Content Protection for Recordable Media Specification

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

Intel Corporation

International Business Machines Corporation

Panasonic Corporation

Toshiba Corporation

Revision 0.92

December 15, 2011

This page is intentionally left blank.

Preface

Notice

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

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

Intellectual Property

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

Contact Information

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

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

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

This page is intentionally left blank.

Table of Contents

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, 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 Video format.

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

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 Video 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/CPPM License Agreement*

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

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

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

4C Entity, LLC, *CPRM Specification: SD Memory Card Book SD-SD (Separate Delivery) Part, Revision 0.91*

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

SD Association, *SD Memory Card Specifications, Part 3: Security Specification, Version 2.0*

SD Association, *SD Memory Card Specifications, Part 15: SD-SD (Separate Delivery) Specification, Version 1.10*

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

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

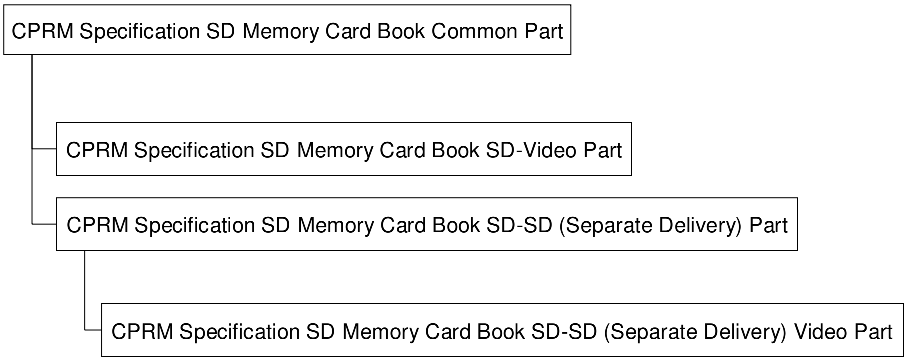
CPRM Specification SD Memory Card Book Common Part
CPRM Specification SD Memory Card Book SD-Video Part
CPRM Specification SD Memory Card Book SD-SD (Separate Delivery) Part
CPRM Specification SD Memory Card Book SD-SD (Separate Delivery) Video Part

Figure 1-1 Specification structure for SD-SD Video

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.

Chapter 2
Abbreviations and Acronyms

2. Abbreviations and Acronyms

The following abbreviations and acronyms are used in this document:

APS	Analog Protection System
APSTB	Analog Protection System Trigger Bit
AST	Analog Sunset Token
C-CBC	Converted Cipher Block Chaining
C2	Cryptomeria Cipher
CCI	Copy Control Information
CKI	Content Key Information
CKMG	Content Key Manager
CPF	Copy Permission Field
CPRM	Content Protection for Recordable Media
ECKUR	Encrypted Content Key and Usage Rule
E_APSTB	Encrypted Analog Protection System Trigger Bit
E_CPF	Encrypted Copy Permission Field
ETS	Extended Transport Stream [1]
EPN	Encryption Plus Non-assertion
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
LLC	Limited Liability Company
NRF	Non Re-encryption Flag
MO	Media Object [1]
MOU	Media Object Unit [1]
MPEG	Moving Picture Experts Group
PKSQ_Ns	Packet Sequence Number [1]
RDI	Real-time Data Information
StrmCCI	Stream Copy Control Information
TSTS	Time Stamp Transport Stream

[1] Defined in *SD Memory Card Specifications, Part 15: Video Profile Specification, Addendum to SD Specifications Part 15 Separate Delivery Specification, Version 1.00*

TKURE	Title Key & Usage Rule Entry
TKURE_SRN	Title Key & Usage Rule Entry Search Number
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_V	Usage Rules for Video

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

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

3.1. Introduction

This chapter specifies details for using CPRM to protect SD-SD Video content and describes details on using CPRM to realize some features. Regarding the SD-SD Video Profile, refer to *SD Memory Card Specifications – Part15 Video 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 *CPRM Specification: SD Memory Card Book Common Part*.

3.3. CPRM Components

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

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

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

3.4.1. Usage Rules for Video

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

As shown in Table 3-1, UR_V consists of UR_V_TRIGGER, UR_V_CURRENT, UR_V_INITIAL, UR_V_EXSDV_INFO, UR_V_CCIFLAGS and Reserved. When recorded, reserved field shall be filled with 0b unless some specific values are provided. If the field is not set to 0b, the device shall ignore the field.

