Advanced Access Content System (AACS)

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 0.921
July 25, 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.

Intellectual Property

Implementation of this specification requires a license from AACS LA LLC.

Contact Information

Please address inquiries, feedback, and licensing requests to AACS LA LLC:

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

The URL for the AACS LA LLC web site is http://www.aacsla.com.

This page is intentionally left blank.

Table of Contents

List of Figures

This page is intentionally left blank.

List of Tables

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 superceded 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 1.1*

DVD Forum, *DVD Specifications for High Density Recordable Disc for Dual Layer, Part 1: Physical Specifications Version 2.0*

DVD Forum, *DVD Specifications for High Density Recordable Disc for Dual Layer, Part 2: File System Specifications Version 2.0*

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
ARF	Advanced Resource File
AV	Audio-Visual
BCA	Burst Cutting Area
CCI	Copy Control Information
CGMS	Copy Generation Management System
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

This page is intentionally left blank.

Chapter 2
AACS Components on HD DVD-R/Rewritable Media

2 AACS Components on HD DVD-R/Rewritable Media

2.1 Introduction

This chapter specifies the location and format details of the AACS 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)[1]:

- 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 AACS protection. Figure 2-1 gives an overview of the locations of AACS 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.

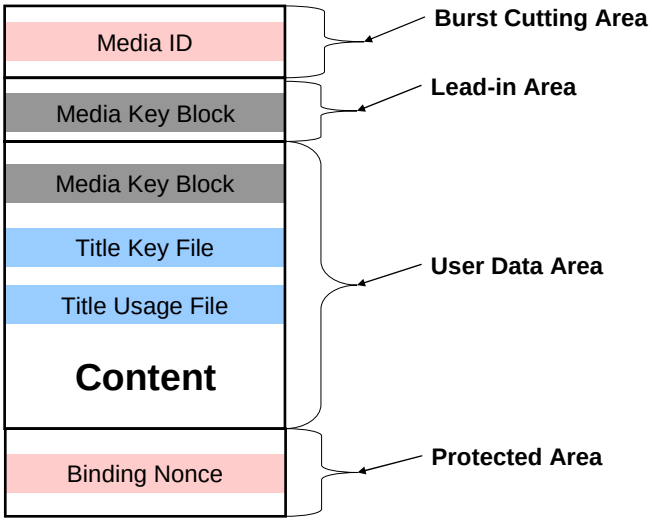


Figure 2-1 – Physical Layout of Common AACS Components on HD DVD-R/Rewritable Media

[1] HD DVD-R/Rewritable includes both single layer and dual layer (if defined by DVD Forum) in this specification.

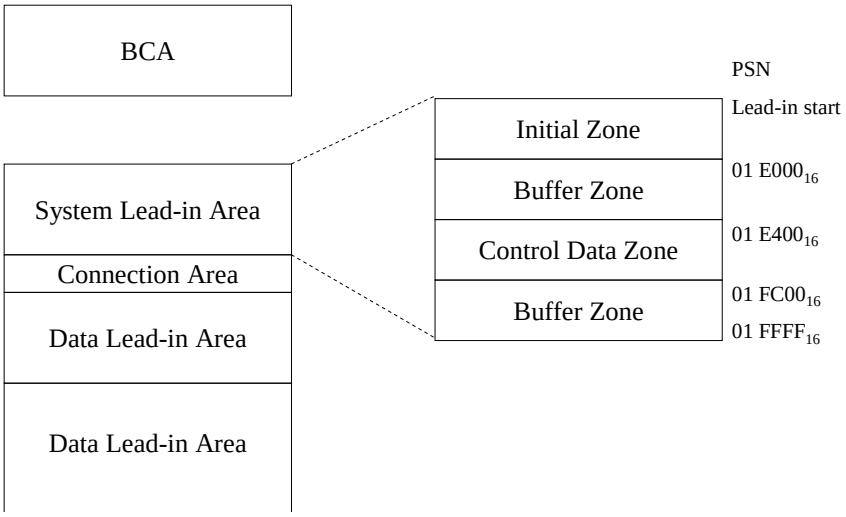


Figure 2-2 – Structure of BCA and Lead-in Area of an HD DVD-R/Rewritable media

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_{16} 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_{16}.

