Content Protection for Recordable Media Specification

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

Intel Corporation

International Business Machines Corporation

Panasonic Corporation

Toshiba Corporation

Revision 0.92

July 19, 2012

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 license from the 4C Entity, LLC. Note that use of this *CPRM for SD Memory Card Book SD-SD (Separate Delivery) eBook Profile Part* book also requires execution of an addendum to the applicable basic 4C license agreement.

Contact Information

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

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

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

This page is intentionally left blank.

Table of Contents

This page is intentionally left blank.

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

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

1.2. Document Organization

This specification is organized as follows:

- Chapter 1 provides an introduction.
- Chapter 2 lists abbreviations and acronyms used in this document.
- Chapter 3 describes the use of CPRM to protect SD-SD eBook content.

1.3. References

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 When the documents are superceded by an approved revision, the revision shall apply.

4C Entity, LLC, *CPRM for eBook Addendum*

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, *CPRM Specification: SD Memory Card Book SD-SD (Separate Delivery) Part, Revision 0.94*

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

SD Association, *SD Memory Card Specifications, Part 15: SD-SD (Separate Delivery) Specification, Version 1.30*

SD Association, *SD Memory Card Specifications, Part 15: eBook Profile Specification, Addendum to SD Specifications Part 15 Separate Delivery Specification, Version 1.10*

The *CPRM Specification SD Memory Card Book Common Part* describes the general CPRM technology for SD Memory Card and all SD applications. The *CPRM Specification: SD Memory Card Book SD-SD (Separate Delivery) Part* describes how to handle SD-SD Keys which are Content Keys and User Keys. This book describes how to protect SD-SD eBook content using SD-SD Keys. Note that CPRM for SD-SD eBook does not support both the Export and the Re-import which are defined in CPRM for SD-SD. Figure 1-1 is the specification structure.

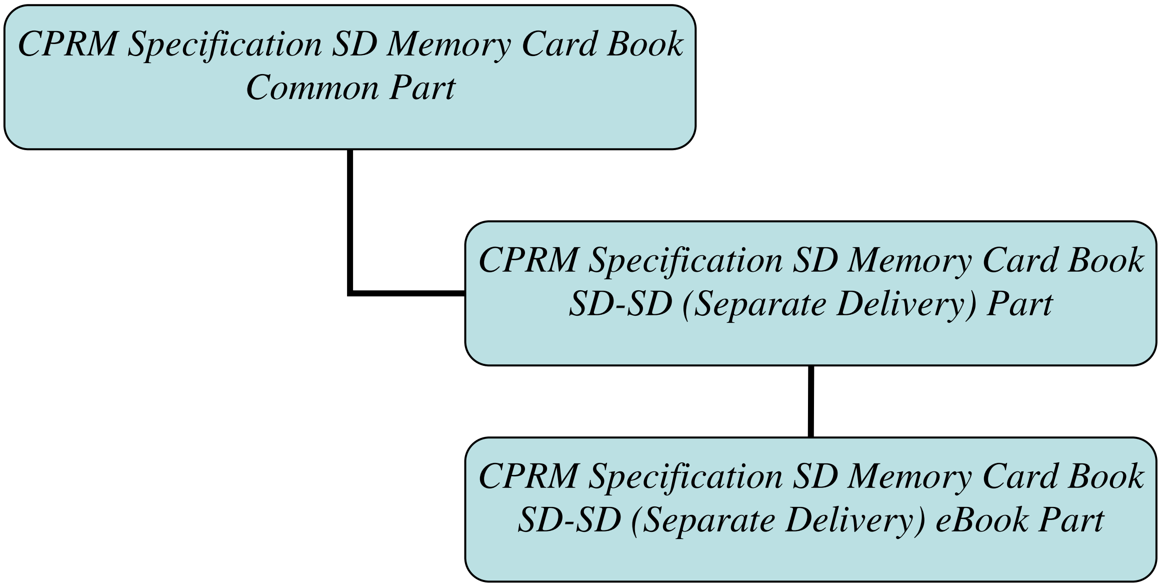
CPRM Specification SD Memory Card Book Common Part
CPRM Specification SD Memory Card Book SD-SD (Separate Delivery) Part
CPRM Specification SD Memory Card Book SD-SD (Separate Delivery) eBook Part

Figure 1-1 Specification structure for SD-SD eBook

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 to the notations and conventions, 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:

AES	Advanced Encryption Standard
AVOP	Analog Video Output Permission
C-CBC	Converted Cipher Block Chaining
C2	Cryptomeria Cipher
CBC	Cipher Block Chaining
CCI	Copy Control Information
CKI	Content Key Information
CKMG	Content Key Manager
CMAC	Cipher-based Message Authentication Code
CPRM	Content Protection for Recordable Media
CTR	Counter
ECKUR	Encrypted Content Key and Usage Rule
ELE	eBook Object Element
ETS	Extended Transport Stream
ExO	Extended Object
ISO	International Organization for Standardization
LLC	Limited Liability Company
MOU	Media Object Unit
SDA	SD Card Association
TOD	Transport Stream Object Data
UDVOP	Unprotected Digital Video Output Permission
UKURE	User Key & Usage Rule Entry
UKURE_SRN	User Key & Usage Rule Entry Search Number
UKURMG	User Key & Usage Rule Manager
UKURMMG	User Key & Usage Rule Master Manager
UR_B	Usage Rules for eBook

This page is intentionally left blank

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

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

3.1. Introduction

This chapter specifies details for using CPRM to protect SD-SD eBook content and describes details on using CPRM to realize some features. Regarding the SD-SD eBook Profile, refer to the *SD Memory Card Specifications – Part15 eBook Profile Specification Addendum to SD Specifications Part 15 Separate Delivery Specifications*.

3.2. Device Requirements

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

3.3. CPRM Components

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

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

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

3.4.1. Usage Rules for eBook

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

As shown in Table 3-1, UR_B consists of UR_B_TRIGGER, UR_B_CURRENT, UR_B_INITIAL, UR_B_PRINT, UR_B_OUTPUT and Reserved field. When content is recorded, Reserved field shall be filled with 00h unless some specific values are provided.

Table 3-1 Usage Rules for eBook

(Description order)

RBP	Field Name	Contents	Number of bytes
0	UR_B_TRIGGER	Trigger Bits for eBook Profile Processes	1 byte
1 to 2	UR_B_CURRENT	Current Fields Group for eBook	2 bytes
3 to 4	UR_B_INITIAL	Initial Fields Group for eBook	2 bytes
5	UR_B_PRINT	Print out control information	1 byte
6	UR_B_OUTPUT	Output control information	1 byte
7 to 9	Reserved	Reserved	3 bytes

Total	10 bytes

(RBP 0) UR_B_TRIGGER

This field describes Trigger Bits for eBook Profile Processes.