Table 3-1 Usage Rules for Video

(Description order)

RBP	Field Name	Contents	Number of bytes
0	UR_V_TRIGGER	Trigger Bits for Video Profile Processes	1 byte
1 to 2	UR_V_CURRENT	Current Fields Group for Video	2 bytes
3 to 4	UR_V_INITIAL	Initial Fields Group for Video	2 bytes
5 to 6	UR_V_EXSDV_INFO	Information for Export to SD-Video	2 bytes
7	UR_V_CCIFLAGS	CCI Flags	1 byte
8 to 9	Reserved	Reserved	2 bytes
Total			10 bytes

(RBP 0) UR_V_TRIGGER

This field describes Trigger Bits for Video Profile Processes.

b7	b6	b5	b4	b3	B2	b1	b0
Trigger Bits for Video Profile Processes							

Trigger Bits for Video Profile Processes ... These bits controls whether or not a process is executed. 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. In use of this version of specification, the Trigger Bits of a Content Key shall set this value only to 00000000b when the Content Key is made.

00000000b: Accessing devices conforming to this version of specification can control the processes described in 3.6.

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

(RBP 1 to 2) UR_V_CURRENT

This field describes Current Fields Group for Video This filed consists of Current Export to SD-Video Flag and Reserved field.

b15	b14	b13	b12	b11	b10	b9	b8
Current Export to SD-Video Flag	Reserved						

b7	b6	b5	b4	b3	b2	b1	b0
Reserved							

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

1b: Export to SD-Video is permitted.

This field shall not be inherited to a replicated Content Key when the Content Key is copied. For example, this flag shall be set to 1b when User Key Type is set to 1b. Please refer section 3.4.2 in this book.

(RBP 3 to 4) UR_V_INITIAL

This field describes Initial Fields Group for Video. This filed consists of Initial Export to SD-Video and Reserved field.

<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>Initial Export to SD-Video Flag</td><td colspan="7">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>

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

1b: Export to SD-Video is permitted.

This field is set when the Content Key is made. It never changes even when the content is viewed. This field shall be inherited to a replicated Content Key when the Content Key is copied. For example, this flag shall be set to 1b when User Key Type is set to 1b. Please refer section 3.4.2 in this book.

(RBP 5 to 6) UR_V_EXSDV_INFO

This field describes Information for Export to SD-Video function. This filed consists of Move Control Information, Reserved, Title Key Type and TKURE Number. A set of Title Key Type and TKURE Number is called Exported Content Identifier in this specification.

<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="2">Move Control Information</td><td colspan="2">Reserved</td><td>Title Key Type</td><td colspan="3">TKURE Number</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">TKURE Number</td></tr>
</table>

Move Control Information ... When the content is exported, exporting device shall store the Current Move Control Information in two bits length, which is defined in CPRM for SD-SD specification. This value is restored when the content is re-imported.

Title Key Type ... Represents the key file where the exported Content Key is stored in the SD-Video format.
0b: The Title Key of exported content is stored in VIDEO001.KEY file under SD-Video directory.
1b: The Title Key of exported content is stored in MOxxx.KEY file under SD-Video directory, where xxx is a serial number (001~009). .
When the Exported Content consists plural MOUs, this field shall be set to 0b. These files are defined in *CPRM SD Memory Card book SD-Video Part*.

TKURE Number ... When the content is exported, exporting device shall store the TKURE_SRN of the Title Key stored in SD-Video format defined in *CPRM SD Memory Card book SD-Video Part* . In the case that Title Key Type is set to 0b, this field is set to the TKURE_SRN for Programs of the Title Key. The range of this value is from 00000000001b to 00001100011b (99 in decimal). In the case that Title Key Type is set to 1b, this field is set to the TKURE_SRN for MOs. The range of this value is from 00000000001b to 11111111111b (2047 in decimal). When the content is not exported, this field shall be set to 00000000000b.

(RBP 7) UR_V_CCIFLAGS

This field describes copy control information and consists of StrmCCI, Non Re-encryption Flag, APSTB, AST and Reserved.

b7	b6	b5	b4	b3	b2	b1	b0
StrmCCI	Non Re-encryption Flag	APSTB		AST	Reserved		

StrmCCI … Represents whether or not the CCI_Byte in the content stream is valid. When the category of content is Digital Stream Use and the Packet Sequence consists ETS packets, this field shall be set to 1b. Otherwise this field shall be set to 0b. The term “category” or “Digital Stream Use” herein is defined in *SD Memory Card Specifications – Part15 Video Profile Specification Addendum to SD Specifications Part 15 Separate Delivery Specifications*. When this bit is set to 1b and Current Export to SD-Video Flag is 1b, setting of CCI in the stream has a restriction described in section 3.4.2..