The Copyright Data Section can contain copyright data or the data of the Copyright Data Section shall be set to 00_{16}.

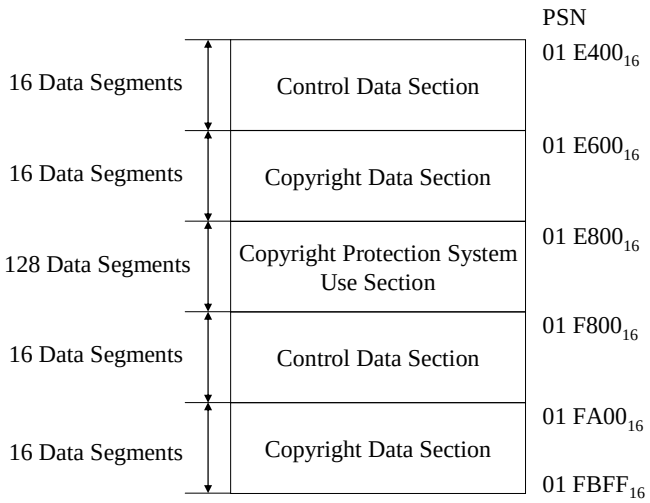
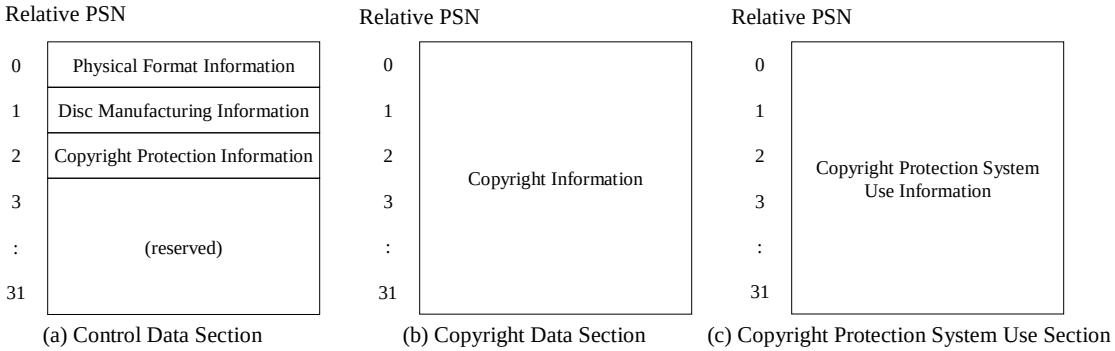


Figure 2-3 – Structure of a Control Data Zone



(a) Control Data Section (b) Copyright Data Section (c) Copyright Protection System Use Section

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

Table 2-1 – Format of Copyright Protection Information

Byte \ Bit	7	6	5	4	3	2	1	0
0	Copyright Protection System Type: 01_{16}							
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.

