

# Advanced Access Content System (AACCS)

## *HD DVD Recordable Book*

*Intel Corporation*

*International Business Machines Corporation*

*Matsushita Electric Industrial Co., Ltd.*

*Microsoft Corporation*

*Sony Corporation*

*Toshiba Corporation*

*The Walt Disney Company*

*Warner Bros.*

*Revision 0.91*

*February 17, 2006*

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. Intel Corporation, International Business Machines Corporation, Matsushita Electric Industrial Co., Ltd, Microsoft Corporation, Sony Corporation, Toshiba Corporation, The Walt Disney Company and Warner Bros. 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 subject to change under applicable license provisions.

Copyright © 2005-2006 by Intel Corporation, International Business Machines Corporation, Matsushita Electric Industrial Co., Ltd , Microsoft Corporation, Sony Corporation, Toshiba Corporation, The Walt Disney Company and Warner Bros. Third-party brands and names are the property of their respective owners.

### Intellectual Property

Implementation of this specification requires a license from AACSLA LLC.

### Contact Information

Please address inquiries, feedback, and licensing requests to AACSLA LLC:

- Licensing inquiries and requests should be addressed to [licensing@aacsla.com](mailto:licensing@aacsla.com).
- Feedback on this specification should be addressed to [comment@aacsla.com](mailto:comment@aacsla.com).

The URL for the AACSLA LLC web site is <http://www.aacsla.com>.

This page is intentionally left blank.

# Table of Contents

<b>PREFACE .....</b>	<b>III</b>
Notice .....	iii
Intellectual Property.....	iii
Contact Information.....	iii
<b>1 INTRODUCTION.....</b>	<b>11</b>
1.1 Purpose and Scope.....	11
1.2 Overview.....	11
1.3 Organization of this Document.....	11
1.4 References .....	11
1.5 Notation .....	12
1.6 Terminology .....	12
1.7 Abbreviations and Acronyms .....	12
<b>2 AACs COMPONENTS ON HD DVD-R/REWRITABLE MEDIA .....</b>	<b>13</b>
2.1 Introduction .....	13
2.2 Control Data.....	14
2.3 Media Key Block.....	15
2.4 Media Identifier .....	17
2.5 Protected Area and Binding Nonce.....	18
<b>3 PROTECTION OF HD DVD VIDEO RECORDING FORMAT .....</b>	<b>21</b>
3.1 Introduction .....	21
3.2 Stored Data Values for HD DVD Video Recording Format .....	21
3.2.1 Stored Data Values for VOB recording mode .....	21
3.2.2 Stored Data Values for SOB recording mode.....	27
3.3 Title Key .....	33
3.3.1 Title Key File.....	33
3.3.2 Encryption and Decryption of Title Key.....	37
3.3.3 Updating Title Key File .....	38

<b>3.4</b>	<b>Usage Rule</b> .....	<b>39</b>
3.4.1	Title Usage File.....	39
<b>3.5</b>	<b>Backup and Recovery</b> .....	<b>43</b>
3.5.1	Recovery for Title Key File .....	43
3.5.2	Backup and Recovery for other Files.....	44
<b>3.6</b>	<b>Content Encryption and Decryption for VOB</b> .....	<b>44</b>
<b>3.7</b>	<b>Content Encryption and Decryption for SOB</b> .....	<b>45</b>
<b>3.8</b>	<b>Secure Move</b> .....	<b>48</b>
<b>4</b>	<b>PROTECTION OF HD DVD INTEROPERABLE CONTENT</b> .....	<b>49</b>
<b>4.1</b>	<b>Introduction</b> .....	<b>49</b>
<b>4.2</b>	<b>Stored Data Values for Interoperable Content</b> .....	<b>49</b>
4.2.1	Stored Data Values for Interoperable Content .....	49
4.2.2	Protection Format for EVOB .....	50
<b>4.3</b>	<b>Title Key File</b> .....	<b>50</b>
<b>4.4</b>	<b>Usage Rule</b> .....	<b>50</b>
4.4.1	Title Usage File.....	50
<b>4.5</b>	<b>Content Decryption for Interoperable Content</b> .....	<b>50</b>
<b>5</b>	<b>PROTECTION OF HD DVD-VIDEO FORMAT</b> .....	<b>51</b>
<b>A</b>	<b>ADDITIONAL REQUIREMENT FOR CARRIAGE OF SRM</b> .....	<b>53</b>
<b>A.1</b>	<b>Introduction</b> .....	<b>53</b>
<b>A.2</b>	<b>SRM (System Renewability Message)</b> .....	<b>53</b>
A.2.1	SRM for DTCP.....	53
A.2.2	SRM for HDCP.....	53

## List of Figures

Figure 2-1 – Physical Layout of Common AACS Components on HD DVD-R/Rewritable Media .....	13
Figure 2-2 – Structure of BCA and Lead-in Area of an HD DVD-R/Rewritable media .....	14
Figure 2-3 – Structure of a Control Data Zone .....	15
Figure 2-4 – Structure of a Data Segment in a Control Data Zone.....	15
Figure 2-5 – Example of storing MKB on Lead-in Area of HD DVD-R/Rewritable media .....	16
Figure 2-6 – Data frame configuration .....	18
Figure 3-1 – Example of SOB and Title Key .....	47

This page is intentionally left blank.

## List of Tables

Table 2-1 – Format of Copyright Protection Information.....	15
Table 2-2 – Format of BCA Record Containing the Media Identifier .....	17
Table 2-3 – Format of Media Identifier .....	17
Table 2-4 – Encoding of M-Type field in BCA.....	18
Table 2-5 – Protected Area Format.....	19
Table 2-6 – Binding Nonce storing location in Protected Area .....	19
Table 3-1 – Storage of AACCS components in M_VOB_GI .....	22
Table 3-2 – RDI pack .....	23
Table 3-3 – Status of CCI_SS in GCI PKT .....	24
Table 3-4 – Status of CCI in GCI PKT.....	24
Table 3-5 – Encoding of Primitive CCI field in GCI_PKT .....	25
Table 3-6 – Encoding of APSTB field in GCI_PKT .....	25
Table 3-7 – Encoding of ICT field in GCI_PKT .....	26
Table 3-8 – Encoding of DOT field in GCI_PKT .....	26
Table 3-9 – Encoding of Trusted Input field in GCI_PKT .....	26
Table 3-10 – Encrypted AV Pack .....	27
Table 3-11 – Storage of AACCS components in SOBI_GI .....	28
Table 3-12 – Encrypted Packet Group.....	29
Table 3-13 – Status of CCI_SS in Packet Group Header .....	30
Table 3-14 – Status of CCI in Packet Group Header.....	30
Table 3-15 – Encoding of Primitive CCI field in Packet Group Header .....	31
Table 3-16 – Encoding of APSTB field in Packet Group Header .....	31
Table 3-17 – Encoding of ICT field in Packet Group Header .....	32
Table 3-18 – Encoding of DOT field in Packet Group Header.....	32
Table 3-19 – Encoding of Trusted Input field in Packet Group Header .....	32
Table 3-20 – Format for VOB Title Key File.....	34
Table 3-21 – Format for SOB Title Key File.....	36
Table 3-22 – Format for VOB Title Usage File.....	40
Table 3-23 – Format for SOB Title Usage File .....	41
Table 3-24 – Format for Usage Rule .....	42
Table 3-25 – Encoding of UR_FLG field in Usage Rule .....	42
Table 3-26 – Encoding of DOT field in Usage Rule .....	42
Table 3-27 – Stored value of RDI pack .....	45
Table 4-1 – Storage of AACCS components in VTS_EVOBI.....	49

This page is intentionally left blank.

# Chapter 1

## Introduction

### 1 Introduction

#### 1.1 Purpose and Scope

The Advanced Access Content System (AACS) specification defines an advanced, robust and renewable method for protecting audiovisual entertainment content, including high-definition content. The specification is organized into several “books”. The *Introduction and Common Cryptographic Elements* book describes the overall goals of AACS and defines cryptographic procedures that are common among its various defined uses. The *Recordable Video* book defines common details for using the system to protect audiovisual content transferred to portable/removable recordable storage media such as optical discs. This document (the *HD DVD Recordable Book*) specifies additional details for using the system to protect audiovisual content distributed on HD DVD-R/Rewritable media.

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 AACS LA is responsible for establishing and administering the content protection system based in part on this specification.

#### 1.2 Overview

In the *HD DVD Recordable Book*, the following procedures of Content Encryption and Decryption are described that are required to protect AACS recordable video content.

This document is provided as a detailed description of procedures and data structures that are specified for the use of the AACS technology on HD DVD-R/Rewritable media.

#### 1.3 Organization of this Document

This document is organized as follows:

- Chapter 1 provides an introduction and overview.
- Chapter 2 describes the AACS Components on HD DVD-R/Rewritable media.
- Chapter 3 describes HD DVD Video Recording (HD DVD-VR) specific procedures for encryption and decryption of AACS video content on HD DVD-R/Rewritable media.
- Chapter 4 describes Interoperable Content specific procedures for encryption and decryption of AACS video content on HD DVD-R/Rewritable media.
- Chapter 5 describes HD DVD-Video specific procedures for encryption and decryption of AACS video content on HD DVD-R/Rewritable media.

#### 1.4 References

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

AACS LA, *License agreement*

AACS LA, *AACS Introduction and Common Cryptographic Elements*

AACS LA, *AACS Recordable Video Book*

DVD Forum, *DVD Specifications for High Density Rewritable Disc, Part 1: Physical Specifications Version 1.0*

DVD Forum, *DVD Specifications for High Density Rewritable Disc, Part 2: File System Specifications Version 1.0*

DVD Forum, *DVD Specifications for High Density Recordable Disc, Part 1: Physical Specifications Version 1.0*

DVD Forum, *DVD Specifications for High Density Recordable Disc, Part 2: File System Specifications Version 1.0*

DVD Forum, *DVD Specifications for High Definition VIDEO RECORDING, Version 1.0*

DVD Forum, *DVD Specifications for High Definition VIDEO, Version 1.0*

## 1.5 Notation

In this document, the following terms are changed to upper case and have the same meaning as defined in the DVD Forum.

- Control Data Section: Control data section
- Control Data Zone: Control data zone
- Copyright Data Section: Copyright data section
- Copyright Protection Information: Copyright Protection information
- Copyright Protection System Use Section: Copyright protection system use section
- Data Segment: Data segment
- Physical Sector: Physical sector

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.

## 1.6 Terminology

**Content Key:** A Content Key is a key to encrypt and decrypt content.

**Packet Group:** A Packet Group consists of a Packet Group Header and multiple pairs of a Packet Arrival Time Stamp (PATS) and a MPEG-TS Packet.