Non Re-encryption Flag ... This flag is used for content which category is Digital Stream Use. That is, when StrmCCI is set to 1b, this flag is valid. When a category of content is not Digital Stream Use, this flag shall be set to 0b.
This flag shall not be set to 1b when RDI packs in the content stream are set to both “No More Copy” and “EPN”. When the flag is set to 1b and a device does the copy process described in section 3.6.3 of this book, the device is not required to re-encrypt the content.

APSTB ... 00b : APS is Off

01b: Type 1 of APS is On

10b: Type 2 of APS is On

11b: Type 3 of APS is On

APS is defined in Compliance Rules in *CPPM/CPRM License Agreements*.

AST	0b: Analog Sunset is not applied. 1b: Analog Sunset is applied to the Decrypted CPRM Video Content in accordance with the *CPRM/CPPM License Agreements*.

Note that the Trigger Bits for Copy/Move, StrmCCI and Non Re-encryption Flag shall be set to the combinations in the table below. Other combinations may be used in a future. Copy Process I and Playback Process for a CKI which is set to a combination is required to another process described in Section 3.6.

Table 3-2 Combinations of Trigger Bits for Copy/Move, StrmCCI and NRF

Trigger Bits for Copy/Move	0000b	1000b	0000b
StrmCCI	0b	1b	1b
Non Re-encryption Flag	0b	0b	1b

3.4.2. User Key Type

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

Table 3-3 Restriction of Usage Rules for Video

Field Name	Restriction
Current Export to SD-Video Flag	0b

These parameters are not updated once the Content Key is stored. Note that a device cannot securely erase a Content Key from CKMG file encrypted with a User Key whose User Key Type is 1b.

3.5. Content Encryption Format

3.5.1. Video Unit Encryption

SD-SD Video Profiles treats two categories of content defined in *SD Memory Card Specifications – Part15 Video Profile Specification Addendum to SD Specifications Part 15 Separate Delivery Specifications*. One is called General Use. The other is called Digital Stream Use.

3.5.1.1. Encryption for General Use content

For coding of General Use content, H.264 is used and designed to contain the media information of an ISO/IEC 14496 presentation as one of the file format that contains plural MOUs. Each MOU is encrypted by the Content Key as follows:

- General Use content consists of SD-SD Content Common Information (SSCOI), SD-SD Video Profile Content Units Information (SSVPI) and Media Object Section (MOSEC)
- MOSEC consists of plural Media Object Units (MOU).
- MOU consists of Movie Box (moov), Movie Fragment Box (moof), Media Data Box (mdat), and other miscellaneous boxes. Movie Box (moov) contains Sample To Chunk Box (stsc) and Movie Fragment Box

(moof) contains Track Fragment Run Box (trun).

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

Figure 3-1 shows the encryption structure of MOU and Chunks.

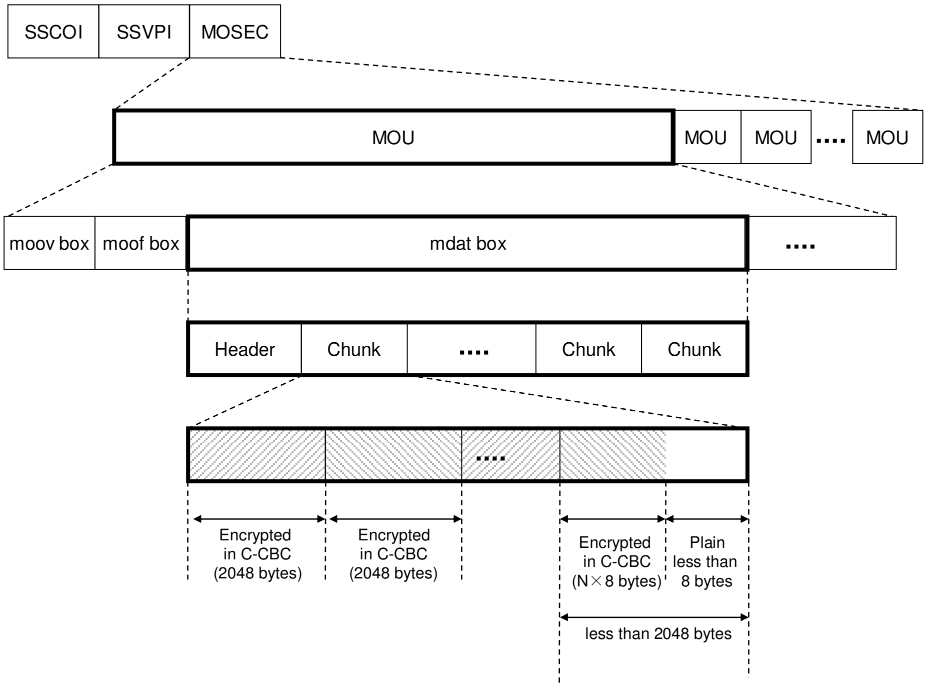

Figure 3-1 Encryption structure of mdat boxes and Chunks

Table 3-4 and Table 3-5 show the encrypted Chunk.