<table>
<tr><th>b7</th><th>b6</th><th>b5</th><th>b4</th><th>b3</th><th>b2</th><th>b1</th><th>b0</th></tr>
<tr><td colspan="8">Trigger Bits for eBook Profile Processes</td></tr>
</table>

Trigger Bits for eBook Profile Processes ... These bits control whether or not an execution of process defined in this book is allowed. In a future version of this specification, the Usage Rules may be expanded, or other information for controlling processes may be added. Accessing devices in a future version may recognize a meaning of Trigger Bits for controlling processes correctly when this bit is set to the value except 00000000b. For this revision of this specification, the Trigger Bits for eBook Prolife Processes shall be set only to 00000000b.

00000000b: Accessing devices conforming to this revision of this specification are allowed to execute the processes described in Section 3.6.

00000001b~11111111b: Accessing devices conforming to this revision of this specification shall not do processes described in Section 3.6.

(RBP 1 to 2) UR_B_CURRENT

Current Fields Group for eBook consists of Reserved field only. In the future, a new usage rules may be added.

<table>
<tr><th>b15</th><th>b14</th><th>b13</th><th>b12</th><th>b11</th><th>b10</th><th>b9</th><th>b8</th></tr>
<tr><td colspan="8">Reserved</td></tr>
</table>

<table>
<tr><th>b7</th><th>b6</th><th>b5</th><th>b4</th><th>b3</th><th>b2</th><th>b1</th><th>b0</th></tr>
<tr><td colspan="8">Reserved</td></tr>
</table>

(RBP 3 to 4) UR_B_INITIAL

Initial Fields Group for eBook consists of Reserved field only. In the future, a new usage rules may be added.

<table>
<tr><th>b15</th><th>b14</th><th>b13</th><th>b12</th><th>b11</th><th>b10</th><th>b9</th><th>b8</th></tr>
<tr><td colspan="8">Reserved</td></tr>
</table>

<table>
<tr><th>b7</th><th>b6</th><th>b5</th><th>b4</th><th>b3</th><th>b2</th><th>b1</th><th>b0</th></tr>
<tr><td colspan="8">Reserved</td></tr>
</table>

(RBP 5) UR_B_PRINT

This field consists of Print Out Control flag and reserved field.

b7	b6	b5	b4	b3	b2	b1	b0
Print Out Control	Reserved						

Print Out Control ... 0b: Print Out is not allowed.

1b: Print Out is allowed. Process of Print Out is defined in Section 3.6. Definition of Print Out is described in Compliance Rules of SD-SD eBook contained in the *CPRM for eBook Addendum*.

(RBP 6) UR_B_OUTPUT

This field consists of Analog Video Output Permission (AVOP) flag, Unprotected Digital Video Output Permission (UDVOP) flag and reserved field.

b7	b6	b5	b4	b3	b2	b1	b0
AVOP	UDVOP	Reserved					

Analog Video Output Permission ... 0b: Analog video output is not permitted.

1b: Analog video output is permitted.

Unprotected Digital Video Output Permission ... 0b: Unprotected digital video output is not permitted.

1b: Unprotected digital video output is permitted.

3.4.2. User Key Type

In this SD-SD specification, two types of User Key are defined. The type is called User Key Type and indicates whether or not a device executes the Hash Calculation Process described in the *CPRM Specification SD Memory Card Book SD-SD (Separate Delivery) Part*. When the User Key Type is set to 0b, the hash data of all Content Key Information (CKIs) encrypted with the User Key is stored in the Protected Area. The hash data is always re-calculated when one of the CKIs is changed, a new CKI is added or a CKI is deleted/moved. The devices can detect altering or counterfeiting the CKIs.

On the other hand, when the User Key Type is set to 1b, the hash data of all CKIs is not stored anywhere. Then the hash calculation is not required in processes, however, the CKIs cannot be protected from roll back attack to replace the CKIs in the User Data Area with the CKIs which were stored before. For example, move of CKI or dynamically decreasing copy counter in the usage rules can be altered in this case.

Therefore, in the SD-SD specification, the usage rules of the CKIs related to the User Key whose User Key Type is set to 1b has some restrictions. However, in this revision, there is no restriction in usage rules of the UR_B because of there is no dynamic Usage Rules. In the future, a restriction may be added when a new usage rule is defined.

3.5. Content Encryption Format

The SD-SD eBook specification defines several formats in the *SD Memory Card Specifications, Part 15: eBook Profile Specification, Addendum to SD Specifications Part 15 Separate Delivery Specification*. CPRM can be applied to the Profile Type 1 which is a format for basic electronic book defined in SDA. CPRM for SD-SD eBook supports C2-CPRM and AES-CPRM defined in the *CPRM Specification: Introduction and Common Cryptographic Elements*. In the following section, it is described how to apply CPRM to the SD-SD eBook format.

3.5.1. Encryption for Profile Type 1

In Profile Type 1, SD-SD eBook content contains several components. In those components, an eBook Object Element (ELE) and an eBook Extended Object (ExO) can be encrypted by CPRM. There are several options of encryption mechanism for the ELE and ExO. Each ELE has a header field called Extended Packet Header which contains three fields, ENC_FLG, VERN_PKT and 4C Defined Area. Those fields are defined in *SD Memory Card Specifications, Part 15: eBook Profile Specification, Addendum to SD Specifications Part 15 Separate Delivery Specification*.

The ENC_FLG is 1 bit length field and indicates whether or not the payload is encrypted. When the ENC_FLG is set to 0b, the payload is not encrypted. When the ENC_FLG is set to 1b, the payload is encrypted.

The VERN_PKT is 2 bytes length field and indicates the format version of the Extended Packet Header. When the VERN_PKT is 0100h, the encryption of payload complies with the section from 3.5.1.1 until 3.5.1.6. When the VERN_PKT is 0110h or larger number, a way of encryption is indicated in a 4C Defined Area.