## 1.7 Abbreviations and Acronyms

APSTB	Analog Protection System Trigger Bits
AV	Audio-Visual
BCA	Burst Cutting Area
CCI	Copy Control Information
CGMS	Copy Generation Management System
DVD	Digital Versatile Disc
EPN	Encryption Plus Non-assertion
ID	Identifier
lsb	Least Significant Bit
LSN	Logical Sector Number
MKB	Media Key Block
MPEG	Moving Picture Experts Group
msb	Most Significant Bit
PSN	Physical Sector Number

# Chapter 2

## AACCS Components on HD DVD-R/Rewritable Media

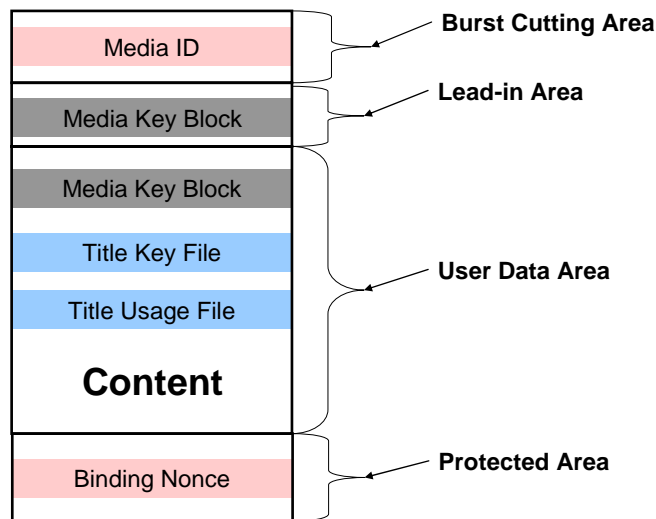
### 2 AACCS Components on HD DVD-R/Rewritable Media

#### 2.1 Introduction

This chapter specifies the location and format details of the AACCS common components to this *HD DVD Recordable Book*. The HD DVD-R/Rewritable format is the subject of a license from the DVD Forum, which also publishes specifications describing the format in detail (see the corresponding references in Section 1.4):

- DVD Specifications for High Density Recordable Disc, Part 1: Physical Specifications
- DVD Specifications for High Density Rewritable Disc, Part 1: Physical Specifications
- DVD Specifications for High Density Recordable Disc, Part 2: File System Specifications
- DVD Specifications for High Density Rewritable Disc, Part 2: File System Specifications

This chapter assumes the reader is familiar with the HD DVD-R/Rewritable formats, and focuses on those aspects of the format that are relevant to AACCS protection. Figure 2-1 gives an overview of the locations of AACCS related components on HD DVD-R/Rewritable media. Figure 2-2 presents the structure of the BCA and the Lead-in area of an HD DVD-R/Rewritable media. The details are provided in subsequent sections.



**Figure 2-1 – Physical Layout of Common AACCS Components on HD DVD-R/Rewritable Media**

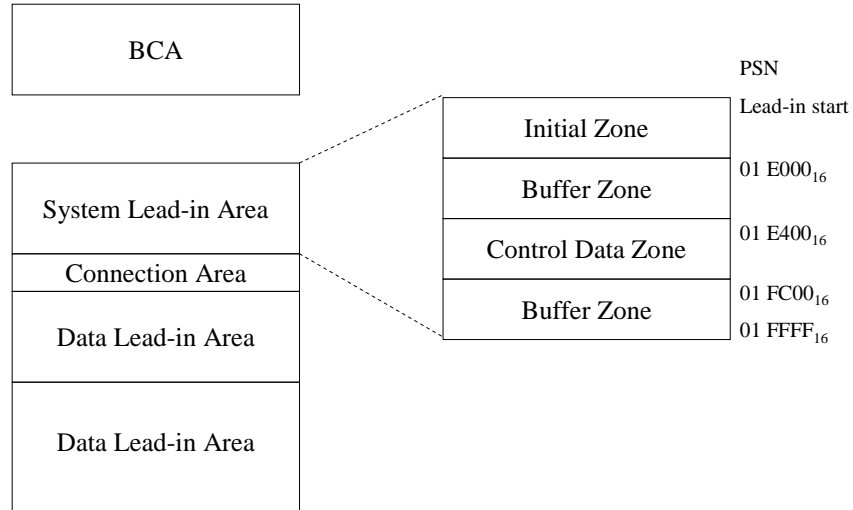
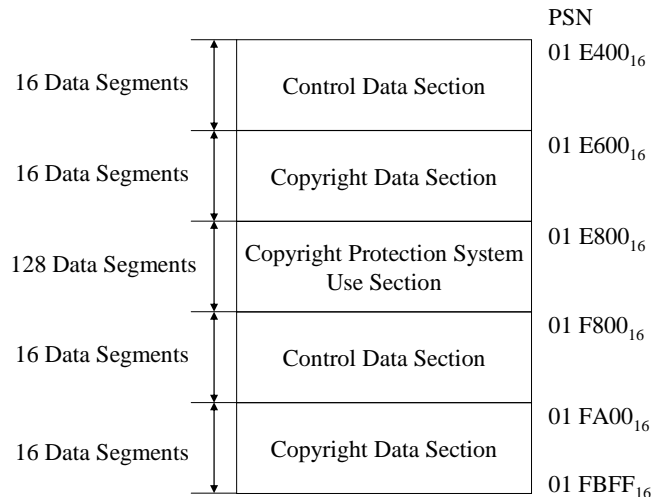


Figure 2-2 – Structure of BCA and Lead-in Area of an HD DVD-R/Rewritable media

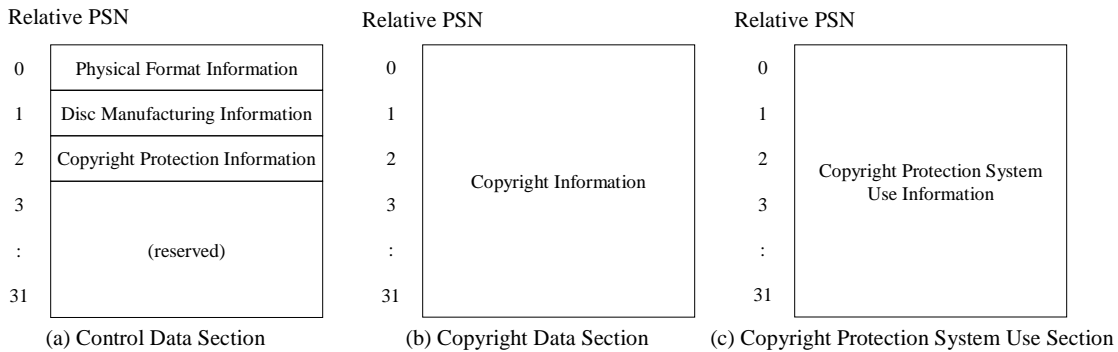
## 2.2 Control Data

A Control Data indicating that AACS is applied to the media is stored in a Control Data Zone of the HD DVD-R/Rewritable media. Figure 2-3 presents the structure of the Control Data Zone. The Control Data Zone has 2 Control Data Sections, 2 Copyright Data Sections, and a Copyright Protection System Use Section. Each Control Data Section is comprised of 16 Data Segments. The contents of the first Data Segment in a Control Data Section or a Copyright Data Section are repeated 16 times. Figure 2-4 shows data structure of each Data Segment which is composed of 32 Physical Sectors. The third Physical Sector in each Data Segment of a Control Data Section contains the Copyright Protection Information. Table 2-1 shows the format of the Copyright Protection Information. A 1-byte Copyright Protection System Type value shall be set to 01<sub>16</sub> in order to indicate that AACS is applied to the media. The Read-Only MKB Packs field denotes the number of MKB Packs, which is calculated by dividing Read-Only MKB data bytes by 32,768, counting fractions as one. All bytes reserved for Copyright Protection System Use field shall be set to 00<sub>16</sub>.

The Copyright Data Section can contain copyright data or the data of the Copyright Data Section shall be set to 00<sub>16</sub>.



**Figure 2-3 – Structure of a Control Data Zone**



**Figure 2-4 – Structure of a Data Segment in a Control Data Zone**

**Table 2-1 – Format of Copyright Protection Information**

Bit	7	6	5	4	3	2	1	0
Byte 0	Copyright Protection System Type: 01 <sub>16</sub>							
1 : 31	reserved							
32	Read-Only MKB Packs							
33 : 2047	reserved for Copyright Protection System Use							

### 2.3 Media Key Block

Each HD DVD-R/Rewritable media that contains content encrypted by AACS shall contain at least one Media Key Block (MKB) for encrypting and decrypting content on the media.

A Read-Only MKB shall be recorded 8 times by the media manufacturer in the Copyright Protection System Use Section of the Control Data Zone (refer to Figure 2-4). The Copyright Protection System Use Section is divided into 8 portions. Each portion consists of 16 Data Segments. Every portion shall contain the same Read-Only MKB. The MKB is recorded on the portion as shown in Figure 2-5. The size of the Read-Only MKB shall be stored in Byte32 of the Copyright Protection Information as shown in Table 2-1. The maximum size of the MKB is 1 MB. If the size of the MKB is less than 1 MB, then the last MKB Pack may end with unused bytes, which shall be zero-filled.

HD DVD-R/Rewritable media may have a Read/Write MKB which is updated by the recording devices and it shall be stored in the file “MKBRecordable.aacs” located in the “/AACS” directory of the Data Area.

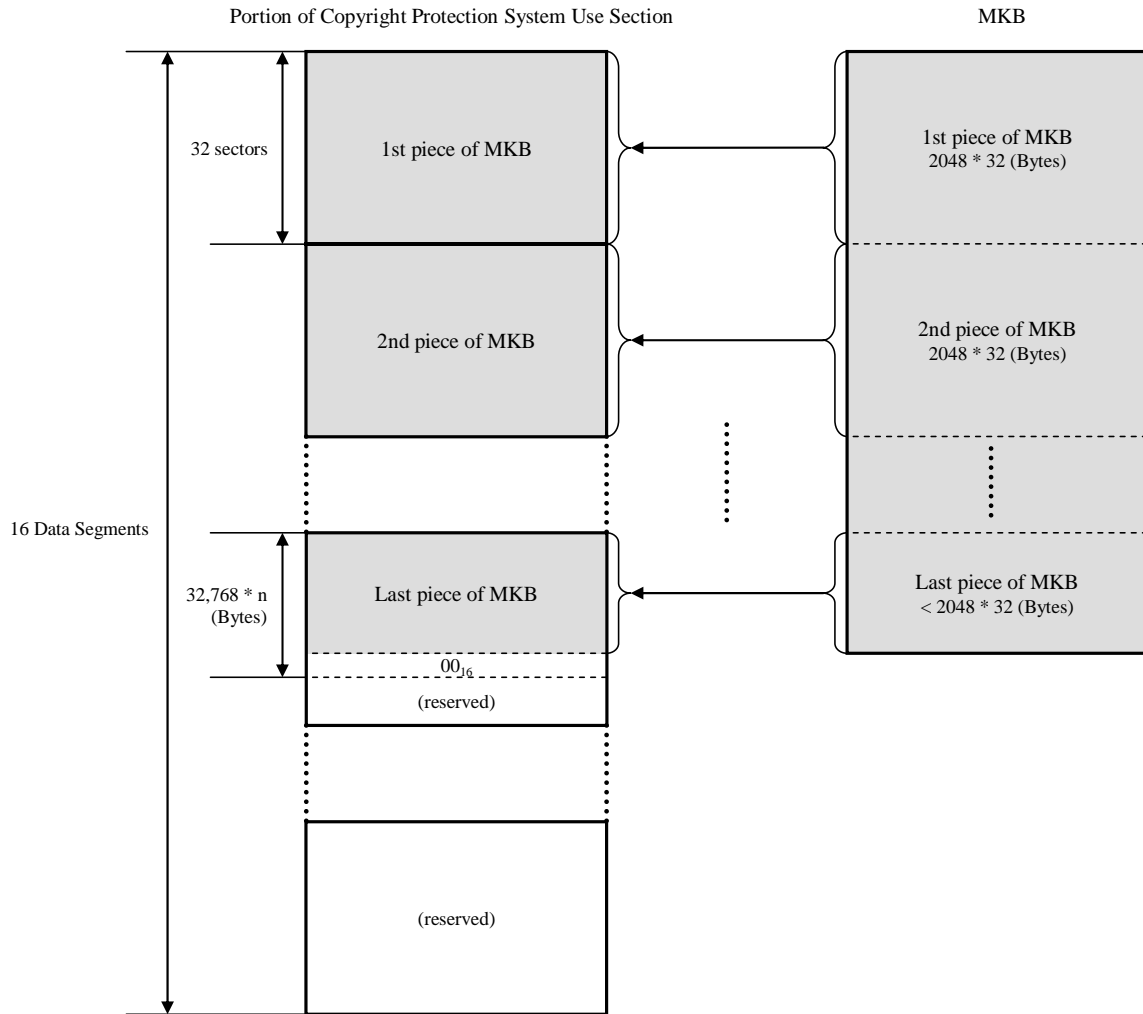


Figure 2-5 – Example of storing MKB on Lead-in Area of HD DVD-R/Rewritable media

## 2.4 Media Identifier

AACS compliant HD DVD-R/Rewritable media shall contain a 128-bit Media Identifier which is recorded in the Burst Cutting Area (BCA) by the media manufacturer with format as shown in Table 2-2