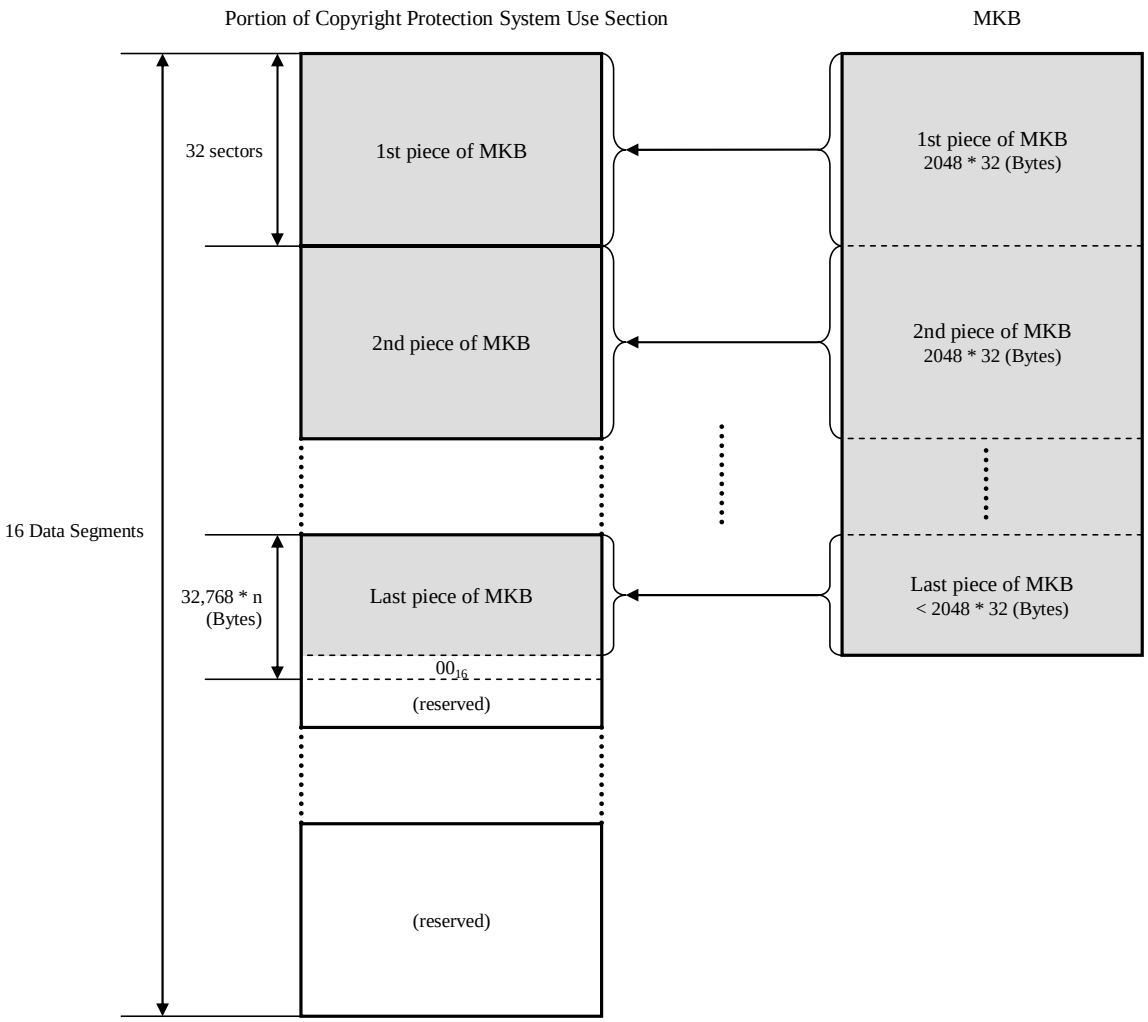


Figure 2-5 – Example of storing MKB on Lead-in Area of HD DVD-R/Rewritable media

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

Byte \ Bit	7	6	5	4	3	2	1	0
0	(msb)			BCA Record ID: 1004_{16}				
1								(lsb)
2	Version: 10_{16}							
3	Data Length: 10_{16}							
4 : 19	(msb)			Record Data: Media Identifier				(lsb)

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 indicting 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

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

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_{16}. 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_{16}.