4C Defined Area is 6 bits length field and indicates encryption option to apply the payload. When the 4C Defined Area is 000000b, C2 encryption is applied. Detail of the encryption is described in section from 3.5.1.1 until 3.5.1.4. When the 4C Defined Area is 000100b, AES CBC mode of each 2KB is applied. Detail of the encryption is described in section 3.5.1.7. When the 4C Defined Area is 000101b, AES CBC mode of single encryption block is applied. Detail of the encryption is described in section 3.5.1.8. When the 4C Defined Area is 000110b, AES Counter mode is applied. Detail of the encryption is described in section 3.5.1.9. Other values are reserved. Table 3-2 is a synoptic one of value in 4C Defined Area

Table 3-2 Value in 4C Defined Area

Value	Meaning	Reference
000000b	C2 encryption	Section from 3.5.1.1 until 3.5.1.4
000100b	AES CBC mode of each 2KB	Section 3.5.1.7
000101b	AES CBC mode of single encryption block	Section 3.5.1.8
000110b	AES Counter mode	Section 3.5.1.9
Other values	Reserved	Not available

3.5.1.1. C2 Encryption for eBook Object Element (ELE)

The ELE consists of one Extended Packet Header and one payload. The payload except offset area can be encrypted. The size of the offset before the encrypted area is specified by Payload Forward Offset Size (PLD_FOZ). The size of the offset after the encrypted area is specified by Payload Backward Offset Size (PLD_BOZ) in the Extended Packet Header. The whole size of Payload is specified by Payload Size in the Extended Packet Header. The encrypted area is divided into integer multiple blocks. The length of each block except the last one is 2048 bytes. The last block is equal to or less than 2048 bytes. In case of C2-CPRM, each divided block except the last block is encrypted in C2 C-CBC mode defined in the *CPRM Specification: Introduction and Common Cryptographic Elements*. When the length of the last block is an integer multiple of 8 bytes, the last block is encrypted in C2 C-CBC mode. When the length of the last bloc k is not an integer multiple of 8 bytes, the last block except a residual area is encrypted in C2 C-CBC mode and the residual area is not encrypted, where the residual area is less than 8 bytes and the length of the last block except the residual area is integer multiple of 8 bytes. When the encrypted area is divided into *n* blocks and the *n*th block is encrypted except residual bytes, the size of payload (PLD_SZ) is calculated by the following formula.

$$\mathrm{PLD\_SZ} = \mathrm{PLD\_FOZ} + 2048\times(n\text{-}1) + 8\times m + (\text{the residual byte size}) + \mathrm{PLD\_BOZ}$$

Figure 3-1 depicts the encryption of eBook Object Element.

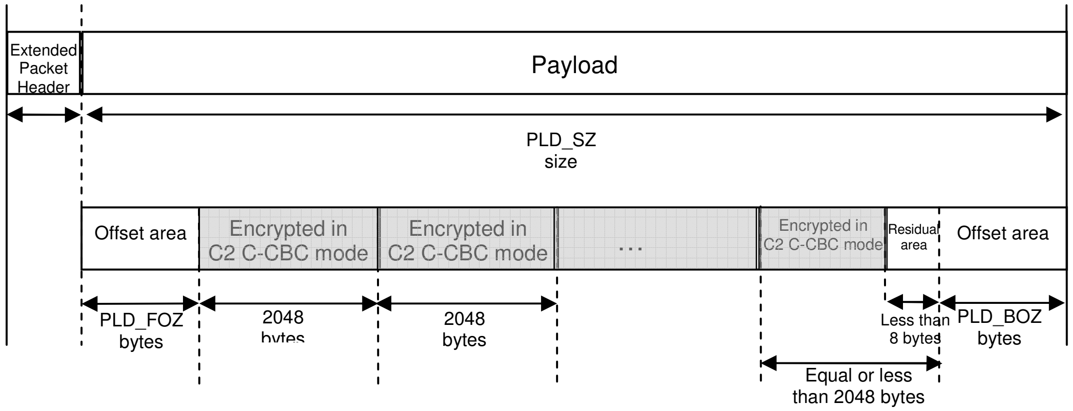

Figure 3-1 C2 Encryption for eBook Object Element

3.5.1.2. C2 Encryption for Normal eBook Extended Object (ExO)

The eBook Extended Object consists of one Extended Object Header and one payload as well as the ELE. The payload can contain several types of data including bitmap, text, sound, audio and video. Regardless of type, any ExO consists of the header first, followed by an offset area, one or more encrypted block(s) and last, an offset area. The last encrypted block may contain a residual area. In the case of C2-CPRM, except (1) MP4 and ETS (Extended Transport Stream) in the ExO, the method to encrypt the encrypted block is the same as the one for the case of the ELE. Figure 3-2 depicts the encryption of a normal eBook Extended Object.

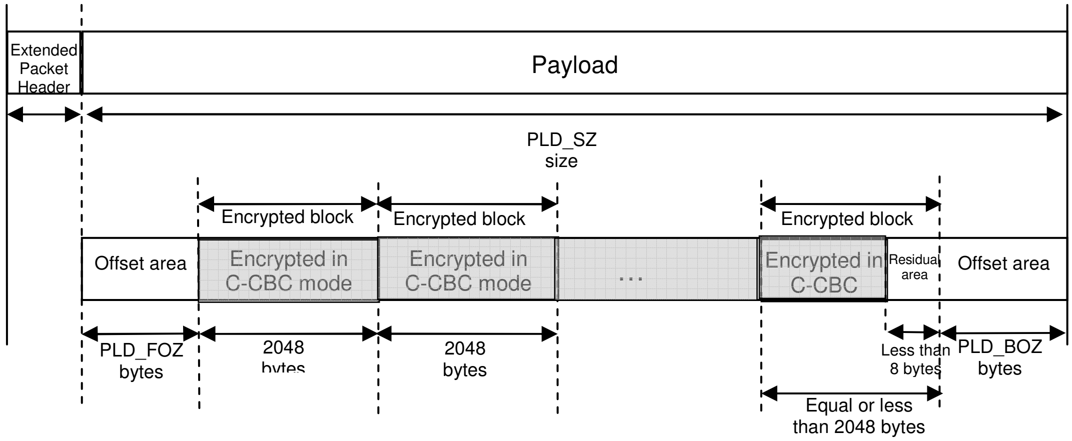

Figure 3-2 Encryption for Normal eBook Extended Object

3.5.1.3. C2 Encryption for ETS in eBook Extended Object (ExO)

In the case that the ExO contains the ETS, the encryption of the payload is as follows. The ETS consists of Extended Packet Header and Transport Packet. The ETSs are contained in Transport Stream Object Data (TOD). Plural TODs are stored in the payload area except its offset area. The number of the ETS in one TOD is denoted as M. The details are defined in the SD-SD eBook Specification defined in SDA. Each TOD is encrypted in the C-CBC mode defined in the *CPRM Specification: Introduction and Common Cryptographic Elements*. The encryption starts from the 161st byte of the TOD until the end of the TOD. The length of encryption is always an integer multiple of 8 bytes. Figure 3-3 depicts this case.