Table 3-4 Encrypted Chunk without residual block (N=8×n)

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

Table 3-5 Encrypted Chunk with residual block (N=8×n+m, m<8)

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

If Chunk size is larger than 2048 bytes, cipher chain in Chunk is reset every 2048 bytes as shown in Table 3-6. Each Encryption Block starts a new C-CBC mode cipher chain.

Table 3-6 Encrypted Chunk (N=2048×p+8×n+m, 8×n+m<2048, m<8)

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

3.5.1.2. Encryption for Digital Stream Use content

For coding of Digital Stream User content, the unique format defined in SD-SD Video specification is used. This format is based on MPEG Transport Stream. The format is defined as Transport Stream Object Data Unit. A Transport Stream Object Data Unit is consisting from two types of transport stream format, the one is Extended Transport Stream (ETS) and the other one is Time Stamped Transport Stream (TSTS).

- Digital Stream Use content consists of following data units:
  - SD-SD Content Common Information (SSCOI),
  - SD-SD Video Profile Content Units Information (SSVPI),
  - Media Object Information Unit Section (MOISEC) or Media Object Information Partial Unit Section (MOIPSEC),
  - Media Object Additional Information Unit Section (MAISEC) or Media Object Additional Information Partial Unit Section (MAIPSEC) and
  - Media Object Unit Section (MOSEC) or Media Object Partial Unit Section (MOPSEC).
- MOSEC consists of plural Media Object Units (MOU), which is .Transport Stream Object Data Unit for Digital Stream Use.
- MOSEC consists of an integer number of Packet Sequences.

One Packet Sequence consists of either (a) plural Extended Transport Stream (ETS) Packets or (b) plural Time Stamp Transport Stream (TSTS) Packets. In this book, both an ETS Packet and TSTS packet are denoted as ETS/TSTS Packet. The number of ETS/TSTS Packets that compose one Packet Sequence is stored in Packet Sequence Number (PKSQ_Ns) field of MOISEC or MOIPSEC in User Data Area. In the case of last Packet Sequence the number of ETS/TSTS Packets may be less than or equal to PKSQ_Ns. Figure 3-2 shows the relationship between Packet Sequence and ETS/TSTS Packet. In this book, M represents the number of PKSQ_Ns.