**Table 2-2 – Format of BCA Record Containing the Media Identifier**

Bit	7	6	5	4	3	2	1	0
Byte 0	(msb) BCA Record ID: 1004 <sub>16</sub> (lsb)							
1								
2	Version: 10 <sub>16</sub>							
3	Data Length: 10 <sub>16</sub>							
4	(msb) Record Data: Media Identifier (lsb)							
:								
19								

The BCA can contain multiple, contiguous blocks of data called BCA Records. The information of each BCA Record exists for different use which begins with a 2-byte Application ID field identifying the Record’s use, followed by a 1-byte Version field, followed by a 1-byte Data Length field indicating the length, in bytes, of the remaining data in the Record. It is better to assume this BCA Record is not a fixed location or is not a fixed size and also the Application ID such as BCA Record ID and Data Length fields may not be used for data search information of the next BCA Record.

Media Identifier consists of Licensee ID, M-Type and Serial Number as shown in Table 2-3.

**Table 2-3 – Format of Media Identifier**

Bit	7	6	5	4	3	2	1	0
Byte 4	(msb) Licensee ID (lsb)							
5								
6	M-Type	reserved						
7								
8	(msb) Serial Number (lsb)							
:								
19								

Licensee ID field indicates the value of Licensee ID assigned by AACS LA. Each licensed manufacturer of recordable media will be assigned a unique Licensee ID.

M-Type field indicates the type of the media as shown in Table 2-4. When the media is write-once media, M-Type field shall be set to ‘0’. The licensed recorder may use this value to distinguish between write-once media and rewritable media.

Reserved field shall be filled with ‘0’.

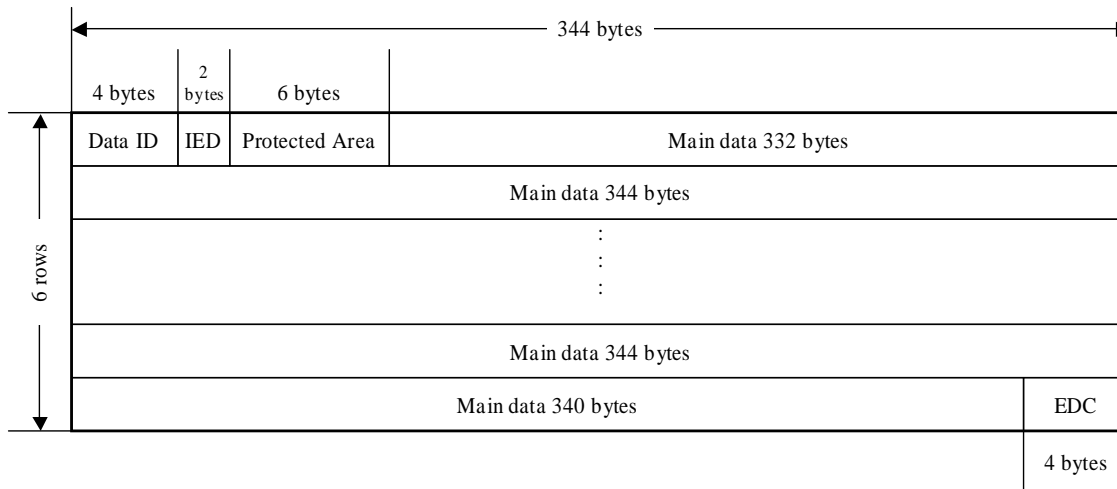
**Table 2-4 – Encoding of M-Type field in BCA**

M-Type	Media type
0	Write-once media
1	Rewritable media

Serial Number field indicates the unique 96-bit value to identify each piece of media assigned by each licensed manufacturer.

## 2.5 Protected Area and Binding Nonce

A Binding Nonce is stored in Protected Area of a Data Area. Figure 2-6 presents the configuration of a Data Frame whose data is stored in a Physical Sector. A 6-byte Protected Area is prepared for each Data Frame. Table 2-5 shows the format of a Protected Area. The first 4 bytes of a Protected Area are used for a piece of a 16-byte Binding Nonce and the latter 2 bytes of a Protected Area are reserved and shall be set to 0000<sub>16</sub>. Table 2-6 shows the location to store a 16-byte Binding Nonce that shall be stored in the Protected Area of 4 continuous Logical Sectors. The correspondence between a Physical Sector and a Logical Sector is described in the *HD DVD-R/Rewritable Part 2* book. The location of the Logical Sectors for storing a piece of a Binding Nonce is described in Section 3.3.1. All bytes of the Protected Area which does not contain a piece of a Binding Nonce shall be set to 00<sub>16</sub>.



**Figure 2-6 – Data frame configuration**

**Table 2-5 – Protected Area Format**

Byte	Bit	7	6	5	4	3	2	1	0
0		(msb) 4 bytes of a 16-byte Binding Nonce (lsb)							
1									
2									
3									
4		reserved							
5									

**Table 2-6 – Binding Nonce storing location in Protected Area**

LSN	Protected Area					
	0	1	2	3	4	5
N	1st 4 bytes of a 16-byte Binding Nonce			reserved		
N+1	2nd 4 bytes of a 16-byte Binding Nonce			reserved		
N+2	3rd 4 bytes of a 16-byte Binding Nonce			reserved		
N+3	4th 4 bytes of a 16-byte Binding Nonce			reserved		

This page is intentionally left blank.

# Chapter 3

## Protection of HD DVD Video Recording Format

### 3 Protection of HD DVD Video Recording Format

#### 3.1 Introduction

The general approach for encryption and decryption of recordable video content protected by AACS is specified in Chapter 3 of the *Recordable Video* book. This chapter describes the additional details of that approach that are specific to the use of AACS encryption and decryption with the HD DVD Video Recording Format.

The HD DVD Video Recording format is defined by the DVD Forum for real-time recording (on Rewritable, Recordable HD DVD media) of video with associated audio, including self-encoded content and digital broadcast content. The HD DVD Video Recording format is the subject of a license from the DVD Forum, which also publishes a specification describing the format in detail (see the corresponding reference in Section 1.4).

- DVD Specifications for High Definition VIDEO RECORDING

The following three types of recording modes are supported in the HD DVD Video Recording Format.

- Recording mode for Video Object (VOB)
- Type A recording mode for Stream Object (SOB)
- Type B recording mode for Stream Object (SOB)

The detailed usages of each recording type are described in the above specification.

#### 3.2 Stored Data Values for HD DVD Video Recording Format

For each media, the HD DVD Video Recording format uses management information files which contain the pointer information indicating the location of Encrypted Title Key in Title Key File and also the location of Usage Rule in Title Usage File. HR\_MANGR.IFO is the main navigation file, and every HD DVD Video Recording Media has this file accompanying content.

##### 3.2.1 Stored Data Values for VOB recording mode

In the case of VOB recording mode, the management information file named HR\_MANGR.IFO is used for navigation which contains some Movie VOB General Information (M\_VOB\_GI) for each VOB. One M\_VOB\_GI describes the information associated with one VOB. Part of M\_VOB\_GI is prepared for storing the pointer information to indicate the location of Encrypted Title Key in VOB Title Key File and the location of Usage Rule in VOB Title Usage File as shown in Table 3-1.

**Table 3-1 – Storage of AACCS components in M\_VOB\_GI**

Bit Byte	7	6	5	4	3	2	1	0
0 : 23	(Data defined in HD DVD-VR specification)							
24	(msb) Copy Protection Pointer (lsb)							
25								
26	(msb) reserved (lsb)							
27								
28 : 31	(Data defined in HD DVD-VR specification)							

Copy Protection Pointer is the pointer information to indicate the location of Encrypted Title Key and Media ID MAC within VOB Title Key File. Copy Protection Pointer also indicates the location of Usage Rule within VOB Title Usage File. Copy Protection Pointer takes a value between 1 and 1998, if valid Encrypted Title Key and valid Usage Rule exist. The Copy Protection Pointer field shall be zero provided that Encrypted Title Key for the VOB does not exist. If the value of the Copy Protection Pointer is zero, the content associated with the VOB shall not be encrypted.

For example, if the value of a Copy Protection Pointer is 3, the third record in VOB Title Key File is just the associated Encrypted Title Key for the VOB and the third record in VOB Title Usage File is the Usage Rule for the VOB.

2 bytes of reserved field following Copy Protection Pointer shall be set to zero.

In the case of VOB recording mode, the HD DVD Video Recording format stores content stream in stream data file. Content stream data flows as a sequence of packs of which each pack has different information depending on the pack type, including Real-time Data Information (RDI) packs which carry General Control Information and Real-time Data Information, Video packs, Audio packs, and Sub-picture packs which carry audio-visual content, and are referred to generically in this chapter as AV Packs. The size of each pack is 2048 bytes.

The RDI packs occur periodically within content stream (with presentation times at least 0.4 seconds and at most 1.001 seconds apart) and are used to carry various types of information about the stream. The RDI packs shall not be encrypted. Table 3-2 shows a structure of RDI pack which comprises a pack header, a system header, a General Control Information packet (GCI\_PKT) and a Real-time Data Information packet (RDI\_PKT).

The data field values in a given RDI pack apply to subsequent AV Packs in the recorded content stream, up to the occurrence of the next RDI pack or the end of the stream. Some data field values may change from one RDI pack to another.

**Table 3-2 – RDI pack**

		Bit Byte	7	6	5	4	3	2	1	0	
<b>GCL_PKT</b>		<b>0</b> : <b>40</b>	(Data defined in HD DVD-VR specification)								
		<b>41</b> : <b>59</b>	(Data defined in HD DVD-VR specification)								
	<b>CPI (Content Protection Information)</b>		<b>60</b>	KEY_VF	reserved						
			<b>61</b>	(msb)	Copy Protection Pointer						(lsb)
			<b>62</b>								
			<b>63</b> : <b>67</b>	reserved							
			<b>68</b>	UR_VF	(msb)	reserved					
			<b>69</b>								(lsb)
			<b>70</b>	(msb)	CCL_SS						(lsb)
			<b>71</b>								
			<b>72</b>	(msb)	CCI						(lsb)
			<b>73</b>								
		<b>74</b> : <b>75</b>	reserved								
		<b>76</b> : <b>303</b>	(Data defined in HD DVD-VR specification)								
		<b>304</b> : <b>2047</b>	(Data defined in HD DVD-VR specification)								

The usage of KEY\_VF field is defined in the *AACS HD DVD and DVD Pre-recorded Book*. In the case of VOB recording mode, KEY\_VF field shall be set to 10<sub>2</sub>.