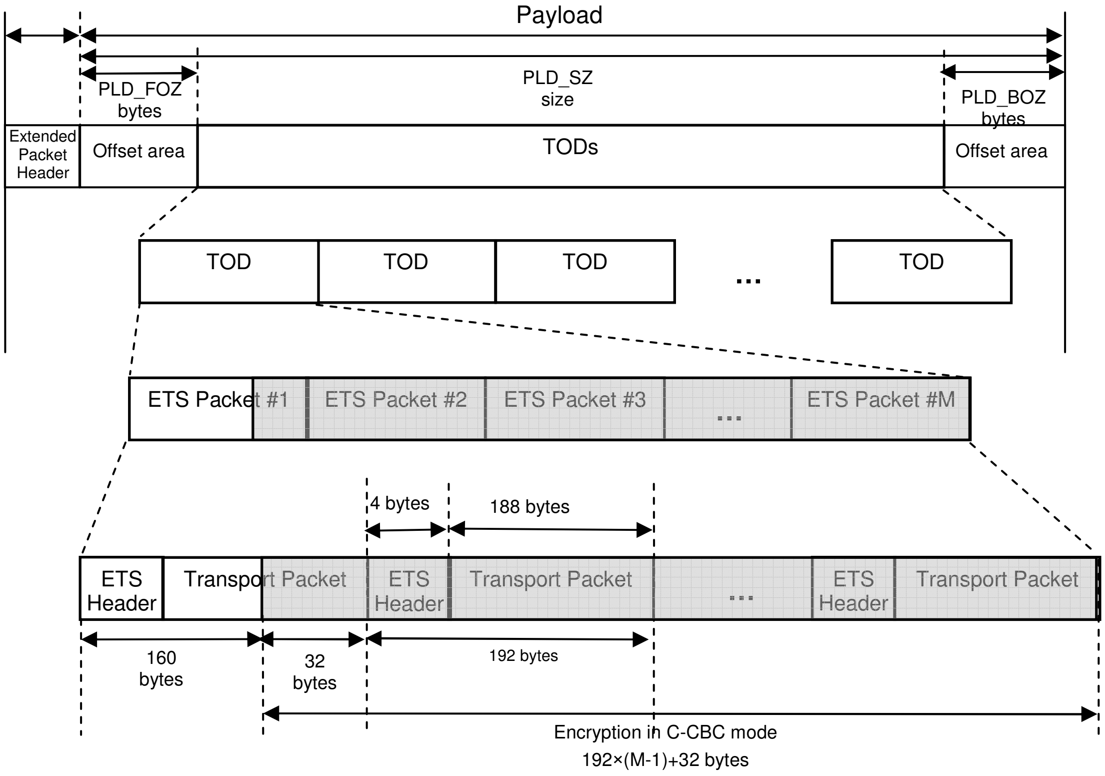

Figure 3-3 Encryption for ETS in eBook Extended Object

3.5.1.4. C2 Encryption for MP4 in eBook Extended Object (ExO)

In the case that the ExO contains the MP4, the encryption of the payload of ExO is as follows. The MP4 is stored in the payload area except its offset area. The payload of ExO contains one or more Media Object Unit(s) (MOUs). Each MOU contains one or more mdat box(s). Each mdat box consists of its header and one or more chunk(s). Each chunk consists of one or more block(s). The length of each block except the last one is 2048 bytes. The length of the last block is equal to or less than 2048 bytes. Each divided block except the last block is encrypted in the C-CBC mode defined in the *CPRM Specification: Introduction and Common Cryptographic Elements*. When the length of the last block is an integer multiple of 8 bytes, the last block is encrypted in the C-CBC mode. When the length of the last bloc k is not an integer multiple of 8 bytes, the last block except a residual area is encrypted in the C-CBC mode, where the residual area is less than 8 bytes and the length of the last block except the residual area is an integer multiple of 8 bytes. Figure 3-4 depicts this case.