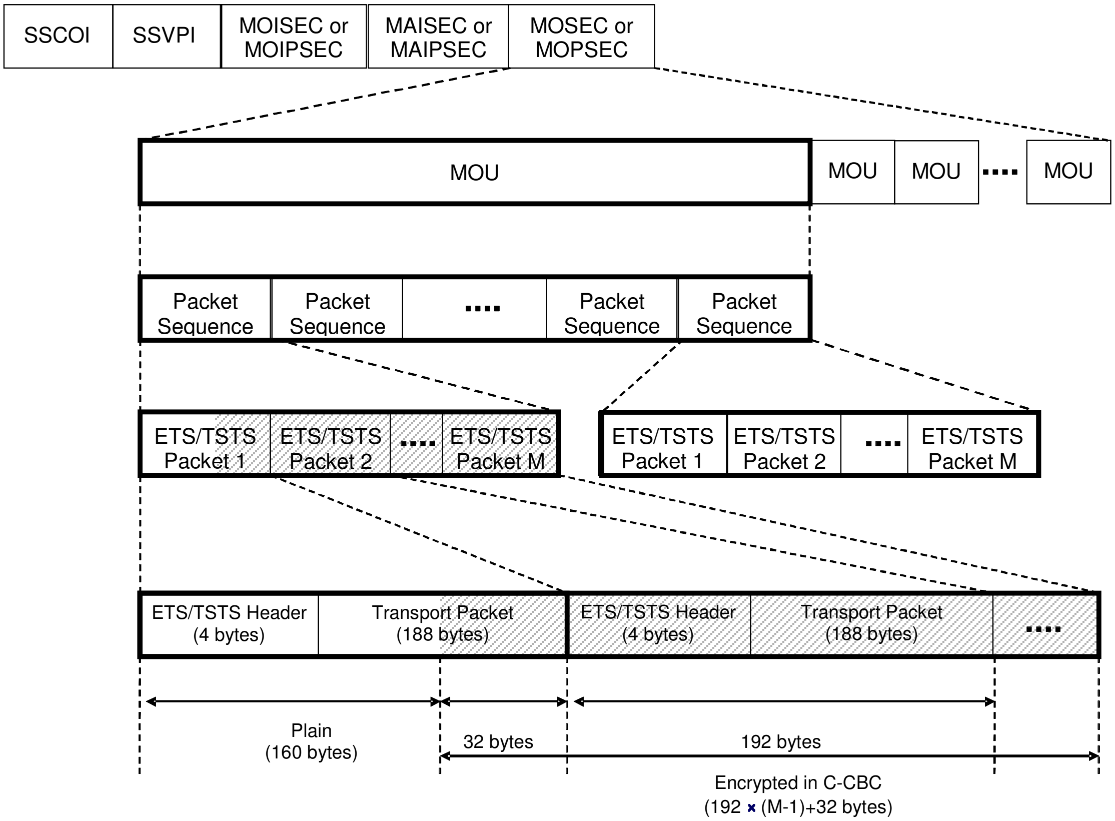

Figure 3-2 Encrypted Structure of ETS/TSTS Packet Sequences

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

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

When a Packet Sequence is required to be encrypted, the Packet Sequence is encrypted with the associated Content Key as follows.

- The encryption is done using C2-ECBC (the C2 cipher algorithm in C-CBC mode) with the Content Key as the encryption key.
- Each Packet Sequence starts a new C-CBC cipher chain.
- 160 bytes from the top of each Packet Sequence is not encrypted and the residual part is encrypted.

Encrypted Packet Sequences and un-encrypted Packet Sequences may coexist in one content stream.

Encryption of Packet Sequence

Table 3-7 shows the encrypted Packet Sequence.

Table 3-7 Encrypted Packet Sequence

	Bit Byte	7	6	5	4	3	2	1	0	
First ETS/TSTS Packet (RDI Packet)	0	(Data defined in SD Memory Card Specification, Part 15)								
	1									
	:									
	11									
	12	CPF		APSTB						CCI_Byte
	13	(Data defined in SD Memory Card Specification, Part 15)								
	:									
	159									
	160	E_CPF		E_APSTB						E_CCI_Byte
	161	(Data defined in SD Memory Card Specification, Part 15)								
	:									
	183									
	184	RDI_CHECK								
	:									
	191									
	192	Second ETS/TSTS Packet								
	193									
	:									
	383									
	:									
	(M-1)×192	M’th ETS/TSTS Packet (if present)								
	:									
	M×192-1									

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

Regarding CCI and APS, SD-SD Video devices uses these value in E_CCI_Bytes or CKI, although SD-Video device always uses E_CCI_Byte when the content is exported to SD-Video. When a content provider makes content or a device records content in this format, these fields shall be set carefully. Refer to the section 3.6

The APSTB field indicates the analog protection status of corresponding ETS/TSTS Packet. The CPF field indicates the copy control status of corresponding ETS/TSTS Packet as shown in Table 3-8.

Table 3-8 Indication of copy control status

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

The RDI_CHECK field stores 64-bit check value, it shall be equal to 0123456789ABCDEFh when E_CPF field are equal to 10b or 11b. Compliant Device shall check this field is set correctly in doing process. How Compliant Device checks this field is described in each process description.

3.6. Process Description for Video Profiles

This section describes Export to SD-Video and Reimport from SD-Video processes and complement of Recording, Copy and Playback processes in this book.

- Recording Process

Specifies how to record Content Key. Analog Sunset Token may be set.

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

Specifies how to copy Content Key and re-encrypt the Content. SD-SD Video content may be required to re-encryption.

- Playback Process

Specifies how to decrypt audiovisual content and check CCI information in the content if any.

- Export to SD-Video Process

Specifies how an exporting device stores a title key of SD-Video which is the same value as a Content Key on an SD Memory Card. Using this function, a user can playback the content in both SD-SD Video format and SD-Video format in the SD Memory Card. Note that the SD-SD Video content shall not be moved (LOCKED) during exporting to SD-Video because of avoidance with the situation that the copied content is made without copy process. For this function, although Content Key is exported to SD-Video and some cryptographically calculation is required, content itself can be transformed to SD-Video format without re-encryption.