The Copy Protection Pointer field indicates the location of Encrypted Title Key and Media ID MAC within VOB Title Key File. The Copy Protection Pointer also indicates the location of Usage Rule. If the value of the Copy Protection Pointer is zero, the associated AV Packs shall not be encrypted.

The usage of UR\_VF field is defined in the *AACS HD DVD and DVD Pre-recorded Book*. In the case of VOB recording mode, UR\_VF field shall be set to 1<sub>2</sub>.

CCI\_SS field indicates the status of each CCI. Table 3-3 shows the status of CCI\_SS field.

**Table 3-3 – Status of CCI\_SS in GCI PKT**

Bit Byte	7	6	5	4	3	2	1	0
70	P-CCI Valid	APS Valid	ICT Valid	DOT Valid	_Source Valid	T-Input Valid		
71	reserved							

Each bit of CCI\_SS shall be set to 1 if corresponding information of the status of CCI is valid or exists, otherwise the field shall be set to 0.

CCI field indicates the copy control status of corresponding AV Packs. Table 3-4 shows the status of CCI field.

**Table 3-4 – Status of CCI in GCI PKT**

Bit Byte	7	6	5	4	3	2	1	0
72	Primitive CCI			APSTB			ICT	DOT
73	_Source	Trusted Input	reserved					

A licensed recorder shall set the CCI based on the characteristics of the content stream. Currently, Primitive CCI, APSTB, ICT, DOT, Source and Trusted Input are defined.

Table 3-5 shows the encoding of Primitive CCI field.

**Table 3-5 – Encoding of Primitive CCI field in GCI\_PKT**

Primitive CCI	Content Status
000 <sub>2</sub>	Copy Freely
100 <sub>2</sub>	Copy One Generation
010 <sub>2</sub>	No More Copies
110 <sub>2</sub>	Copy Never
011 <sub>2</sub>	Protection using AACS, but copy control restrictions not asserted without redistribution (EPN)
other combinations	reserved

Input CGMS value shall be properly updated when the associated stream is recorded. When content stream with "Copy One Generation" is inputted, Primitive CCI value shall be updated to "No More Copies". Any content stream with "No More Copies" shall not be recorded.

When content stream with Copy Freely is input, the licensed recorder shall set the Primitive CCI field corresponding to that content in the recorded stream to 000<sub>2</sub>, and shall not encrypt the AV Data corresponding to the AV Packs. For content recorded with AACS protection, the licensed recorder shall set the Primitive CCI field corresponding to that content in the recorded stream to 100<sub>2</sub>, 010<sub>2</sub> or 011<sub>2</sub>, and shall encrypt all of the corresponding AV Packs as described in Section 3.5. When P-CCI Valid field in CCI\_SS is set to '0', Primitive CCI field shall be filled with '0'.

When no copies of AACS protected content are to be permitted, the Primitive CCI field corresponding to that content in the recorded stream shall be set to 010<sub>2</sub>. Where copy control restrictions are not asserted with respect to such protected content, the Primitive CCI field shall be set to 011<sub>2</sub>.

The APSTB field indicates the status of the analog protection of corresponding AV Packs, as shown in Table 3-6. When APS Valid field in CCI\_SS is set to '0', APSTB field shall be filled with '0'.

**Table 3-6 – Encoding of APSTB field in GCI\_PKT**

APSTB	Content Status
000 <sub>2</sub>	APSTB is OFF
001 <sub>2</sub>	Type 1 of APS1 is ON
010 <sub>2</sub>	Type 2 of APS1 is ON
011 <sub>2</sub>	Type 3 of APS1 is ON
110 <sub>2</sub>	APS2 is ON
111 <sub>2</sub>	APS2 is ON
other combinations	reserved

Input APSTB value shall be properly set when the associated content stream is recorded.

ICT field indicates the status of Image Constraint Token information of corresponding AV Packs, as shown in Table 3-7. When ICT Valid field in CCI\_SS is set to '0', ICT field shall be set to '0'.

**Table 3-7 – Encoding of ICT field in GCI\_PKT**

ICT	Content Status
0	High Definition Analog Output in High Definition Analog Form
1	High Definition Analog Output in the form of Constrained Image

Input ICT value shall be properly set when the associated content stream is recorded.

The definition and usage of Source Valid field and Source field are specified in HD DVD-VR specification.

DOT indicates the status of Digital Only Token information of corresponding AV Packs, as shown in Table 3-8. When DOT Valid field in CCI\_SS is set to '0', DOT field shall be set to '0'.

**Table 3-8 – Encoding of DOT field in GCI\_PKT**

DOT	Content Status
0	Decrypted outputs are permitted for all approved outputs
1	Decrypted outputs are permitted only for approved digital outputs

Trusted Input indicates the status of Trusted Input information of corresponding AV Packs, as shown in Table 3-9. When T-Input Valid field in CCI\_SS is set to '0', Trusted Input field shall be set to '0'.

**Table 3-9 – Encoding of Trusted Input field in GCI\_PKT**

Trusted Input	Content Status
0	Non Trusted Input
1	Trusted Input

All bytes reserved for CPI field shall have a value of zero.

Table 3-10 shows an encrypted AV Pack.

For VOB recording format, a 2-bit PES\_scrambling\_control field is set to 11<sub>2</sub> in an encrypted AV Pack, and to 00<sub>2</sub> in an unencrypted AV Pack. The use of the 32-bit Title Key Data (D<sub>tk</sub>) is described in Section 3.5. The first 128 bytes of the pack are unencrypted. The final 1920 bytes, referred to as the Encrypted Content, are encrypted as described in Section 3.5. Before encryption (or after decryption), those same 1920 bytes are referred to as Unencrypted Content.

**Table 3-10 – Encrypted AV Pack**

		Bit	7	6	5	4	3	2	1	0	
		Byte									
Unencrypted Portion (128 bytes)	0 : 19	(Data defined in HD DVD-VR specification)									
	20				PES_scrambling _control						
	21 : 83	(Data defined in HD DVD-VR specification)									
	84 : 87	Title Key Data (D <sub>tk</sub> )									
	88 : 127	(Data defined in HD DVD-VR specification)									
Encrypted Portion (1920 bytes)	128 : 2047	Encrypted Content									

### 3.2.2 Stored Data Values for SOB recording mode

In the case of SOB recording mode, the management information file named HR\_SFInn.SFI referred from HR\_MANGR.IFO is used.

In the case of SOB Type A recording mode, 'nn' is an application specific number defined in HD DVD-VR specification and is one of '01', '02', ..., 'FE', 'FF'.

In the case of SOB Type B recording mode, 'nn' takes a fixed value '00', and the name of the management information file is HR\_SFI00.SFI.

The HR\_SFInn.SFI file includes SOBI General Information (SOBI\_GI) for each SOB. One SOBI\_GI describes the information associated with one SOB. Part of SOBI\_GI is prepared for storing the pointer information to indicate the location of Encrypted Title Key in SOB Title Key File and the location of Usage Rule in SOB Title Usage Rule as shown in Table 3-11.

**Table 3-11 – Storage of AACS components in SOBI\_GI**

Bit Byte	7	6	5	4	3	2	1	0
0 : 57	(Data defined in HD DVD-VR specification)							
58	(msb)		Copy Protection Pointer				(lsb)	
59								
60	(msb)		reserved				(lsb)	
61								
62 : :	(Data defined in HD DVD-VR specification)							

Copy Protection Pointer is the pointer information to indicate the location of Encrypted Title Key and Media ID MAC within SOB Title Key File. Copy Protection Pointer also indicates the location of Usage Rule within SOB Title Usage File. Copy Protection Pointer takes a value between 1 and 1998, if valid Encrypted Title Key and valid Usage Rule exist. The Copy Protection Pointer field shall be zero provided that Encrypted Title Key for the SOB does not exist. If the value of the Copy Protection Pointer is zero, the content associated with the SOB shall not be encrypted.

For example, if the value of a Copy Protection Pointer is 3, the third record in SOB Title Key File is just the associated Encrypted Title Key for the SOB and the third record in SOB Title Usage File is the Usage Rule for the SOB.

2 bytes of reserved field following Copy Protection Pointer shall be set to zero.

In the case of SOB recording mode, the HD DVD Video Recording format stores content stream data in stream data files. Content stream data is structured as a sequence of 32Kbyte Packet Group, which consists of Packet Group Header, multiple pairs of Packet Arrival Time Stamp (PATS) and MPEG-TS Packet. Table 3-12 shows a structure of a Packet Group.

Each Packet Group can be divided into 2 parts, the first 144 bytes that are unencrypted and the remaining 32624 bytes, referred to as Encrypted Content, are encrypted as described in Section 3.6. Before encryption (or after decryption), those same 32624 bytes are referred to as Unencrypted Content.

**Table 3-12 – Encrypted Packet Group**

		Bit	7	6	5	4	3	2	1	0						
		Byte														
Unencrypted Portion (144 bytes)	Packet Group Header	CPI (Content Protection Information)	0	(Data defined in HD DVD-VR specification)												
			:													
			19													
			20	reserved												
			21													
			22	(msb)	Copy Protection Pointer						(lsb)					
			23													
			24	reserved												
			25													
			26	(msb)	CCI_SS						(lsb)					
			27													
			28	(msb)	CCI						(lsb)					
			29													
			30	reserved												
31																
32	(Data defined in HD DVD-VR specification)															
:																
127																
128									Title Key Data ( $D_{tk}$ )							
:																
135																
136	Unencrypted Content															
:																
143																
144	Encrypted Content															
:																
32767																

Copy Protection Pointer field indicates the location of Encrypted Title Key and Media ID MAC within SOB Title Key File to calculate the Title Key for the corresponding Packet Group. Copy Protection Pointer also indicates the location of Usage Rule within SOB Title Usage File. If the value of the Copy Protection Pointer is zero, the Packet Group shall not be encrypted.

CCI\_SS field indicates the status of each CCI. Table 3-13 shows the encoding of CCI\_SS field.

**Table 3-13 – Status of CCI\_SS in Packet Group Header**

Bit Byte	7	6	5	4	3	2	1	0
26	P-CCI Valid	APS Valid	ICT Valid	DOT Valid	_Source Valid	T-Input Valid		
27	reserved							

Each bit of CCI\_SS field shall be set to 1 if corresponding information of the status of CCI is valid or exists, otherwise the field shall be set to 0. Some CCI information is embedded in the content stream. When a licensed recorder supporting Type B recording mode for SOB records the stream, it shall set at least P-CCI as valid and set Primitive CCI value based on the characteristics of the content stream. Depending on the input method, the licensed recorder may treat some part of CCI as invalid.

CCI field indicates the copy control status of corresponding Packet Group. Table 3-14 shows the status of CCI field.