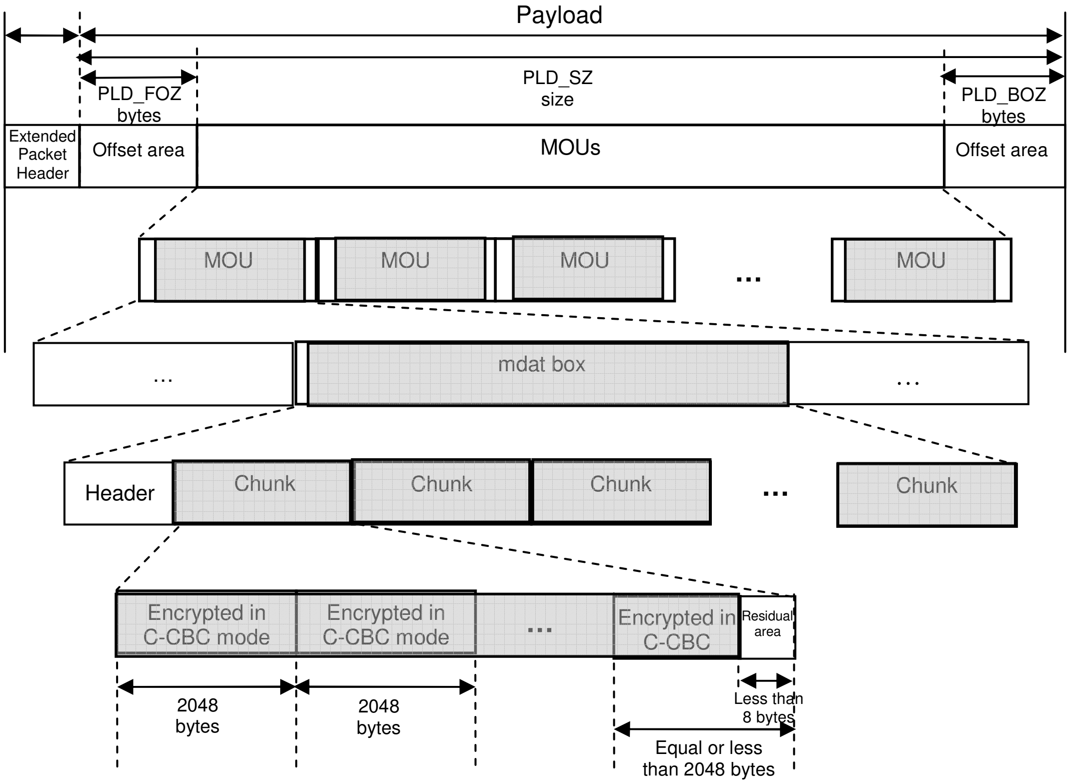

Figure 3-4 Encryption for MP4 in eBook Extended Object

3.5.1.5. AES Encryption for eBook Object Element (ELE)

In the case of AES-CPRM, each divided block of the ELE except the last block is encrypted in the AES CBC mode defined in the *CPRM Specification: Introduction and Common Cryptographic Elements*. When the length of the last block is an integer multiple of 16 bytes, the last block is encrypted in AES CBC mode. When the length of the last block is not an integer multiple of 16 bytes, the last block except a residual area is encrypted in AES CBC mode, where the residual area is less than 16 bytes and the length of the last block except the residual area is an integer multiple of 16 bytes. When the encrypted area is divided into *n* blocks and the *n*th block is encrypted except residual bytes, the size of payload (PLD_SZ) is calculated by the following formula.

$$\text{PLD\_SZ} = \text{PLD\_FOZ} + 2048\times(n-1) + 16\times m + (\text{the residual byte size}) + \text{PLD\_BOZ}$$

Figure 3-5 depicts the encryption of the eBook Object Element.

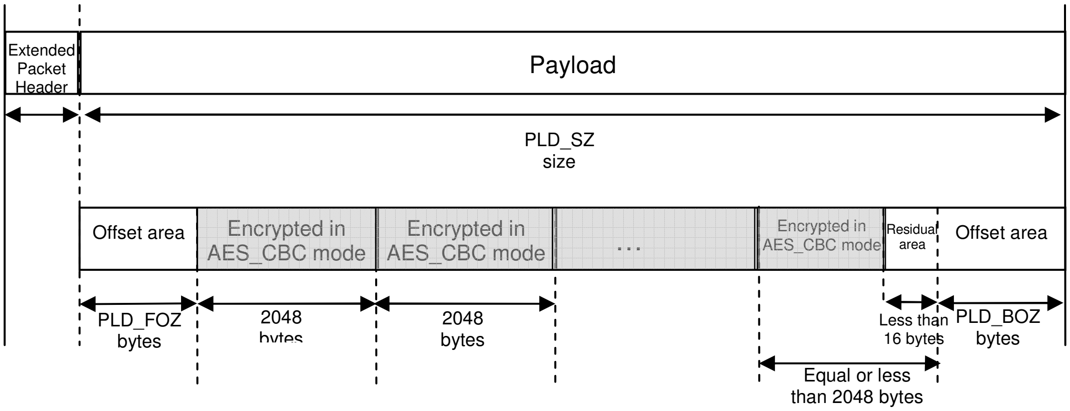

Figure 3-5 AES Encryption for eBook Object Element

3.5.1.6. AES Encryption for eBook Extended Object (ExO)

In the case of AES-CPRM, the AES Counter mode is used for the encryption of the ExO. The payload of the ExO is encrypted by AES Counter mode. The value of initial counter block (T_1) described in the *CPRM Specification: Introduction and Common Cryptographic Elements* is calculated by the following formula:

$$T_1 = \text{AES\_G}(CV\ \text{Content ID}) \oplus \text{an additional value}$$

The *CV* is the secret constant value of 16 bytes length and provided in the *CPRM Specification: SD Memory Card Book SD-SD (Separate Delivery) eBook Profile Confidential Part*. The additional value is 16 bytes length and consists of the fields defined in Table 3-3. The counter for CTR mode shall be incremented by one (1) for every block encountered.

Table 3-3 Additional Value for Initial Counter Block

(Description order)

RBP	Field Name	Contents	Number of bytes
0 to 1	I_BOS	Index of BOS including the ExO	2 bytes
2 to 3	Reserved	0000h	2 bytes
4 to 5	I_EXO	Index of the ExO in the BOS	2 bytes
6 to 15	Reserved	00000000000000000000h	10 bytes
Total			16 bytes

Figure 3-6 depicts the encryption of normal eBook Extended Object.

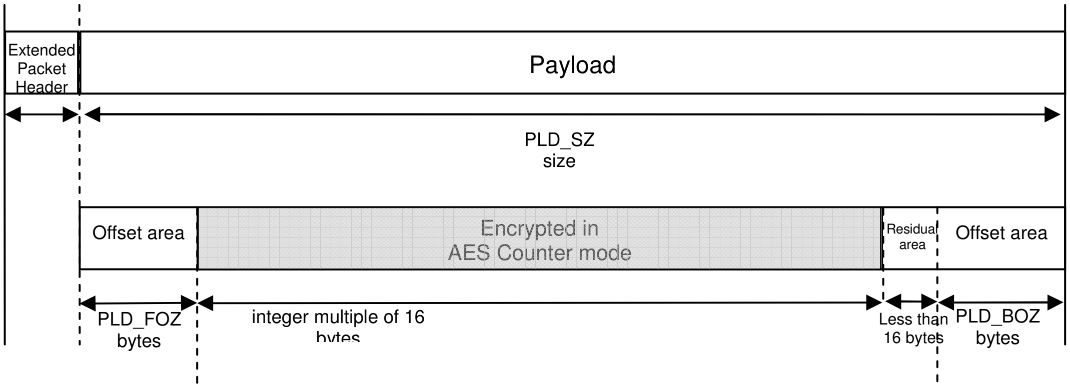

Figure 3-6 AES Encryption for eBook Extended Element

3.5.1.7. AES Encryption in AES CBC mode of each 2KB

This section describes encryption in AES CBC mode of each 2KB. Figure 3-7 depicts the AES encryption. Payload except offset area is divided into one or more blocks. Each block except the last one is 2 KB length. The last block is no more than 2 KB length. Each divided block is individually encrypted in AES CBC mode. When the length of the last block is not an integer multiple of 16 bytes, the last block except a residual area is encrypted in the AES CBC mode, where the residual area is less than 16 bytes and the length of the last block except the residual area is an integer multiple of 16 bytes. When the encrypted area is divided into *n* blocks and the *n*th block is encrypted except residual bytes, the size of payload (PLD_SZ) is calculated by the following formula.

PLD_SZ = PLD_FOZ + 2048×(n-1) + 16×m + (the residual byte size) + PLD_BOZ

where PLD_FOZ is Payload Forward Offset Size and PLD_BOZ is Payload Backward Offset Size.

