services or applications. This specification does not define the format of this field. Each service that uses this field has to define the strict behavior of compliance devices.

(RBP 48 to 55) UR_CHECK

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

3.8 Process Description

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

- Recording Process

  Specifies how a Recording Device writes CPRM protected SD-Binding content to an SD Memory Card.

- Erasing Process

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

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

  Specifies how CPRM protected SD-Binding 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-Binding 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-Binding 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-Binding 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-Binding 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 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 (5a.1)) of this specification.
- 'TKURE Decryption Process (Title Key & Usage Rule Decryption Process)' is described in Section 3.4 (step (5b.3)) of this specification.

3.8.1 Recording Process

The Recording Device securely holds information associated with SD-Binding 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). It also includes the Encryption Block Size Factor and the Unencrypted Header Size Factor that has any valid value (e.g. specified by the content provider or chosen by the Recording Device).

(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 of the TKURE are set to the value specified by the Content Provider.
- 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 ‘0b.’
- The Encryption Block Size Factor and the Unencrypted Header Size Factor are set to the value held in the Recording Device.
- 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.

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:

$\boldsymbol{s} = (\boldsymbol{n} - 1) * 250 + \boldsymbol{m}$ ($\boldsymbol{n}$: TKURMG file number, $\boldsymbol{m}$: 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 TKURMG filename shall be “BIND0005.KEY” (the fifth TKURMG file) and the TKURE shall be the tenth entry in the “BIND0005.KEY.”

(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.

(3a) 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.

(3b) 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:

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

$1 \le \boldsymbol{m} \le 250, \quad 1 \le \boldsymbol{n} \le 256$

For example, when the TKURE_SRN is 1010, the TKURMG filename shall be “BIND0005.KEY” (the fifth TKURMG file) and the TKURE shall be the tenth entry in the “BIND0005.KEY.”

(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 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 ‘1b,’ the process shall be aborted.
- 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:

- 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.

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. The content that is copied from SD Memory Card to the Destination Device shall still be bound to the associated Bind.

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

The Source Device securely holds information associated with SD-Binding content to be copied. The information includes the Usage Rules and a secret unpredictable Title Key. It also includes the Encryption Block Size Factor and the Unencrypted Header Size Factor that has any valid value (e.g. already included in the Usage Rules or chosen by the Source Device).

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

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

- If the Copy Count Control Information is equal to ‘0000b,’ then 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:

- 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 Trigger bit of the TKURE is set to '0b.'
- The Encryption Block Size Factor and the Unencrypted Header Size Factor of the TKURE are set to the value held in the Source Device.
- 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).

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:

$\boldsymbol{s} = (\boldsymbol{n} - 1) * 250 + \boldsymbol{m}$ (***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 TKURMG filename shall be "BIND0005.KEY" (the fifth TKURMG file) and the TKURE shall be the tenth entry in the "BIND0005.KEY."

(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 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 '1b,' 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.

(4a) 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).

(4b) 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. The content that moved from SD Memory Card to the Destination Device shall still be bound to the associated Bind ID.

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

The Source Device securely holds information associated with SD-Binding content to be moved. The information includes the Usage Rules and a secret unpredictable Title Key. It also includes the Encryption Block Size Factor and the Unencrypted Header Size Factor that has any valid value (e.g. already included in the Usage Rules or chosen by the Source Device).

(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.

(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 Trigger bit of the TKURE is set to ‘0b.’
- The Encryption Block Size Factor and the Unencrypted Header Size Factor of the TKURE are set to the value held in the Source Device.
- 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-Binding 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

(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:

$s = (n - 1) * 250 + m$ (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 TKURMG filename shall be “BIND0005.KEY” (the fifth TKURMG file) and the TKURE shall be the tenth entry in the “BIND0005.KEY.”

(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 in the temporary TKURMG image.

The Playback Device decrypts the TKURE using the Title Key and Usage Rule 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 field is ‘1b,’ then the process shall be aborted.

(4) Start Playing back

The Playback Device starts play back the content.

3.9 MKB Extensions for SD-Binding

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

The usage of MKB Extensions for SD-Binding is different from other applications. Each service shall make a choice of 3 alternatives for MKB Extension: (1) Using the MKB Extension file located in the “SD_BIND” directory, (2) Using the MKB Extension file located in the service directory (SVCnnnnn), (3) Not supporting MKB Extensions. Each alternative is described below.

(1) Using the MKB Extension file located in the “SD_BIND” directory

The MKB Extension file is named “SD_BIND.MKB” and shared with all services choosing (1). In a MKB processing, the MKB Extension file in “SD_BIND” is used and the other MKB Extension files are not used. Writing/replacing the MKB Extension file shall be done only when the device can decrypt and re-encrypt all title keys stored in all service directories choosing (1).

(2) Using the MKB Extension file located in the Service Directory (SVCnnnnn)

The MKB Extension file is named “SD_BIND.MKB” and used by the service exclusively. In a MKB processing, the MKB Extension file in the Service Directory is used and the other MKB Extension files are not used. Writing/replacing the MKB Extension file shall be done only when the device can decrypt and re-encrypt all title keys stored in the Service Directory. When the device initially creates “SD_BIND” directory and the Service Directory and writes the MKB Extension file in the Service Directory, the device shall also write the same MKB Extension file in “SD_BIND” directory.

(3) Not supporting MKB Extensions.

In this case, devices ignore all MKB Extension files in an MKB processing.