- Reimport from SD-Video Process

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

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

In these processes, when a device updates a CKMG file, devices may update two or more CKIs from a CKMG at one process for the purpose of reducing the number of accessing a Protected Area. For example, in Exporting to SD-Video process, a device may export all or selected Content Key in a CKMG at one process.

3.6.1. Recording Process

In Recording Process, when there is an indication that Analog Sunset in accordance with the *CPRM/CPPM License Agreement* is required, the AST shall be set to 1b.

3.6.2. Playback Process

In Playback Process, devices shall use the E_APSTB for output of Compliance Rules when the devices use APSTB field for output. The device shall check whether or not the RDI_CHECK field in the RDI Packet is equal to 0123456789ABCDEFh, during playback. For this purpose of check, the device is allowed to use the APSTB for output of Compliance Rules with additionally check that the APSTB is equal to E_APSTB. If these checks above are failed, the device shall not playback this Packet Sequence.

In Playback Process, devices shall check the Analog Sunset Token. If the Analog Sunset Token is equal to '1b,' Analog Sunset shall be applied to the Decrypted CPRM Video Content of decrypted content in accordance with the *CPRM/CPPM License Agreements*.

3.6.3. Content Key Copy Process I (SD Memory Card to Host)

Copy process is controlled by Copy Count Control Information in CKI, but when the StrmCCI is 1b and the NRF is 0b, the copy of the CKI requires additional process to re-encrypt the associated encrypted content. Therefore the Trigger Bits for Copy/Move in the CKI shall be set to 1000b. Copy Process I for CKI which has such combination is required to not only copy the CKI but also generate a new Content Key and re-encrypt Content itself. In this process, following steps shall be done for re-encryption of Content before step (10) in Content Key Copy Process I described in *CPRM Specification: SD Memory Card Book SD-SD (Separate Delivery) Part* is done.

(1) Generate a new Content Key that has a secret unpredictable value.

(2) Securely re-encrypt the all of Packet Sequences in the source with the associated Content Key and the new Content Key as following steps:.

- Decrypt each Packet Sequence with the associated Content Key. If the CPF field in RDI Pack of the Packet Sequence is equal to 00b, this Packet Sequence is plain and does not need to decrypt.
- Check the corresponding RDI Packet from the SD Memory Card.
- If the RDI_CHECK field in the RDI Packet is not equal to 0123456789ABCDEFh, the packet shall not be copied.
- If the E_CPF field in the RDI Packet is equal to 11b, this Packet Sequence shall not be copied to the Host, that is, skip the copy of Packet Sequence and the process continues for next Packet Sequence.
- If the E_CPF field in the RDI Packet is equal to 00b, this Packet Sequence is copied as is and then continues for next Packet Sequence.
- If the E_CPF field in the RDI Packet is equal to 10b, or 01b, encrypt the Packet Sequence with the new Content Key.

  The process shall be aborted if all the E_CPF fields in RDI Packet in the processed Packet Sequences are equal to 11b.

(3) Securely write the new Content Key for the copied Packet Sequence to the Host.

3.6.4. Export to SD-Video Process

When the Current Export to SD-Video flag of a Content Key is set to 1b, the SD-SD Video Content is permitted to be stored in the same SD Memory Card as an SD-Video Content. In this process, Exporting Device shall check that all of Content Keys having the same Content ID as exported Content Key have not been already exported. How to export SD-SD Video Content to SD-Video format is out of this specification.

(1) Search the CKIs which has the same Content ID

The Exporting Device searches the all CKIs which have the same Content ID as exported CKI. How to search is described in SD Association, *SD Memory Card Specifications, Part 15: SD-SD (Separate Delivery) Specification, Version 1.0*.

(2) Determine the CKMG files and CKIs selected in step (1).

The Exporting Device determines the CKMG filenames and the CKIs selected in step (1).

(3) Read the CKMG files from the SD Memory Card.

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

Then, the Exporting Device checks the corresponding all of CKI Used flags in the temporary CKMG images. If either of them is equal to 0b, the process shall be aborted.

Otherwise, the Exporting Device obtains the selected CKIs in the temporary CKMG images.

(4) Determine the UKURMG files and UKUREs associated with SD-SD Video Content to be exported.

The Exporting Device shall execute (4.1) and (4.2) for each selected CKI.

(4.1) Obtain UKURE_SRN.

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

(4.2) Determine the UKURMG file and UKURE associated with the SD-SD Video Content to be exported.