**Table 3-14 – Status of CCI in Packet Group Header**

Bit Byte	7	6	5	4	3	2	1	0
28	Primitive CCI			APSTB			ICT	DOT
29	_Source	Trusted Input	reserved					

A licensed recorder shall set the CCI based on the characteristics of the content steam. If the stream consists of multiple substreams with different CCI, the strictest CCI will be used. CCI field indicates the copy control status of corresponding Packet Group. Currently Primitive CCI, APSTB, ICT, DOT, Source and Trusted Input are defined.

Table 3-15 shows the encoding of Primitive CCI field.

**Table 3-15 – Encoding of Primitive CCI field in Packet Group Header**

Primitive CCI	Content Status
000 <sub>2</sub>	Copy Freely
100 <sub>2</sub>	Copy One Generation
010 <sub>2</sub>	No More Copies
110 <sub>2</sub>	Copy Never
011 <sub>2</sub>	Protection using AACS, but copy control restrictions not asserted without redistribution (EPN)
other combinations	reserved

Input CGMS value shall be properly updated when the associated stream is recorded. When content stream with "Copy One Generation" is input, Primitive CCI value shall be updated to "No More Copies". Any content stream with "No More Copies" shall not be recorded.

When content stream with Copy Freely is input, the licensed recorder shall set the Primitive CCI field corresponding to that content in the recorded stream to 000<sub>2</sub>, and shall not encrypt the AV Data corresponding to the Packet Group. For content recorded with AACS protection, licensed recorder shall set the Primitive CCI field corresponding to that content in the recorded stream to 100<sub>2</sub>, 010<sub>2</sub> or 011<sub>2</sub>, and shall encrypt all of the corresponding AV Data of the Packet Group as described in Section 3.6. When P-CCI Valid field in CCI\_SS is set to '0', Primitive CCI field shall be filled with '0'.

When no copies of AACS protected content are to be permitted, the Primitive CCI field corresponding to that content in the recorded stream shall be set to 010<sub>2</sub>. Where copy control restrictions are not asserted with respect to such protected content, the Primitive CCI field shall be set to 011<sub>2</sub>.

The APSTB field indicates status of the analog protection information of corresponding Packet Group, as shown in Table 3-16. When APS Valid field in CCI\_SS is set to '0', APSTB field shall be filled with '0'.

**Table 3-16 – Encoding of APSTB field in Packet Group Header**

APSTB	Content Status
000 <sub>2</sub>	APSTB is OFF
001 <sub>2</sub>	Type 1 of APS1 is ON
010 <sub>2</sub>	Type 2 of APS1 is ON
011 <sub>2</sub>	Type 3 of APS1 is ON
110 <sub>2</sub>	APS2 is ON
111 <sub>2</sub>	APS2 is ON
other combinations	reserved

Input APSTB value shall be properly set when the associated content stream is recorded.

ICT field indicates the status of Image Constraint Token information of corresponding Packet Group, as shown in Table 3-17. When ICT Valid field in CCI\_SS is set to '0', ICT field shall be set to '0'.

**Table 3-17 – Encoding of ICT field in Packet Group Header**

ICT	Content Status
0	High Definition Analog Output in High Definition Analog Form
1	High Definition Analog Output in the form of Constrained Image

Input ICT value shall be properly set when the associated content stream is recorded.

The definition and usage of Source Valid field and Source field are specified in HD DVD-VR specification.

DOT indicates the status of Digital Only Token information of corresponding Packet Group, as shown in Table 3-18. When DOT Valid field in CCI\_SS is set to '0', DOT field shall be set to '0'.

**Table 3-18 – Encoding of DOT field in Packet Group Header**

DOT	Content Status
0	Decrypted outputs are permitted for all approved outputs
1	Decrypted outputs are permitted only for approved digital outputs

The definition and usage of Title Key Data ( $D_{tk}$ ) is described in Section 3.6.

Trusted Input indicates the status of Trusted Input information of corresponding Packet Group, as shown in Table 3-19. When T-Input Valid field in CCI\_SS is set to '0', Trusted Input field shall be set to '0'.

**Table 3-19 – Encoding of Trusted Input field in Packet Group Header**

Trusted Input	Content Status
0	Non Trusted Input
1	Trusted Input

All bytes reserved for CPI field shall have a value of zero.

### 3.3 Title Key

#### 3.3.1 Title Key File

Encrypted Title Keys ( $K_{te}$ ) shall be stored in Title Key File. For backup purpose, three Title Key Files (TKF\_X, TKF\_Y, TKF\_Z) are defined in each Title Key File. Three Title Key Files are defined in Title Key File Set by 1 set. The Title Key File for VOB shall be stored in the file “HR\_V\_TKFx.aacs”, “HR\_V\_TKFy.aacs” and “HR\_V\_TKFz.aacs” located in the “/AACCS” directory. The Title Key File for SOB shall be stored in the file “HR\_Snn\_TKFx.aacs”, “HR\_Snn\_TKFy.aacs” and “HR\_Snn\_TKFz.aacs” located in the “/AACCS” directory. ‘nn’ takes the same value as the value used for the corresponding management file. For example, if an SOB is included in HR\_SFI01.SFI, the Encrypted Title Key for the SOB is stored in “HR\_S01\_TKFx.aacs”, “HR\_S01\_TKFy.aacs” and “HR\_S01\_TKFz.aacs”. Note that, when multiple HR\_SFI<sub>nn</sub>.SFI files exist in a single media, one Title Key File Set is defined for each management file.

Three Title Key Files for SOB and VOB have the same structure and the size of each Title Key File is 64K bytes.

Each HD DVD-R/Rewritable media which contains HD DVD Video Recording content protected by AACCS shall have at least one Title Key File Set. For clarification, when the media contains only VOB formatted content protected by AACCS, VOB Title Key File Set is required. When the media contains only SOB formatted content protected by AACCS, SOB Title Key File Set(s) is required. When the media contains both VOB and SOB formatted content protected by AACCS, at least two Title Key File Sets shall exist on the media. When multiple Title Key Files exist on a single media, each Title Key File has the Binding Nonce of a different value. It is recommended that each Title Key File among the same Title Key File Set is allocated in a different ECC block, because two of the three Title Key Files are necessary to decrypt Title Key.

Table 3-20 shows the structure of VOB Title Key File.

**Table 3-20 – Format for VOB Title Key File**

Byte	Bit	7	6	5	4	3	2	1	0
	0 : 11	(msb) VTKF_ID (lsb)							
	12 : 15	(msb) HR_VTKF_EA (lsb)							
	16 : 31	reserved							
	32 : 33	(msb) VERN (lsb)							
	34 : 127	reserved							
	128 : 143	(msb) Title Key File Generation (lsb)							
	144 : 159	(msb) Title Key File Nonce (lsb)							
Title Key Information (TKI)	160 : 175	(msb) Encrypted Title Key ( $K_{te}$ ) #1 (lsb)							
	176 : 191	(msb) Media ID MAC ( $MAC_{id}$ ) #1 (lsb)							
	192 : 64095	Encrypted Title Key, Media ID MAC (#2 .. #1998)							
	64096 : 65535	reserved							

Because the maximum number of VOBs in a single HD DVD-R/Rewritable media is defined as 1998, the maximum number of Encrypted Title Keys stored in the VOB Title Key File is also limited to 1998.

VTKF\_ID field indicates the 12-byte value to identify the VOB Title Key File. The value is set to “DVD\_HR\_V\_TKF” with character set code of ISO/IEC 646:1983 (a-characters).

HR\_VTKF\_EA field indicates the end address of the VOB Title Key File. Because the size of the VOB Title Key File is fixed to 64KB, this field is filled with the value of ‘65535’.

VERN field indicates the version number of the Title Key File, currently defined as the value of ‘0’.

Title Key File Generation indicates the generation number of the Title Key File. Title Key File Generation takes the same value among the same Title Key File Set. The detailed usage of Title Key File Generation is described in Section 3.5.1

Title Key File Nonce is the value of a 128-bit nonce. A licensed recorder shall be capable of generating a statistically unique (e.g., random) 128-bit nonce used to encrypt Title Key stored in other Title Key File of the same Title Key File Set. Title Key File Nonce takes different value within the same Title Key File Set. The detailed calculation method of Title Key is described in Section 3.3.2.

Title Key Information (TKI) consists of 1998 pairs of Encrypted Title Keys and Media ID MACs.

Encrypted Title Key is the value of a 128-bit Encrypted Title Key. The Encrypted Title Key of the number specified by the management file is stored in this field. The value which is encrypted ‘0’ by the Protected Area Key ( $K_{pa}$ ), Usage Rule filled with zero and Title Key File Nonce is defined as invalid.

Media ID MAC field is the value of a 128-bit Media ID MAC associated with the Title Key used to encrypt the VOB. The detailed calculation method of Media ID MAC is described in Chapter 3 of the *AACS Recordable Video* book.

All bytes of reserved field shall be set to  $00_{16}$ .

Table 3-21 shows the structure of SOB Title Key File.

**Table 3-21 – Format for SOB Title Key File**

	Bit Byte	7	6	5	4	3	2	1	0
	0 : 11	(msb) STKF_ID (lsb)							
	12 : 15	(msb) HR_STKF_EA (lsb)							
	16 : 31	reserved							
	32 : 33	(msb) VERN (lsb)							
	34 : 127	reserved							
	128 : 143	(msb) Title Key File Generation (lsb)							
	144 : 159	(msb) Title Key File Nonce (lsb)							
Title Key Information (TKI)	160 : 175	(msb) Encrypted Title Key ( $K_{te}$ ) #1 (lsb)							
	176 : 191	(msb) Media ID MAC ( $MAC_{id}$ ) #1 (lsb)							
	192 : 64095	Encrypted Title Key, Media ID MAC (#2 .. #1998)							
	64096 : 65535	reserved							

Because the maximum number of SOBs in a single HD DVD-R/Rewritable media is defined as 1998, the maximum number of Encrypted Title Keys stored in the SOB Title Key File is also limited to 1998.

STKF\_ID field indicates the 12-byte value to identify the SOB Title Key File. The value is set to "DVD\_S\_nn\_TKF" with character set code of ISO/IEC 646:1983 (a-characters). 'nn' takes the same value as the value use for the corresponding management file.

HR\_STKF\_EA field indicates the end address of the SOB Title Key File. Because the size of the SOB Title Key File is fixed to 64KB, this field is filled with the value of '65535'.

VERN field indicates the version number of the Title Key File, currently defined to as the value of '0'.

Title Key File Generation indicates the generation number of the Title Key File. Title Key File Generation takes the same value among the same Title Key File Set. The detailed usage of Title Key File Generation is described in Section 3.5.1

Title Key File Nonce is the value of a 128-bit nonce. A licensed recorder shall be capable of generating a statistically unique (e.g., random) 128-bit nonce used to encrypt Title Key stored in other Title Key File of the same Title Key File Set. The detailed calculation method of Title Key is described in Section 3.3.2.

Title Key Information (TKI) consists of 1998 pairs of Encrypted Title Keys and Media ID MACs.

Encrypted Title Key is the value of a 128-bit Encrypted Title Key. The Encrypted Title Key of the number specified by the management file is stored in this field. The value which is encrypted '0' by the Protected Area Key ( $K_{pa}$ ), Usage Rule filled with zero and Title Key File Nonce is defined as invalid.