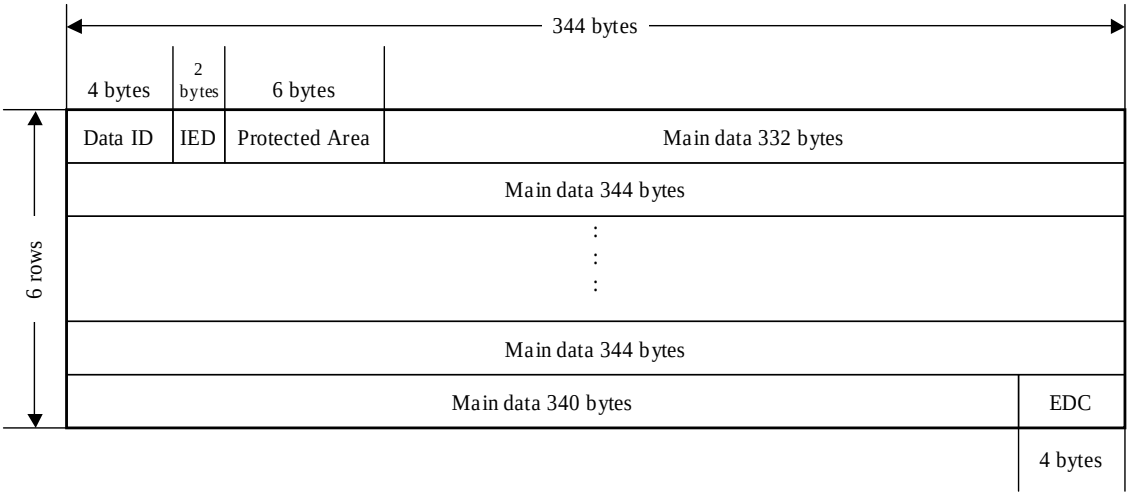


Figure 2-6 – Data frame configuration

Table 2-5 – Protected Area Format

Byte \ Bit	7	6	5	4	3	2	1	0
0	(msb)							
1	4 bytes of a 16-byte Binding Nonce							
2								
3								(lsb)
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 AACS components in M_VOB_GI

Byte \ Bit	7	6	5	4	3	2	1	0
0 : 23	(Data defined in HD DVD-VR specification)							
24	(msb) Copy Protection Pointer							
25	Copy Protection Pointer							(lsb)
26	(msb) reserved							
27	reserved							(lsb)
28 :	(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. Real-time Data Information (RDI) packs 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 steam (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
		0 : 40	(Data defined in HD DVD-VR specification)							
GCI_PKT		41 : 59	(Data defined in HD DVD-VR specification)							
	CPI (Content Protection Information)	60	KEY_VF		reserved					
		61	(msb) Copy Protection Pointer							
		62	(lsb)							
		63 : 67	reserved							
		68	UR_VF	(msb) reserved						
		69	(lsb)							
		70	(msb) CCI_SS							
		71	(lsb)							
		72	(msb) CCI							
		73	(lsb)							
		74	reserved							
		75								
		76 : 303	(Data defined in HD DVD-VR specification)							
		304 : 2047	(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_2.

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_2.

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 indicates the status of corresponding CCI. When the corresponding CCI is valid or exists, each bit of CCI_SS shall be set to 1, otherwise the field shall be set to 0. Each bit of CCI_SS shall be set by the Licensed Recorder based on the rules defined for the input data stream being recorded. When a Licensed Recorder supporting VOB recording mode records the stream encrypted by AACS, it shall set at least P-CCI as valid and set Primitive CCI value based on the characteristics of the content stream. When the value of each bit of CCI_SS is 1, a Licensed Player shall behave according to the corresponding CCI based on the Compliance Rules. When the value of particular bit of CCI_SS is 0, and if there is a specific corresponding rule described in this section, a Licensed Player shall behave according to the rule. Otherwise the Licensed Player may ignore each CCI when the corresponding value of CCI_SS is 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 each CCI based on the rules defined for the input data stream being recorded. 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_2	Copy Freely
100_2	Copy One Generation
010_2	No More Copies
110_2	Copy Never
011_2	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_2, 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_2, 010_2 or 011_2, 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_2. Where copy control restrictions are not asserted with respect to such protected content, the Primitive CCI field shall be set to 011_2.

If P-CCI Valid field in CCI_SS is invalid, a Licensed Player shall not decrypt the corresponding AV Packs.