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

$\boldsymbol{s} = (\boldsymbol{n} - 1) \times 250 + \boldsymbol{m}$ ($\boldsymbol{n}$: UKURMG file number, $\boldsymbol{m}$: UKURE number in a UKURMG)

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

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

(5) Read the UKURMG files from the SD Memory Card.

The Exporting Device shall execute following process for each UKURMG selected in previous step.

- The Exporting Device securely reads the ***n***th UKURMG file from the SD Memory Card using Secure Read Process described in *CPRM Specification: SD Memory Card Book SD-SD (Separate Delivery) Part* and holds it as the temporary UKURMG image. Then, The Exporting Device checks the ***m***th UKURE Used flag in the temporary UKURMG image. If it is equal to 0b, the process shall be aborted. Otherwise, The Exporting Device obtains the ***m***th UKURE in the temporary UKURMG image.

(6) Check the UKUREs in the temporary UKURMG images.

The Exporting Device decrypts the all of selected UKURE using the UKURE Decryption process and securely holds it as the decrypted UKURE images. The Exporting Device checks all of decrypted UKURE images as follows:

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

(7) Check the CKIs in the temporary CKMG image.

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

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

In this step, the Exporting Device shall check whether or not all of Content Keys having the same Content ID have been already exported. If either Content Key has been already exported, the Exported Device shall abort this process. In other words, only one Content Key among Content Keys having the same Content ID can be exported. In this step, if the all of checks are valid, the condition of export is confirmed. The following steps are described for how to set the parameters in CKI to be exported.

(8) Obtain the Exported Content Identifier.

The Exporting Device shall execute the step (1), (2) and (3) of Recording Process described in chapter 3, *CPRM SD Memory Card book SD-Video Part*. In this Recording Process, each field in the TKURE shall be set as follows:

- The Title Key is the same value of the Content Key.
- The Trigger bit is set to 00b
- UR_MCCNTRL is set to 00000000b.
- StrmCCI is set to the same value of StrmCCI in exported CKI.
- APSTB is set to the same value of APSTB in exported CKI.
- UR_C_STRTDATE, UR_C_ENDDATE, UR_I_STRTDATE and UR_I_ENDDATE are set to 000000h.
- UR_C_P_CNT and UR_I_P_CNT are set to 0000h.
- UR_SPAN is set to 000000h.

These parameters are described in *CPRM SD Memory Card book SD-Video Part*. After executing these processes, the Exporting Device finds out the exact place of exported Title Key. If the Exporting Device can not obtain the Title Key Type and TKURE number, then the process shall be aborted.

(9) Update the exported CKI in the temporary CKMG image.

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

- The Title Key Type is set to the value which corresponds to the place of Exported Title Key..
- The TKURE Number is set to the TKURE_SRN of the Title Key of exported content in SD-Video format.
- The Move Control Information field is set to the same value as that of the Current Move Control Information field.
- The Current Move Control Information field is set to 00b.

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

(10) Update the temporary UKURMG image to be associated to the exported CKI.

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

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

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

Exporting Device securely reads the updated UKURMG file from the SD Memory Card using the Secure Read Process and verifies that the update of the ***m***th UKURE in the UKURMG file has completed successfully.

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

(12) Start to Export to SD-Video

The Exporting Device exports the Content Key into the Title Key, and then executes the remained steps in Recording Process described in *CPRM SD Memory Card book SD-Video Part*.