Media ID MAC is the value of a 128-bit Media ID MAC associated with the Title Key used to encrypt the SOB. The detailed calculation method of Media ID MAC is described in Chapter 3 of the *AACS Recordable Video* book.

All bytes of reserved field shall be set to  $00_{16}$ .

For HD DVD Rewritable media, when the Title Key File is first created, a licensed recorder shall generate a statistically unique (e.g., random) 128-bit Title Key File Generation and a Title Key. And it shall initialize all remaining records of Encrypted Title Key filled with the value encrypted '0' by Protected Area Key. That is where the first Encrypted Title Key is stored in the Title Key File, one record of the Title Key File is filled with the Encrypted Title Key and the other 1997 records are filled with the value encrypted '0' by Protected Area Key.

When the licensed recorder stores the new Encrypted Title Key in the Title Key File, it searches the invalid field and overwrites with the new Encrypted Title Key. When the licensed recorder deletes the Title Key, it shall overwrite the value encrypted '0' by Protected Area Key.

For HD DVD-R media, when the Title Key File is first created, a licensed recorder shall generate a statistically unique (e.g., random) 128-bit Title Key File Generation, and it may generate additional Title Keys or it may store multiple records of Encrypted Title Key encrypted the same Title Key by the different Usage Rules in the Title Key File. All the remaining records of Encrypted Title Key shall be filled with the value encrypted '0' by Protected Area Key.

When a licensed recorder first makes the Title Key File, all Logical Sectors for the Title Key File shall be marked with Non-relocatable attribute. Because available size of each Protected Area where the Binding Nonce is stored is 4 bytes, 4 Physical Sectors (8 Kbytes) are necessary to store the Binding Nonce. The Binding Nonce shall be sequentially stored in the Protected Areas of the first 4 continuous Logical Sectors where the Title Key File is written and the Protected Areas in the latter Logical Sectors shall be filled with '0' as described in Section 2.5.

### 3.3.2 Encryption and Decryption of Title Key

Title Key File Set consists of three Title Key Files. Each Title Key File within the same Title Key File Set shall have the same value of Title Key. Each Protected Area Key ( $K_{pa}$ ) is encrypted by Media Key ( $K_m$ ) and

associated Binding Nonce. For each Title Key File, associated Binding Nonce (Binding Nonce\_X, Binding Nonce\_Y, Binding Nonce\_Z) within the same Title Key File Set takes different value. Each Title Key ( $K_t_X$ ,  $K_t_Y$ ,  $K_t_Z$ ) stored in each Title Key File (TKF\_X, TKF\_Y, TKF\_Z) shall be encrypted by its own Protected Area Key and Title Key File Nonce (TKFN) stored in other Title Key File (TKFN\_Z, TKFN\_X, TKFN\_Y) as follows:

$K_{pa\_X} = \text{AES-G}(K_m, \text{Binding Nonce\_X})$ ,  $K_{te\_X} = \text{AES-128E}(K_{pa\_X} \oplus \text{TKFN\_Z}, K_t \oplus \text{AES-H}(\text{Usage Rule}))$

$K_{pa\_Y} = \text{AES-G}(K_m, \text{Binding Nonce\_Y})$ ,  $K_{te\_Y} = \text{AES-128E}(K_{pa\_Y} \oplus \text{TKFN\_X}, K_t \oplus \text{AES-H}(\text{Usage Rule}))$

$K_{pa\_Z} = \text{AES-G}(K_m, \text{Binding Nonce\_Z})$ ,  $K_{te\_Z} = \text{AES-128E}(K_{pa\_Z} \oplus \text{TKFN\_Y}, K_t \oplus \text{AES-H}(\text{Usage Rule}))$

where AES-G represents a cryptographic one-way function based on the AES algorithm as defined in the *Introduction and Common Cryptographic Elements* book.

and AES-128E represents encryption by the AES cipher with the Electronic Codebook (ECB) mode as defined in the *Introduction and Common Cryptographic Elements* book

and AES-H represents a cryptographic one-way function based on the AES algorithm as defined in the *Introduction and Common Cryptographic Elements* book.

The process to decrypt Title Key is as follows:

$K_{pa\_X} = \text{AES-G}(K_m, \text{Binding Nonce\_X})$ ,  $K_t = \text{AES-128D}(K_{pa\_X} \oplus \text{TKFN\_Z}, K_{te\_X}) \oplus \text{AES-H}(\text{Usage Rule})$

where AES-G represents a cryptographic one-way function based on the AES algorithm as defined in the *Introduction and Common Cryptographic Elements* book.

and AES-128D represents decryption by the AES cipher with the Electronic Codebook (ECB) mode as defined in the *Introduction and Common Cryptographic Elements* book

and AES-H represents a cryptographic one-way function based on the AES algorithm as defined in the *Introduction and Common Cryptographic Elements* book.

### 3.3.3 Updating Title Key File

The general approach for updating the Title Key File is specified in Section 2.4 of the *Recordable Video* book. This section describes the additional procedures and details of that approach that are specific to HD DVD Video Recording Format.

When the Title Key File is modified or MKB is updated, the Binding Nonce and all the Title Key File Nonce within the same Title Key File Set shall be updated each time as described in Section 2.1 of the *Recordable Video* book. When updating Title Key File, a licensed recorder shall check Title Key File Generation of each Title Key File. If the values of the Title Key File Generation of three Title Key Files are the same, a licensed recorder shall update three Title Key Files. Otherwise, a licensed recorder shall recover Title Key File as described in Section 3.5 before updating.

The process to update Title Key File is as follows:

1. Decrypt all the Title Key(s)
2. Modify Title Key File
3. Update Title Key File Generation and Title Key File Nonce

Update Title Key File Generation to increment the value by 1 and regenerate three Title Key File Nonces

4. Re-encrypt all the Title Key(s) and store TKF\_X

Update the Binding Nonce\_X, re-encrypt all the Title Key(s) of TKF\_X, store TKF\_X with the Title Key File Generation and Title Key File Nonce\_Z on the media

5. Re-encrypt all the Title Key(s) and store TKF\_Y

Update the Binding Nonce, re-encrypt all the Title Key(s) of TKF\_Y, store TKF\_Y with the Title Key File Generation and Title Key File Nonce\_X on the media

6. Re-encrypt all the Title Key(s) and store TKF\_Z

Update the Binding Nonce, re-encrypt all the Title Key(s) of TKF\_Z, store TKF\_Z with the Title Key File Generation and Title Key File Nonce\_Y on the media

The process to update Title Key File when MKB is updated is as follows:

1. Rename existing Read/Write MKB

Read/Write MKB is stored in the file “MKBRecordable.aacs” located in the “/AACS” directory as described in Section 2.3. The Read/Write MKB is temporarily renamed “MKBRecordableBK.aacs” and located in the same directory.

2. Write new MKB

New MKB shall be stored in the file “MKBRecordable.aacs” located in the “/AACS” directory.

3. Update Title Key Files

Title Key shall be re-encrypted by the new Media Key ( $K_m$ ) calculated by the new MKB.

In the case of SOB, when multiple management files exist on a media, the Title Key File Set and the Title Usage File of the same number exists. If one of the Title Key File Sets is modified, only the Binding Nonce of the three Title Key Files within the Title Key File Set shall be updated. When the Read/Write MKB is updated, the Binding Nonce and Title Key File Nonce of all the Title Key Files shall be updated.

4. Delete renamed old MKB

## 3.4 Usage Rule

### 3.4.1 Title Usage File

Usage Rules shall be stored in Title Usage File. The Title Usage File for VOB shall be stored in the file “HR\_V\_TUF.aacs” located in the “/AACS” directory. The Title Usage File for SOB shall be stored in the file “HR\_Snn\_TUF.aacs” located in the “/AACS” directory. ‘nn’ takes the same value as the value used for the corresponding management file. For example, if an SOB is included in HR\_SFI01.SFI, the Usage Rule for the SOB is stored in “HR\_S01\_TUF.aacs”. Note that when multiple HR\_SFI<sub>nn</sub>.SFI files exist in a single media, Title Usage File is defined for each management file.

HR\_V\_TUF.aacs and HR\_Snn\_TUF.aacs are the same structure and the size of each Usage Rule is 32K bytes.

Each HD DVD-R/Rewritable media including AACS protected content shall have at least one Title Usage File. For clarification, when the media contains only VOB formatted content protected by AACS, VOB Title Usage File is required. When the media contains only SOB formatted content protected by AACS, SOB Title Usage File(s) is required. When the media contains both VOB and SOB formatted content protected by AACS, at least two Title Usage Files shall exist on the media.

Table 3-22 shows the structure of VOB Title Usage File.

**Table 3-22 – Format for VOB Title Usage File**

Bit Byte	7	6	5	4	3	2	1	0
0 : 11	(msb) VTUF_ID (lsb)							
12 : 15	(msb) HR_VTUF_EA (lsb)							
16 : 31	reserved							
32 : 33	(msb) VERN (lsb)							
34 : 127	reserved							
128 : 143	(msb) Usage Rule #1 (lsb)							
144 : 32095	Usage Rule (#2 .. #1998)							
32096 : 32767	reserved							

Because the maximum number of VOBs in a single HD DVD-R/Rewritable media is defined as 1998, the maximum number of VOB Usage Rules stored in each Title Usage File is also limited to 1998.

VTUF\_ID field indicates the 12-byte value to identify the VOB Title Usage File. The value is set to “DVD\_HR\_V\_TUF” with character set code of ISO/IEC 646:1983 (a-characters).

HR\_VTUF\_EA field indicates the end address of the VOB Title Usage File. Because the size of the VOB Title Usage File is fixed to 32KB, this field is filled with the value of ‘32767’.

VERN field indicates the version number of the Title Usage File, currently defined as the value of ‘0’.

Usage Rule is the value of a 128-bit Usage Rule. The Usage Rule of the number specified by the management file is stored in this field.

All bytes of reserved field shall be set to 00<sub>16</sub>.

Table 3-23 shows the structure of SOB Title Usage File.

**Table 3-23 – Format for SOB Title Usage File**

Bit Byte	7	6	5	4	3	2	1	0
0 : 11	(msb) STUF_ID (lsb)							
12 : 15	(msb) HR_STUF_EA (lsb)							
16 : 31	reserved							
32 : 33	(msb) VERN (lsb)							
34 : 127	reserved							
128 : 143	(msb) Usage Rule #1 (lsb)							
144 : 32095	Usage Rule (#2 .. #1998)							
32096 : 32767	reserved							

Because the maximum number of SOBs in a single HD DVD-R/Rewritable media is defined as 1998, the maximum number of SOB Usage Rules stored in each Title Usage File is also limited to 1998.

STUF\_ID field indicates the 12-byte value to identify the SOB Title Usage File. The value is set to “DVD\_S\_nn\_TUF” with character set code of ISO/IEC 646:1983 (a-characters). ‘nn’ takes the same value as the value used for the corresponding management file.

HR\_STUF\_EA field indicates the end address of the SOB Title Usage File. Because the size of the SOB Title Usage File is fixed to 32KB, this field is filled with the value of ‘32767’.

VERN field indicates the version number of the Title Usage File, currently defined as the value of ‘0’.

Usage Rule is the value of a 128-bit Usage Rule. The Usage Rule of the number specified by the management file is stored in this field.

All bytes of reserved field shall be set to 00<sub>16</sub>.