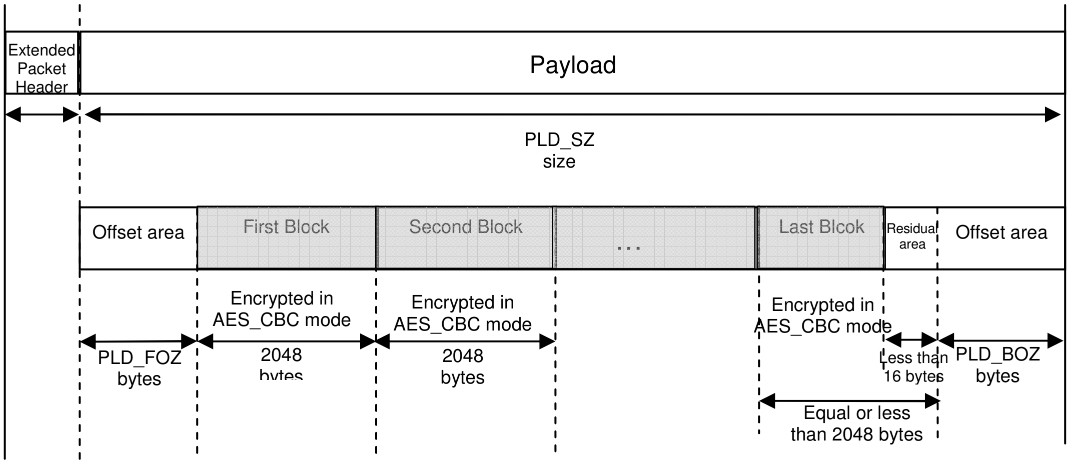

Figure 3-7 AES Encryption in AES CBC mode of each 2KB

3.5.1.8. AES Encryption in AES CBC mode of single encryption block

This section describes encryption in AES CBC mode of single encryption block. Figure 3-8 depicts the AES Encryption in AES CBC mode of single encryption block. Payload except offset area is encrypted as single encryption block. When the length of the encryption block is an integer multiple of 16 bytes, the whole encryption block is encrypted in AES CBC mode. When the length of the encryption block is not an integer multiple of 16 bytes, the encryption block except a residual area is encrypted in AES CBC mode, where the encrypted block is divided into main area and residual area where the main area is an integer multiple of 16 bytes and the residual area is less than 16 bytes.

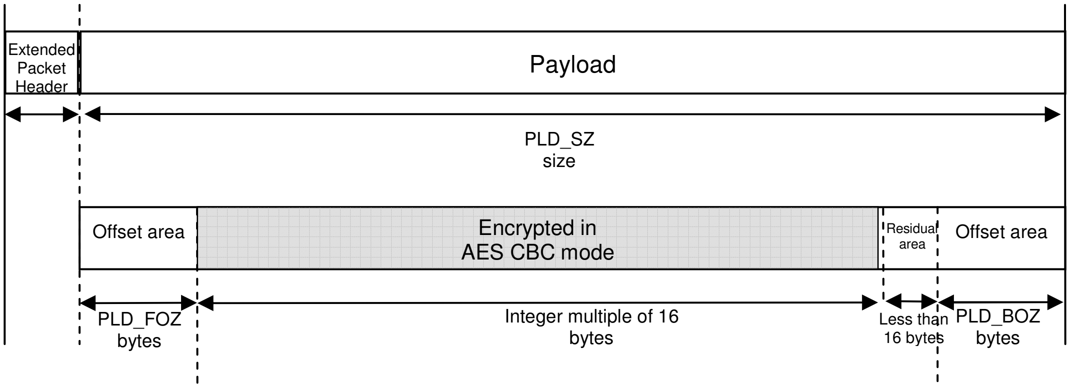

Figure 3-8 Encryption in AES CBC mode of single encryption block

3.5.1.9. AES Encryption in AES Counter mode

This section describes the AES Counter mode for payload. Figure 3-9 depicts the AES Encryption in AES Counter mode. Payload except offset area is encrypted as single encryption block. When the length of the encryption block is an integer multiple of 16 bytes, the encryption block is encrypted in AES Counter mode. When the length of the encryption block is not an integer multiple of 16 bytes, the encryption block except a residual area is encrypted in AES Counter mode, When the length of the encryption block is not an integer multiple of 16 bytes, the encryption block except a residual area is encrypted in AES Counter mode, where the encrypted block is divided into main area and residual area where the main area is an integer multiple of 16 bytes and the residual area is less than 16 bytes.

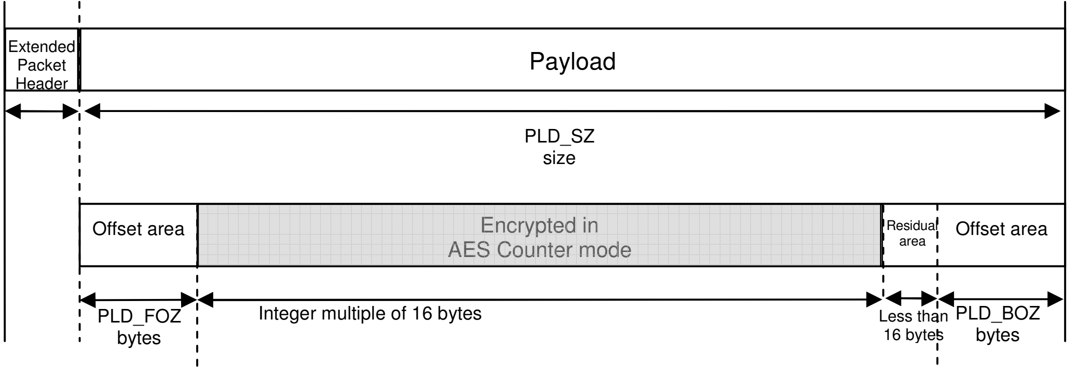

Figure 3-9 Encryption in AES Counter Mode

The value of initial counter block (T_1) for the AES Counter mode described in the *CPRM Specification: Introduction and Common Cryptographic Elements* is calculated by the following formula:

$$T_1 = \text{AES\_G}(CV\ \text{Content ID}) \oplus \text{an additional value}$$

The *CV* is the secret constant value of 16 bytes length and provided in the *CPRM Specification: SD Memory Card Book SD-SD (Separate Delivery) eBook Profile Confidential Part*. The additional value is 16 bytes length and consists of the fields defined in Table 3-4. The counter for AES Counter mode shall be incremented by one (1) for every block encountered.