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_2	APSTB is OFF
001_2	Type 1 of APS1 is ON
010_2	Type 2 of APS1 is ON
011_2	Type 3 of APS1 is ON
110_2	APS2 is ON
111_2	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_2 in an encrypted AV Pack, and to 00_2 in an unencrypted AV Pack. The use of the 32-bit Title Key Data (D_{tk}) 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 / Byte	7	6	5	4	3	2	1	0
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_{tk})							
	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

Byte \ Bit	7	6	5	4	3	2	1	0
0 : 57	(Data defined in HD DVD-VR specification)							
58	(msb) Copy Protection Pointer							
59								(lsb)
60	(msb) reserved							
61								(lsb)
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 / Byte	7	6	5	4	3	2	1	0
Unencrypted Portion (144 bytes)	Packet Group Header		0 : 19	(Data defined in HD DVD-VR specification)							
		CPI (Content Protection Information)	20	reserved							
			21								
			22	(msb) Copy Protection Pointer							
			23								(lsb)
			24	reserved							
			25								
			26	(msb) CCI_SS							
			27								(lsb)
			28	(msb) CCI							
			29								(lsb)
			30	reserved							
			31								
			32 : 127	(Data defined in HD DVD-VR specification)							
	170 pairs of PATS and TS Packet	AV data	128 : 135	Title Key Data (D_{tk})							
			136 : 143	Unencrypted Content							
Encrypted Portion (32624 bytes)			144 : 32767	Encrypted Content							

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 indicates the status of corresponding CCI. When the corresponding CCI is valid or exists, each bit of CCI_SS shall be set to 1, otherwise the field shall be set to 0. Each bit of CCI_SS shall be set by the Licensed Recorder based on the rules defined for the input data stream being recorded. Some CCI information is embedded in the content stream. When a Licensed Recorder supporting SOB recording mode records the stream encrypted by AACS, 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. When the value of each bit of CCI_SS is 1, a Licensed Player shall behave according to the corresponding CCI based on the Compliance Rules. When the value of particular bit of CCI_SS is 0, and if there is a specific corresponding rule described in this section, a Licensed Player shall behave according to the rule. Otherwise the Licensed Player may ignore each CCI when the corresponding value of CCI_SS is 0.

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 each CCI based on the rules defined for the input data stream being recorded. 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_2	Copy Freely
100_2	Copy One Generation
010_2	No More Copies
110_2	Copy Never
011_2	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_2, 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_2, 010_2 or 011_2, 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_2. Where copy control restrictions are not asserted with respect to such protected content, the Primitive CCI field shall be set to 011_2.

If P-CCI Valid field in CCI_SS is invalid, a Licensed Player shall not decrypt the corresponding Packet Group.

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_2	APSTB is OFF
001_2	Type 1 of APS1 is ON
010_2	Type 2 of APS1 is ON
011_2	Type 3 of APS1 is ON
110_2	APS2 is ON
111_2	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.

In case where either APSTB Valid field or ICT Valid field in CCI_SS is invalid, and if a Licensed Player cannot recognize the CCI originally embedded in the stream, the Licensed Player shall not output the content of the corresponding Packet Group to an analog interface. The Licensed Player may always render or output to an allowed digital interface based on the value of Primitive CCI. If a Licensed Player can recognize the APSTB and ICT originally embedded in the stream, it shall behave based on the values of APSTB and ICT embedded in the stream.

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

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

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

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 “/AACS” 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 “/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 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_SFInn.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 AACS shall have at least one Title Key File Set. For clarification, when the media contains only VOB formatted content protected by AACS, VOB Title Key File Set is required. When the media contains only SOB formatted content protected by AACS, SOB Title Key File Set(s) is required. When the media contains both VOB and SOB formatted content protected by AACS, 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

	Bit / Byte	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	(msb) VERN							
	33	(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	(msb) VERN							
	33	(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 128-bit random number as 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 128-bit random number as 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, Title Key File Nonce (TKFN) stored in other Title Key File (TKFN_Z, TKFN_X, TKFN_Y) and Usage Rule corresponding to the Title Key as follows:

K_{pa}_X = AES-G($K_{m,}$ Binding Nonce_X), K_{te}_X = AES-128E (K_{pa}_X ⊕ TKFN_Z, K_t ⊕ AES-H (Usage Rule))