The common format of Usage Rule is applied to both VOB and SOB. Table 3-24 shows the structure of each Usage Rule. Currently DOT is defined. The priority bit is defined as DOT, respectively. The DOT is also defined in the content stream and is used to calculate Content Key. For each rule, when the priority bit is set to 1, priority is given to the rule defined in Usage Rule over the rule defined in the stream. Otherwise, the rule defined in the stream is superior to the rule defined in Usage Rule.

**Table 3-24 – Format for Usage Rule**

Bit Byte	7	6	5	4	3	2	1	0
0	UR_FLG	DOT-P	DOT	reserved				
1 : 15	reserved							

Usage Rule Flag (UR\_FLG) indicates the status of Usage Rule, as shown in Table 3-25.

**Table 3-25 – Encoding of UR\_FLG field in Usage Rule**

UR_FLG	Content Status
0	Usage Rule is invalid
1	Usage Rule is valid

When the Usage Rule is invalid, other field in Usage Rule shall be set to 0.

DOT indicates the status of Digital Only Token information of corresponding SOB, as shown in Table 3-26.

**Table 3-26 – Encoding of DOT field in Usage Rule**

DOT	Content Status
0	Decrypted outputs are permitted for all approved outputs
1	Decrypted outputs are permitted only for approved digital outputs

Other fields are reserved for future use and are currently defined to have a value of zero.

For HD DVD-Rewritable media, when the Title Usage File is first created, a licensed recorder shall initialize all records of Usage Rule filled with the value zero. When the licensed recorder stores the new Usage Rule in the Title Usage File, it searches the invalid record and overwrites with a proper value corresponding to the SOB or VOB. When the licensed recorder deletes a record of the Usage Rule, it shall overwrite the record with the value zero.

For HD DVD-R media, when the Title Usage File is first created, a licensed recorder may store multiple records of Usage Rules in the Title Usage File. All the remaining records of Usage Rule shall be filled with the value zero.

## 3.5 Backup and Recovery

### 3.5.1 Recovery for Title Key File

For backup purpose, three Title Key Files are defined as described in Section 3.3. When a licensed recorder updates Title Key File and detects the following conditions, it shall recover Title Key File.

1. In the case of detecting the value of Title Key File Generation for three Title Key Files are not the same
2. In the case of not being able to read one of the Title Key Files correctly within the Title Key File Set

Note that when a licensed recorder cannot read two or more Title Key Files within the Title Key File Set correctly, recovery procedure shall be aborted.

When a licensed recorder cannot read TKF<sub>X</sub> correctly or the value of Title Key Generation of TKF<sub>X</sub> is not the same as the value of Title Key File Generation of TKF<sub>Y</sub> and TKF<sub>Z</sub>, TKF<sub>Y</sub> and TKF<sub>Z</sub> are used to recover Title Key.

The process to recover Title Key is as follows:

1. Validate the value of the Binding Nonce<sub>Y</sub>

A licensed recorder shall check the value of the Binding Nonce<sub>Y</sub> associated with TKF<sub>Y</sub>. If the value is equal to zero, recovery procedure shall be aborted.

2. Decrypt all the Title Key(s)

Title Key(s) stored in TKF<sub>Z</sub> is decrypted as follows:

$$K_{pa\_Z} = \text{AES-G}(K_m, \text{Binding Nonce\_Z}), K_t = \text{AES-128D}(K_{pa\_Z} \oplus \text{TKFN\_Y}, K_{te\_Z}) \oplus \text{AES-H}(\text{Usage Rule})$$

where AES-G represents a cryptographic one-way function based on the AES algorithm as defined in the *Introduction and Common Cryptographic Elements* book.

and AES-128D represents decryption by the AES cipher with the Electronic Codebook (ECB) mode as defined in the *Introduction and Common Cryptographic Elements* book

and AES-H represents a cryptographic one-way function based on the AES algorithm as defined in the *Introduction and Common Cryptographic Elements* book.

3. Update Title Key Generation and Title Key File Nonce

Update the Title Key File Generation to increment the value by 1 and generate Title Key File Nonce<sub>X</sub>, update Title Key File Nonce<sub>Y</sub> and Title Key File Nonce<sub>Z</sub>.

4. Re-encrypt and store three Title Key Files

For each Title Key File, re-encrypt Title Key(s) by new Binding Nonce and the Title Key File Nonce, store the Title Key File with the updated Title Key Generation as described in Step 3 of Section 3.3.3.

5. Delete renamed old MKB

If renamed old MKB exists on the media, a licensed recorder shall check whether re-encryption of other Title Key File Sets has completed. If all the Title Key File Sets are encrypted by new MKB, the old MKB shall be deleted. Otherwise, the licensed recorder shall update other Title Key Files by new MKB as described in Section 3.3.3.

When a licensed recorder cannot read TKF<sub>Y</sub> correctly, TKF<sub>X</sub> and TKF<sub>Z</sub> are used to recover Title Key.

The process to recover Title Key is the same as described above.

When a licensed recorder cannot read TKF\_Z correctly or the value of Title Key Generation of TKF\_Z is not the same as the value of Title Key File Generation of TKF\_X and TKF\_Y, TKF\_X and TKF\_Y are used to recover Title Key.

The process to recover Title Key is the same as described above.

### 3.5.2 Backup and Recovery for other Files

Read/Write Media Key Block and Title Usage File shall have these backup files in the “AACs\_BACK” directory of the Data Area. A licensed recorder may use any of the backup files if it cannot correctly read the original files. If the original file is updated, the corresponding backup file shall be updated.

## 3.6 Content Encryption and Decryption for VOB

For each AV Pack, if a 2-bit “PES\_scrambling\_control” field is set to 11<sub>2</sub>, the AV Pack shall be encrypted.

The process to encrypt VOB Video Recording formatted content is as follows:

1. Generate the Title Key ( $K_t$ )

The licensed recorder generates a statistically unique 128-bit Title Key, searches an invalid record in the VOB Title Key File, and chooses a record number of VOB Title Key File to store the Encrypted Title Key.

2. Generate Media ID MAC ( $MAC_{id}$ ) using the Title Key
3. Calculate Content Key

For each AV Pack to be encrypted, the licensed recorder uses Title Key, a 32-bit Title Key Data ( $D_{tk}$ ), and the least significant 96 bits of CPI field in the RDI pack to calculate a 128-bit Content Key ( $K_c$ ) as follows:

$$K_c = \text{AES-G}(K_t, D_{tk} \parallel \text{CPI}_{lsb\_96})$$

where AES-G represents a cryptographic one-way function based on the AES algorithm as defined in the *Introduction and Common Cryptographic Elements* book.

When the value of the Title Key Data is different with each AV Pack, the licensed recorder recalculates Content Key. Because RDI pack exists only at the beginning of the VOB, the same CCI information is used to encrypt all the AV Packs within the VOB.

4. Encrypt the content

The Content Key is used to encrypt the AV Pack’s 1920-byte Encrypted Portion of Unencrypted Content (C) as follows:

$$C_e = \text{AES-128CBCE}(K_c, C)$$

where AES-128CBCE represents encryption by the AES algorithm in CBC mode as defined in the *Introduction and Common Cryptographic Elements* book.

For each RDI pack, the licensed recorder shall set the values as shown in Table 3-27.

5. Encrypt the Title Key(s)

The Title Key(s) is encrypted as described in Section 3.3.2.

If other Encrypted Title Keys encrypted by the old Binding Nonce exist in the Title Key File and the old Title Key File Nonce, those Encrypted Title Keys are re-encrypted by the updated Binding Nonce and updated Title Key File Nonce.

6. Transfer the data

The licensed recorder stores the Encrypted Title Key(s) and Media ID MAC(s) in the correct record of the VOB Title Key File indicated by the Copy Protection Pointer of the corresponding RDI pack. Three Title Key Files shall be updated as described in Section 3.3.3. Usage Rule(s) are also stored in the correct record of the VOB Title Usage File indicated by the Copy Protection Pointer of the corresponding RDI pack. The record number of the Title Key and Usage Rule is stored in the Copy Protection Pointer field in the management file. Encrypted Content is packed into the AV Pack and stored on the media.

**Table 3-27 – Stored value of RDI pack**

Field	Value
KEY_VF	01 <sub>2</sub>
Copy Protection Pointer	record number of the Title Key and the Usage Rule
UR_VF	1

When the licensed recorder records the stream, it shall change neither Title Key nor Usage Rule in the middle of VOB. In other words, if the Usage Rule is changed in the middle of recording, the licensed recorder shall make a new VOB.

The process to decrypt VOB Video Recording formatted content is as follows:

1. Select the Title Key(s) and Usage Rule(s)

The licensed recorder first selects the correct Encrypted Title Key from VOB Title Key File and Usage Rule from VOB Title Usage File corresponding to the VOB.

2. Decrypt the Encrypted Title Key(s)

The Title Key(s) is decrypted as described in Section 3.3.2.

3. Select and verify Media ID MAC (MAC<sub>id</sub>)

The correct MAC value is selected to read the management file, and the MAC value is checked. If the verification fails, playback of the media shall be aborted.

4. Calculate Content Key:

For each AV Pack, if “PES\_scrambling\_control” is 11<sub>2</sub>, the licensed recorder uses Title Key, Title Key Data (D<sub>tk</sub>), and the least significant 96 bits of CPI field in the RDI pack to calculate a 128-bit Content Key (K<sub>c</sub>) as follows:

$$K_c = \text{AES-G}(K_t, D_{tk} \parallel \text{CPI}_{sb,96})$$

where AES-G represents a cryptographic one-way function based on the AES algorithm as defined in the *Introduction and Common Cryptographic Elements* book.

If “PES\_scrambling\_control” bit is 00<sub>2</sub>, decryption is terminated because current pack is not encrypted.

5. Decrypt the Content

The Content Key is used to decrypt the AV Pack’s 1920-byte Encrypted Portion of Encrypted Content (C<sub>e</sub>) as follows:

$$C = \text{AES-128CBCD}(K_c, C_e)$$

where AES-128CBCD represents decryption by the AES algorithm in CBC mode as defined in the *Introduction and Common Cryptographic Elements* book.

For each AV Pack, if the Copy Protection Pointer field of the RDI pack is changed from the previous RDI pack, the corresponding Encrypted Title Key should be reloaded (Step1).

### 3.7 Content Encryption and Decryption for SOB

The process to encrypt SOB Video Recording formatted content is as follows:

1. Generate the Title Key (K<sub>t</sub>)

The licensed recorder generates a statistically unique 128-bit Title Key, searches an invalid record in the SOB Title Key File, and chooses a record number of SOB Title Key File to store the Encrypted Title Key.

2. Generate Media ID MAC ( $MAC_{id}$ ) using the Title Key
3. Calculate Content Key

For each Packet Group to be encrypted, the licensed recorder uses Title Key, Title Key Data ( $D_{tk}$ ), and the least significant 64 bits of CPI field in the Packet Group header to calculate a 128-bit Content Key ( $K_c$ ) as follows:

$$K_c = \text{AES-G}(K_t, D_{tk} \parallel \text{CPI}_{\text{lsb}_{64}})$$

where AES-G represents a cryptographic one-way function based on the AES algorithm as defined in the *Introduction and Common Cryptographic Elements* book.