Table 3-4 Additional Value for Initial Counter Block

(Description order)

RBP	Field Name	Contents	Number of bytes
0 to 1	I_BOS	Index of BOS including the ExO	2 bytes
2 to 3	Reserved	0000h	2 bytes
4 to 5	I_EXO	Index of the ExO in the BOS	2 bytes
6 to 15	Reserved	00000000000000000000h	10 bytes
Total			16 bytes

3.6. Process Description for eBook Profiles

This section describes processes of CPRM for SD-SD eBook.

3.6.1. Print Out Process

A Print Out Device which executes Print Out shall execute the Print Out Process described below. The Print Out Process is based on the Playback Process defined in the *CPRM Specification: SD Memory Card Book SD-SD (Separate Delivery) Part*. Note that the Time Based Usage Rules of SD-SD Content is applied to Print Out function. That means the Playback Counter and set of the period at the first time using Current First Playback Flag field are treated in Print Out Process as well as Playback Process. The Print Out Device shall execute the following steps.

(1) Determine the CKMG file and CKI associated with the SD-SD Content to be printed out.

The Print Out Device determines the CKMG filename and the CKI.

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

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

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

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

(3) Determine the UKURMG file and UKURE associated with the SD-SD Content.

(3.1) Obtain UKURE_SRN.

The Print Out Device obtains the UKURE_SRN ***s*** associated with the SD-SD Content.

(3.2) Determine the UKURMG file and UKURE associated with the SD-SD Content.

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

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

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

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

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

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

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

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

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

The Print Out Device decrypts the UKURE using the UKURE Decryption process and securely holds it as the decrypted UKURE image.

In the case of C2-CPRM, the Print Out Device checks this decrypted UKURE image as follows:

- If the Check Value is not '0123456789ABCDEFh,' the process shall be aborted.
- If the TB for AES is not equal to 0b, this process shall be aborted.
- If the TB for future use is not equal to '000000b,' the process shall be aborted.
- If the User Key Type in the UKURE is equal to '0b,' the Print Out Device checks the Hash Value in UKURE. If the stored Hash Value in UKURE is not equal to the calculated value from the temporary CKMG image using Hash Calculation Process, the device shall execute CKMG Recovery Process described in Section 5.7 of the *CPRM Specification SD Memory Card Book SD-SD (Separate Delivery) Part*.

In the case of AES-CPRM, the Print Out Device checks this decrypted UKURE image as follows:

- If the Check Value is not equal to the value of calculated CMAC(K_{u128}, high 40 bytes of the UR_U), the process shall be aborted..
- If the TB for AES is not equal to 1b, this process shall be aborted.
- If the TB for future use is not equal to '000000b,' the process shall be aborted.
- If the User Key Type in the UKURE is equal to '0b,' the Print Out Device checks the Hash Value in UKURE. If the stored Hash Value in UKURE is not equal to the calculated value from the temporary CKMG image using Hash Calculation Process, the device shall execute CKMG Recovery Process described in Section 5.7 of the *CPRM Specification SD Memory Card Book SD-SD (Separate Delivery) Part*.

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

The Print Out Device decrypts the CKI using the CKI Decryption process and securely holds it as the decrypted CKI image.

In the case of C2-CPRM, the Print Out Device checks this decrypted CKI image as follows:

- If the Check Value is not '0123456789ABCDEFh,' the process shall be aborted.
- If the PTB for AES is not equal to '0b,' this process shall be aborted.
- If the Trigger Bits for eBook Profile Processes is not equal to '00000000b,' the process shall be aborted.
- If the Current Playback Counter is equal to '0000h,' then the process shall be aborted.

In the case of AES-CPRM, the Print Out Device checks this decrypted CKI image as follows:

- If the Check Value is not equal to the value of calculated CMAC(K_{c128}, high 40 bytes of the UR_C), the process shall be aborted.
- If the PTB for AES is not equal to 1b, this process shall be aborted.
- If the Trigger Bits for Print Out Processes is not equal to '00000000b,' the process shall be aborted.
- If the Current Playback Counter is equal to '0000h,' then the process shall be aborted.

(7) Check if Time-Based Usage Rules are set in the CKI and UKURE

The Print Out Device checks if Time-Based Usage Rules are valid in the CKI and UKURE. Specifically, if at least one of following conditions is true, Time-Based Usage Rules are valid. Note that if the device works in a Mode, the device shall not change the Mode to another during this process.

(a) Validity of Current Start Date in the CKI is '1b'

(b) Validity of Current End Date in the CKI is '1b'

(c) Validity of Span in the CKI is '1b' and Span Length in the CKI is '0b'

(d) Current Playback Counter in the CKI is not 'FFFFh'

(e) Validity of Span is '1b' in the CKI and Span Length in the CKI is '1b'

(f) Validity of UK_STARTDDATE in the UKURE is '1b'

(g) Validity of UK_ENDDATE in the UKURE is '1b'

(h) Validity of UK_SPAN in the UKURE is '1b'

Then the device goes to following sub-steps.

(7.1) When all of conditions above are false (not true), the Print Out Device goes to the last step (15).

(7.2) When one of the conditions is true and the Print Out Device does not support Time-Based Usage Rules or the device does not work in neither Mode A, Mode B1 nor Mode B2, this process shall be aborted.

(7.3) When either (d) or (e) is true and all of (a), (b), (c), (f), (g) and (h) are false (not true), that is, rules require no date and time clock, the Print Out Device goes to the step (11).

(7.4) When the Clock Usage Flag in UR_C_TBUR_CDT is '01b,' this process shall be aborted.

(7.5) When the Clock Usage Flag in UR_C_TBUR_CDT is '11b' and the device does not work in Mode B2, this process shall be aborted.

(7.6) When the Clock Usage Flag in UR_C_TBUR_CDT is '10b' and the device does not work in Mode B2 nor Mode B1, this process shall be aborted.

(7.7) Otherwise (rules require date and time clock), the Print Out Device executes following steps from (8) to (13).

(8) Obtain the current date and time

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

(9) Update the decrypted CKI image and UKURE image (Phase 1).

In this phase, the CKI is checked if playback or Print Out of the CKI with span-limited is done for the first time. The Print Out Device checks the Current First Playback Flag field and the Validity of Span field. When the Current First Playback Flag field in the CKI is equal to '0b,' the Validity of Span field in the CKI is equal to '1b' and the Span Length is equal to '0b,' the Print Out Device executes sub-steps from (9.1) to (9.3). When the First Playback Flag field in the UKURE is equal to '0b' and the Validity of

UK_SPAN field in the UKURE is equal to ‘1b,’ the Print Out Device executes sub-steps from (9.4) to (9.6). Otherwise the Print Out Device skips these sub-steps and go to step (10).