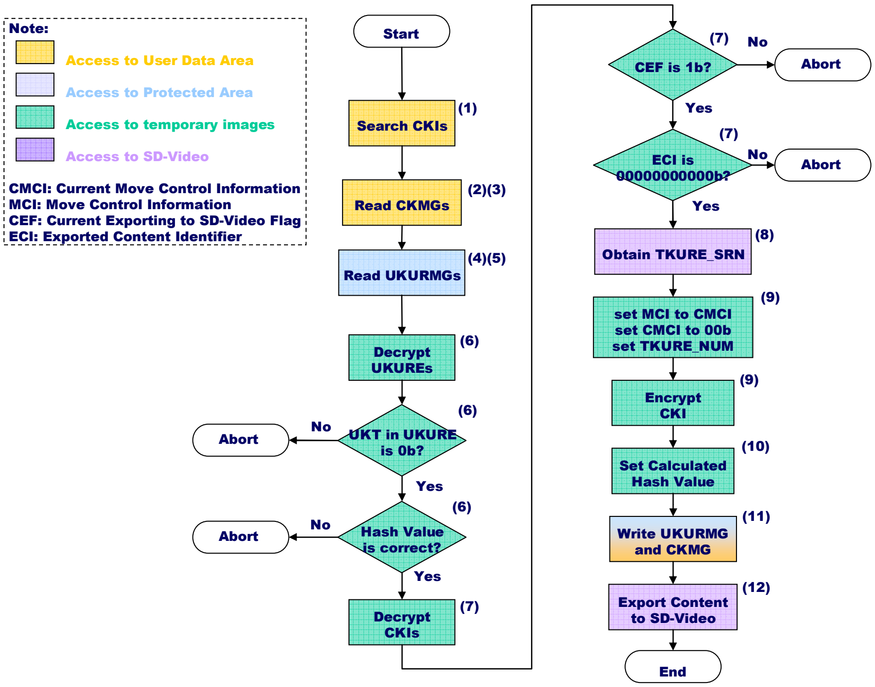

Figure 3-3 Flowchart of Export to SD-Video Process

3.6.5. Reimport from SD-Video Process

When the Current Export to SD-Video flag of an SD-SD Content is 1b and the TKURE Number is set to other than 00000000000b, the exported content can be reimported.

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

The Reimporting Device determines the CKMG filename and the CKI.

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

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

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

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

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

(3.1) Obtain UKURE_SRN.

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

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

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

$\boldsymbol{s} = (\boldsymbol{n} - 1) \times 250 + \boldsymbol{m}$ ($\boldsymbol{n}$: UKURMG file number, $\boldsymbol{m}$: UKURE number in a UKURMG)

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

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

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

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

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

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

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

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

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

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

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

- If the Check Value is not 0123456789ABCDEFh, the process shall be aborted.
- If the Trigger Bits for Video Profile Processes is not equal to 00h, the process shall be aborted.
- If the Current Export to SD-Video Flag is equal to 0b, then the process shall be aborted.
- If the TKURE Number is equal to 00000000000b, the process shall be aborted.

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

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

- The TKURE Number is set to 00000000000b.
- The Current Move Control Information field is set to the same value as that of the Move Control Information field.

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

(8) Update the temporary UKURMG image.

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

(9) Check the Title Key to be reimported.

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

- If the Title Key identified by the Exported Content Identifier in CKI associated with the Content Key to be reimported does not present, the process shall be aborted.

- If the value of Title Key identified in above is not identical to the value of Content Key to be reimported, the process shall be aborted.

(10) Delete the TKURE in the TKURMG file in SD Memory Card.

The Reimporting Device executes Erasing Process described in *CPRM Specification SD Memory Card SD-Video Part* to erase the exported Title Key.

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

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

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

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

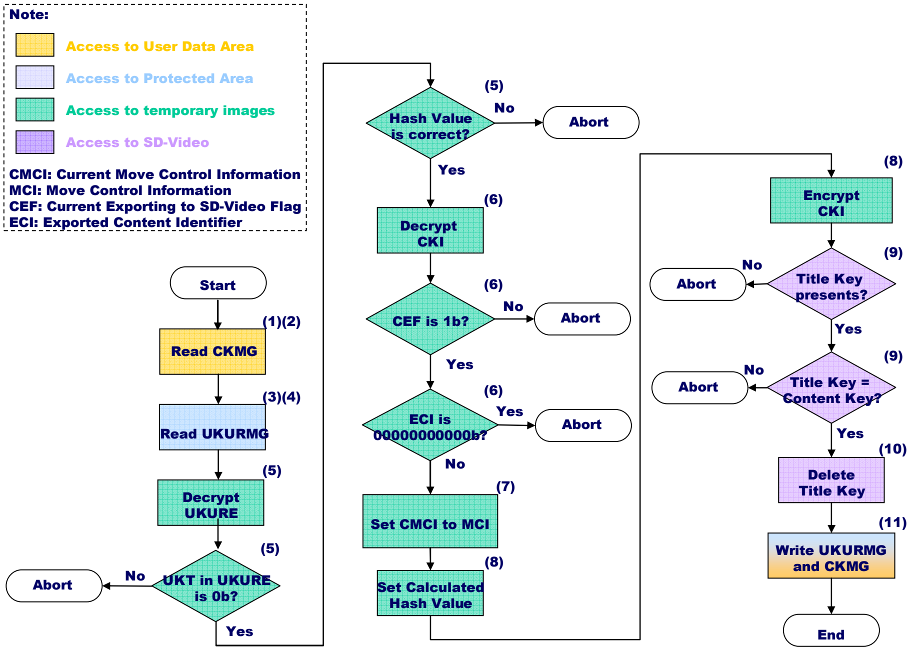

Figure 3-4 Flowchart of Reimport from SD-Video Process