K_{pa}_Y = AES-G($K_{m,}$ Binding Nonce_Y), K_{te}_Y = AES-128E (K_{pa}_Y ⊕ TKFN_X, K_t ⊕ AES-H (Usage Rule))

K_{pa}_Z = AES-G($K_{m,}$ Binding Nonce_Z), K_{te}_Z = AES-128E (K_{pa}_Z ⊕ TKFN_Y, K_t ⊕ AES-H (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 = AES-G($K_{m,}$ Binding Nonce_X), K_t = AES-128D (K_{pa}_X ⊕ TKFN_Z, K_{te}_X) ⊕ AES-H (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 Section2.3. 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_SFInn.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	(msb) VERN							
33	(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_{16}.

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	(msb) VERN							
33	(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_{16}.

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_X correctly or the value of Title Key Generation of TKF_X is not the same as the value of Title Key File Generation of TKF_Y and TKF_Z, TKF_Y and TKF_Z are used to recover Title Key.

The process to recover Title Key is as follows:

1. Validate the value of the Binding $Nonce_y$

A Licensed Recorder shall check the value of the Binding Nonce_Y associated with TKF_Y. 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_z is decrypted as follows:

K_{pa}_Z = AES-G($K_{m,}$ Binding Nonce_Z), K_t = AES-128D ($K_{pa}\_Z \oplus$ TKFN_Y, K_{te}_Z) $\oplus$ AES-H (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_X, update Title Key File Nonce_Y and Title Key File Nonce_Z.

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_Y correctly, TKF_X and TKF_Z 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 or a Licensed Player 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_2, 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 128-bit random number as 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:

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

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 VOBU, the same CCI information is used to encrypt all the AV Packs within the VOBU.

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	10_2
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 Player 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_{id})

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_2, the Licensed Player uses Title Key, 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:

$$K_c = \text{AES-G}\ (K_t, D_{tk} \,||\, CPI_{lsb\_96})$$

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

If "PES_scrambling_control" bit is 00_2, 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_e) 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_t)

The Licensed Recorder generates a 128-bit random number 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:

$$K_c = \text{AES-G}\ (K_t, D_{tk} \parallel CPI_{lsb\_64})$$

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

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.