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

a) When the Validity of Current Start Date field is equal to ‘0b,’ the Print Out Device sets the Current Start Date of Playback Period field of the decrypted CKI 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 Print Out 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 Print Out Device sets the Current Start Date of Playback Period field of the decrypted CKI image to the current date and time.

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

a) When the Validity of Current End Date field is equal to ‘0b,’ the Print Out 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 CKI 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 Print Out 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 Print Out 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 CKI image, the Print Out Device sets the Current End Date of Playback Period field of the decrypted CKI image to the calculated end date and time.

(9.3) The Print Out Device sets the Current First Playback Flag field to ‘1b.’

(9.4) Update the UR_UK_STARTDATE

When the Validity of UK_STARTDATE field is equal to ‘0b,’ the Print Out Device sets fields of the decrypted UKURE image by following settings:

- The Date of UK_STARTDATE field is set to the date of the current date and time.
- The Hour of UK_STARTDATE field is set to the hour of the current date and time.
- The Validity of UK_STARTDATE field is set to ‘1b.’

When the Validity of UK_STARTDATE field is equal to ‘1b,’ the Print Out Device compares the current date and time with the date and time of the UK_STARTDATE field.

- If the current date and time precedes the UK_STARTDATE, then the process shall be aborted.
- If the current date and time does not precede the UK_STARTDATE, then the Print Out Device sets (1) the Date of UK_STARTDATE field of the decrypted CKI image to the date of the current date and time and (2) the Hour of UK_STARTDATE field of the decrypted CKI image to the hour of the current date and time.

(9.5) Update the UR_UK_ENDDATE

When the Validity of UK_ENDDATE is equal to '0b,' the Print Out Device calculates the end date and time by adding the value specified in the UR_UK_SPAN field to the current date and time. Then the Print Out Device set fields of the decrypted UKURE image by following settings:

- The Date of UK_ENDDATE field is set to the date of the calculated date and time.
- The Hour of UK_ENDDATE field is set to the hour of the calculated date and time.
- The Validity of UK_ENDDATE field is set to '1b.'

When the Validity of UK_ENDDATE is equal to '1b,' the Print Out Device compares the current date and time with the date and time of the UR_UK_ENDDATE.

- If the current date and time does not precede the UR_UK_ENDDATE, then the process shall be aborted.
- If the current date and time precedes the UR_UK_ENDDATE, then the Print Out Device calculates the end date and time by adding the value specified in the UR_UK_SPAN field to the current date and time. If the calculated date and time precedes the UR_UK_ENDDATE of the decrypted CKI image, the Print Out Device sets (1) the Date of UK_ENDDATE of the decrypted CKI image to the date of the calculated end date and time and (2) the Hour of UK_ENDDATE of the decrypted CKI image to the hour of the calculated end date and time.

(9.6) The Print Out Device sets the First Playback Flag field to '1b.'

(10) Check the CKI and UKURE in the temporary CKMG image (Phase 2).

In this phase, it checks if the current time is in the designated period.

(10.1) 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.

(10.2) 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.

(10.3) If the Validity of UK_STARTDATE field is equal to '1b' and the current date and time precedes the UR_UK_STARTDATE, then this process shall be aborted.

(10.4) If the Validity of UK_ENDDATE field is equal to '1b' and the current date and time does not precede the UR_UK_ENDDATE, then this process shall be aborted.

(11) Update the temporary CKI (Phase 3).

In this phase, a process about the number of playback or Print Out times is done. Specifically, if the Current Playback Counter of the decrypted CKI image is not equal to 'FFFFh,' the Print Out Device decrements the value of the Current Playback Counter and encrypts the CKI in the temporary CKMG image using the CKI Encryption process.

(12) Check the User Key Type in UKURE.

The Print Out Device checks the User Key Type which is obtained in step (5).

(a) When the User Key Type is equal to '0b,' go to step (13).

(b) When the User Key Type is equal to '1b,' go to step (15).

(13) Update the temporary UKURMG image.

If the decrypted CKI image has not been updated in step (9), (11), then go to step (15).

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

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

The Print Out Device securely writes the updated temporary UKURMG and CKMG images as the updated UKURMG and CKMG files to the SD Memory Card using the CKMG Update Process in described in Section 5.7 of the *CPRM for SD-SD Part* book. Then the Print Out Device securely reads the updated UKURMG file from the SD Memory Card using the Secure Read Process and verifies that the update of the ***m***th UKURE in the UKURMG file has completed successfully.

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

(15) Start Print Out

The Print Out Device starts to print out the SD-SD Content. Notice that after starting Print Out, the Print Out Device does not need to abort the Print Out before the Print Out completes even when the SD-SD Content contains a time control restriction such as Short Span Mode and the Print Out does not complete within the period.

In step (6), the Print Out Device may check two or more CKIs from a CKMG at one process. The Print Out Device can store the valid CKIs temporarily and securely. When the device prints out the content corresponding to the stored CKIs, the device can print out the content with skipping from step (1) to step (5). Temporarily and securely stored CKIs shall be deleted in the event of the following conditions:

The SD Memory Card is pulled out.

The CKI in the SD Memory Card is deleted.

The Print Out Device's power is off.

The Print Out Device application is terminated

3.6.2. Playback Process

To playback SD-SD eBook content, the Playback Device compliant with the current revision of this book shall modify the Playback Process defined in Section 6.12 of the *CPRM Specification: SD Memory Card Book SD-SD (Separate Delivery) Part*.

In Step (6) of the Playback Process, in the case of both C2-CPRM and AES-CPRM, the Playback Device shall additionally check UR_B_OUTPUT field as follows:

- If the AVOP flag is set to ‘0b’, the Playback Device shall not output video stream of the SD-SD eBook content through analog video output.
- If the AVOP flag is set to ‘1b’, the Playback Device is allowed to output video stream of the SD-SD eBook content through analog video output in accordance with Compliance Rules of SD-SD eBook described in the *CPRM for eBook Addendum*.
- If the UDVOP flag is set to ‘0b’, the Playback Device shall not output video stream of the SD-SD eBook content through unprotected digital video output.
- If the UDVOP flag is set to ‘1b’, the Playback Device is allowed to output video stream of the SD-SD eBook content through unprotected digital video output in accordance with Compliance Rules of SD-SD eBook described in the *CPRM for eBook Addendum*.