4. Encrypt the content

The Content Key is used to encrypt the Packet Group's Encrypted Portion of Unencrypted Content ( $C$ ) of the Packet Group as follows:

$$C_e = \text{AES-128CBCE}(K_c, C)$$

where AES-128CBCE represents encryption by the AES algorithm in CBC mode as defined in the *Introduction and Common Cryptographic Elements* book.

A licensed recorder shall neither reset the cipher block chain nor change the Content Key in the middle of the Packet Group.

For each Packet Group, the licensed recorder writes the record number of the Title Key into the Copy Protection Pointer field and the record number of the Usage Rule into the Usage Rule Pointer field of the Packet Group Header. The record number corresponding to SOB in the management file is stored in the Packet Group Header.

5. Encrypt the Title Key(s)

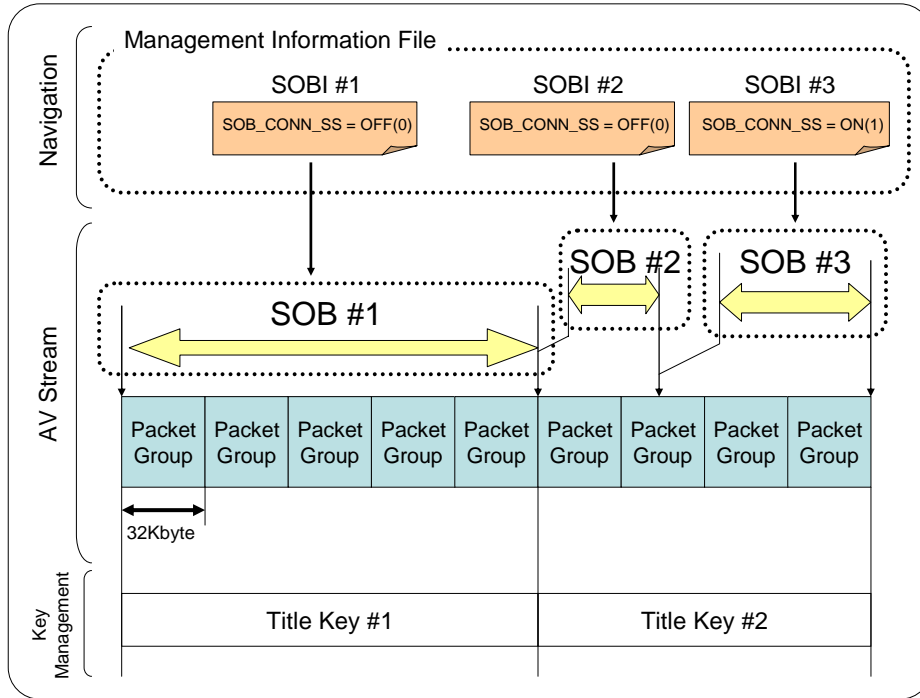
The Title Key(s) is encrypted as described in Section 3.3.2.

If other Encrypted Title Keys encrypted by the old Binding Nonce exist in the Title Key File and the old Title Key File Nonce, those Encrypted Title Keys are re-encrypted by the updated Binding Nonce and the updated Title Key File Nonce.

6. Transfer the data

The licensed recorder stores the encrypted Title Key(s) and Media ID MAC(s) to the correct record of the SOB Title Key File indicated by the Copy Protection Pointer of the Packet Group Header. Three Title Key Files shall be updated as described in Section 3.3.3. Usage Rule(s) is stored in the correct record of the SOB Title Usage File indicated by the Copy Protection Pointer of the corresponding Packet Group. The record number of the Title Key and Usage Rule are stored in Copy Protection Pointer field in the management file. Encrypted Content is packed into the Packet Group and stored on the media.

When AV stream is continuously recorded, one or more Packet Groups are organized into a logical unit named SOB (Stream Object). The licensed recorder shall not change the Title Key in a single SOB. When recording device records multiple SOBs, the licensed recorder may change the Title Key. Figure 3-1 shows an example of the relationship between SOB and Title Key. The first and the second SOB are encrypted with different Title Keys.



**Figure 3-1 – Example of SOB and Title Key**

When the licensed recorder continuously records the stream and SOB\_CONN\_SS flag in the SOB\_CONNI field of SOBI is 01<sub>2</sub>, the Title Key to encrypt the SOB shall not change the previous one that is used to encrypt the previous SOB and Copy Protection Pointer shall not be changed from the previous one.

When the licensed recorder changes the Title Key, Copy Protection Pointer defined in the Packet Group Header shall be changed. When the licensed recorder changes the Usage Rule, Title Key shall be changed.

For clarification, although plural SOBs encrypted by the same Title Key may have different Copy Protection Pointer, plural SOBs encrypted by a different Title Key shall not have the same Copy Protection Pointer within a Title Key File. If the SOBs are included in different management file, a value of the Copy Protection Pointer may use the same value, even if these SOBs are encrypted by the different Title Key. The plural SOBs which are encrypted by the same Title Key but use different Usage Rule shall not include the same management file.

The process to decrypt SOB Video Recording formatted content is as follows:

1. Select the Title Key(s) and Usage Rule(s)

The licensed recorder first selects the correct Encrypted Title Key from SOB Title Key File and Usage Rule from SOB Usage Rule File corresponding to the SOB.

2. Decrypt the Encrypted Title Key(s)

The Title Key(s) is decrypted as described in Section 3.3.2.

3. Select and verify Media ID MAC

The correct MAC value is selected to read the management file and verify the MAC value of Media ID. If the verification fails, playback of the media shall be aborted.

4. Calculate Content Key:

For each Packet Group, if “P-CCI Valid” bit of CCI\_SS field is ‘1’ and Primitive CCI is “100<sub>2</sub>”, “010<sub>2</sub>” or “011<sub>2</sub>”, the licensed recorder uses Title Key, Title Key Data (D<sub>tk</sub>), and the least significant 64 bits of CPI field in the Packet Group Header to calculate a 128-bit Content Key (K<sub>c</sub>) as follows:

$$K_c = \text{AES-G}(K_t, D_{tk} \parallel \text{CPI}_{lsb_{64}})$$

where AES-G represents a cryptographic one-way function based on the AES algorithm as defined in the *Introduction and Common Cryptographic Elements* book.

If “P-CCI Valid” bit of CCI\_SS field is ‘0’ or Primitive CCI is “000<sub>2</sub>”, decryption is terminated because current Packet Group is not encrypted.

#### 5. Decrypt the Content

The Content Key is used to decrypt the Packet Group’s 1920-byte Encrypted Portion of Encrypted Content ( $C_e$ ) of the Packet Group as follows:

$$C = \text{AES-128CBCD}(K_c, C_e)$$

where AES-128CBCD represents decryption by the AES algorithm in CBC mode as defined in the *Introduction and Common Cryptographic Elements* book.

For each Packet Group, if the Copy Protection Pointer field of the Packet Group Header is changed from the previous Packet Group, the corresponding Encrypted Title Key should be reloaded (Step1).

### 3.8 Secure Move

The general approach for secure move is specified in Section 3.6.1 of the *Recordable Video* book. This section specifies the additional requirements that are specific to HD DVD Video Recording Format.

A minimum unit which can move is all VOBs or SOBs encrypted by the same Title Key. The licensed recorder shall neither move a part of several VOBs encrypted by the same Title Key, nor move a part of the same VOB.

The licensed recorder shall not leave any Title Key, which is the same value as that used for the moved content, on the media.

# Chapter 4

## Protection of HD DVD Interoperable Content

### 4 Protection of HD DVD Interoperable Content

#### 4.1 Introduction

The HD DVD Video Recording format supports Interoperable Content which HD DVD-Video disc system has a capability to playback. Interoperable Content is originally generated from the HD DVD VOB recording mode. This chapter describes the method for encryption and decryption with Interoperable Content protected by AACS. The HD DVD Interoperable Content is the subject of a license from the DVD Forum, which also publishes a specification describing the format in detail (see the corresponding reference in Section 1.4).

#### 4.2 Stored Data Values for Interoperable Content

##### 4.2.1 Stored Data Values for Interoperable Content

In the case of Interoperable Content, the management information file named HR\_IVTSL.VTI is used.

**Table 4-1 – Storage of AACS components in VTS\_EVOBI**

Bit Byte	7	6	5	4	3	2	1	0
0 : 301	(Data defined in HD DVD-Video specification)							
302	(msb)		Copy Protection Pointer				(lsb)	
303								
304	(msb)		reserved				(lsb)	
305								
306 : 319	(Data defined in HD DVD-Video specification)							

The value of Copy Protection Pointer of corresponding VOB stored in M\_VOB\_GI is copied in the Copy Protection Pointer field.

2 bytes of reserved field following Copy Protection Pointer shall be set to zero.

## 4.2.2 Protection Format for EVOB

Because the format of each RDI Pack and AV Pack for Interoperable Content is completely identical to Video Object (VOB) recording mode, it is not necessary to re-encrypt the content.

## 4.3 Title Key File

Encrypted Title Keys ( $K_{te}$ ) shall be stored in Title Key File. The Title Key File Set for Recording mode for Video Object (VOB) shall be stored in the file “HR\_V\_TKfx.aacs”, “HR\_V\_TKFy.aacs” and “HR\_V\_TKFz.aacs” located in the “/AACs” directory. The same title Key File Set is used for Interoperable Content. For clarification, the format of the Title Key File is not changed and each Encrypted Title Key is not re-encrypted.

Because the maximum number of VOBs in a single HD DVD-R/Rewritable media is defined as 1998, the maximum number of Title Keys stored in the EVOB Title Key File is also limited to 1998. Note that, although the maximum number of Title Keys for HD DVD Pre-recorded Video is 64, the maximum number of Title Keys for Interoperable Content is expanded to 1998.

## 4.4 Usage Rule

### 4.4.1 Title Usage File

Usage Rule shall be stored in Title Usage File. The Title Usage File for Recording mode for Video Object (VOB) shall be stored in the file “HR\_V\_TUF.aacs” located in the “/AACs” directory. The same Title Usage File is used for Interoperable Content. For clarification, the format of the Title Usage File is not changed.

Because the maximum number of VOBs in a single HD DVD-R/Rewritable media is defined as 1998, the maximum number of Usage Rules stored in the Title Usage File is also limited to 1998. Note that, although the maximum number of Usage Rules for HD DVD Pre-recorded Video is 64, the maximum number of Usage Rules for Interoperable Content is expanded to 1998.

## 4.5 Content Decryption for Interoperable Content

Because the licensed recorder converts Recording mode of Video Object (VOB) to Interoperable Content without any change for AV pack and RDI pack, the process to encrypt Interoperable Content is completely identical to HD DVD Video Recording form described in Section 3.6. The same Title Key File and Title Usage for VOB shall be used to decrypt content.

# **Chapter 5**

## **Protection of HD DVD-Video Format**

### **5 Protection of HD DVD-Video Format**

This page is intentionally left blank.

# Appendix A

## Additional requirements for carriage of SRM

### A Additional requirement for carriage of SRM

#### A.1 Introduction

In the event that an SRM is stored on the media, this chapter describes the method to store SRM on HD DVD-R/Rewritable media.

#### A.2 SRM (System Renewability Message)

##### A.2.1 SRM for DTCP

SRM for DTCP shall be stored in the file “DTCP.SRM” located in the “/” directory of the Data Area.

##### A.2.2 SRM for HDCP

SRM for HDCP shall be stored in the file “HDCP.SRM” located in the “/” directory of the Data Area.