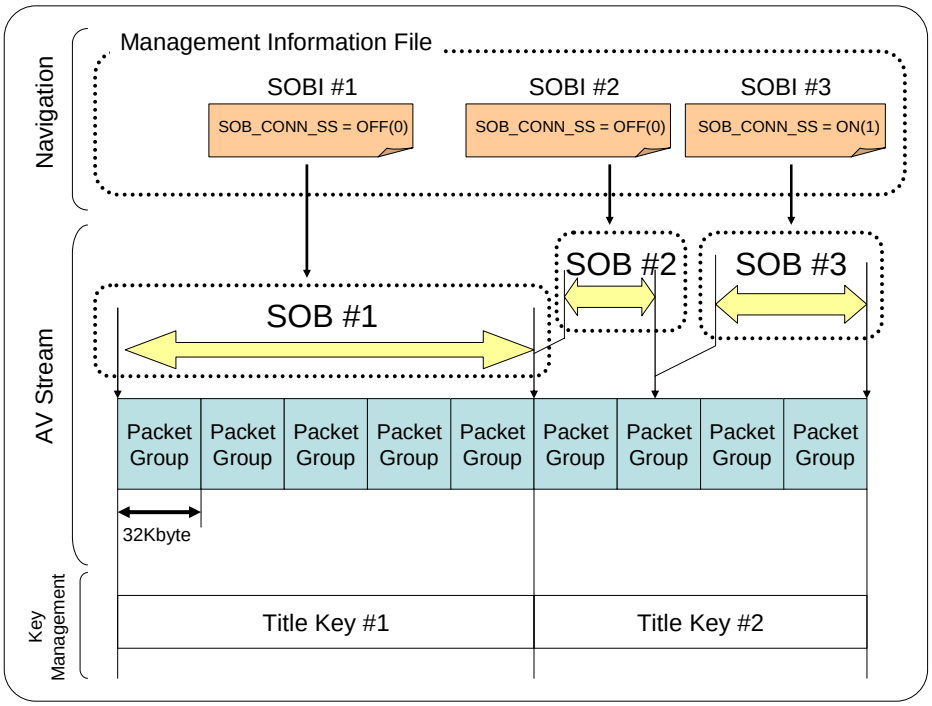


Figure 3-1 – Example of SOB and Title Key

When the Licensed Recorder continuously records the stream and SOB_CONN_SS flag in the SOB_CONNI field of SOBI is 01_2, 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 Player 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_2", "010_2" or "011_2", the Licensed Player 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:

$$K_c = \text{AES-G}\ (K_t, D_{tk} \parallel CPI_{lsb\_64})$$

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_2", 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 32624-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 AACS Interoperable Content Mode

A Licensed Player has two modes: AACS Mode and Non-AACS Mode as defined in *AACS HD DVD and DVD Pre-recorded Book*. In addition to AACS Mode, the Licensed Player which has a capability to playback AACS Interoperable Content shall have AACS Interoperable Content Mode.

AACS Interoperable Content Mode is very similar to AACS Mode but is different in the following points.

- The Licensed Player shall enter into AACS Interoperable Content Mode when it playbacks Interoperable Content protected by AACS. In AACS Interoperable Content Mode, the Licensed Player shall handle both AACS encapsulation format defined in this specification and plaintext ARF format defined in the *HD DVD-Video Specifications*.
- The Licensed Player may enter into and leave AACS Interoperable Content Mode at anytime. For clarification, the Licensed Player may enter into AACS Interoperable Content Mode when it is in Non-AACS Mode.
- In AACS Interoperable Content Mode, AACS Object defined in *AACS HD DVD and DVD Pre-recorded Book* exists but the treatment of properties and function properties are different.

4.3 Stored Data Values for Interoperable Content

4.3.1 Stored Data Values for Interoperable Content

In the case of Interoperable Content, the management information file named HR_IVTSI.VTI is used.

Table 4-1 – Storage of AACS components in VTS_EVOBI

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

4.3.2 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.

4.3.3 Protection Format for Advanced Resources

Interoperable Content may include Advanced Resources. A file which contains data of Advanced Resources is called Advanced Resource File (ARF) in this specification. Though five kinds of encapsulation formats are defined in *AACS HD DVD and DVD Pre-recorded Book*, only Encapsulation Format for Encryption is used in AACS Interoperable Content. In AACS Interoperable Content Mode, ECMAScript Codes (JS), JPEG/PNG images, captured drawing images, MNG animations, LPCM/WAV effect audios, fonts (OTF, TTF and TTC) may be applied to the Encapsulation Format for Encryption and other ARFs are not allowed to be applied to the format. The protection format for encryption of Advanced Resources is as shown in Table 4-2.

To prevent from AACS encapsulation formatted ARF and plaintext ARF co-existing on a single media, the AACS encapsulated Advanced Resources shall be archived as an archiving file, which is defined in *HD DVD-Video Specifications* and takes ".aca" for its filename extension. The Resource Data Search Pointer defined in the *HD DVD-Video Specifications* in the archiving file shall indicate the attribute of the AACS encapsulated ARF. Note that each AACS encapsulated ARF in the archiving file shall have a MIME Type code value of FFh. For clarification, MIME Type and Suffix of each AACS encapsulated ARF in an archived file indicated by a URL take the same value of their original values (e.g., "image/ipeg" as MIME Type and "jpg" as Suffix). An archiving file itself shall not be AACS encapsulated.

Table 4-2– Encapsulation Format for Encryption of Advanced Content

Byte \ Bit	7	6	5	4	3	2	1	0
0 : 3	File ID							
4	Protection Type: 01_{16}							
5	(msb) Copy Protection Pointer							
6	Copy Protection Pointer (lsb)							
7 : 10	Resource File Size (N_{fs})							
11 : 282	Resource File Name (D_{RFN})							
283 : N_{fs}+283	ARF data (D_{RD})							

FILE ID field indicates the characters “AACS” with the character set code of ISO646 (a-characters).

Protection Type indicates the Encapsulation Format. In the case of Interoperable Content, this field shall be set to 01_{16}.

The Copy Protection Pointer field indicates the location of Encrypted Title Key within VOB Title Key File. Copy Protection Pointer takes a value between 1 and 1998, if valid Encrypted Title Key exists.

Resource File Size field indicates the size of the ARF. The size does not include the 272-byte Resource File Name defined in Encrypted Data field.

Resource File Name field indicates the filename of the ARF. For example, if the JPEG formatted file name is “foo.jpg”, Resource File Name field would be “foo.jpg.aacs”. If the Resource File Name is smaller than 272 bytes, the Resource File Name is so padded with 00_{16} after the file name that it becomes 272 bytes.

The ARF data field indicates the encrypted data of ARF.

4.4 Title Key

4.4.1 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.

4.5 Usage Rule

4.5.1 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.

4.6 Treatment of APIs and AACS Object

Some APIs and AACS Object are defined in *AACS HD DVD and DVD Pre-recorded Book.*

When an access to any property or any function property of AACS Object occurs during AACS Interoperable Content Mode it shall throw the exception such as HDDVD_E_INVALIDCALL.

When DrawingArea.captureWithMAC(), MainVideo.capture(), DrawingArea.capture() or MainVideo.changeImageSize() is called during decrypting EVOB of Interoperable Content in AACS Interoperable Content Mode, the Licensed Player shall throw the exception of AACS_E_INVALIDCAPTURE.

4.7 Content Decryption for EVOB of 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.

If P-CCI Valid field in CCI_SS is invalid, the Licensed Player shall not decrypt the corresponding AV Packs. The Licensed Player may ignore each CCI except P-CCI when the corresponding value of CCI_SS is 0.

When the Licensed Player decrypts AV Packs with/without Advanced Resources, the Licensed Player shall behave as described in Section 3.2.1 and Section 3.4.

If the CCIs of Main Video are different from Sub Video, more restrictive CCIs shall be used.

When the screen is composed of protected Advanced Resources only and includes no video, the CCIs shall be applied as shown in Table 4-3.

Table 4-3– CCI setting for Advanced Resources

CCI	Status
Primitive CCI	Copy Never (110_2)
APSTB	APSTB is OFF (000_2)
ICT	High Definition Analog Output in High Definition Analog Form (0_2)
DOT	Decrypted outputs are permitted for all approved outputs (0_2)

4.8 Content Encryption and Decryption for Advanced Resources of Interoperable Content

The process to encrypt Advanced Resources is as follows:

1. Select the Title Key (K_t)

If Advanced Resources are made from content marked as “Copy Never” or “No More Copies”, the Licensed Recorder shall use the same Title Key used for the content to encrypt the Advanced Resources.

If Advanced Resources are made from content marked as “Copy One Generation” or “EPN”, the Licensed Recorder may use the same Title Key used for the content, or may generate a 128-bit random number Title Key to encrypt the Advanced Resources. When the Licensed Recorder generates the new Title Key, it searches a 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. Encrypt the ARF data

The Resource File Name (D_{RFN}) and ARF data (D_{RD}) are encrypted as follows:

D_e = AES-128CBCE(K_t, D_{RFN} || D_{RD}),

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

If the length of ARF data is not a multiple of 16 bytes, the residual of data shall be left unencrypted.

The Licensed Recorder writes the record number of the Title Key into the Copy Protection Pointer field.

3. Encrypt the Title Key(s)

If the Title Key(s) is newly generated in Step 1, the Title Key is encrypted as described in Section 3.3.2 and other remaining Title Key are re-encrypted by updated the Binding Nonce and updated Title Key File Nonce.

4. Transfer the data

The Licensed Recorder stores the encrypted Advanced Resources. Three Title Key Files shall be updated if necessary.

The process to decrypt Advanced Resources is as follows:

1. Select the Title Key

The Licensed Player first selects the correct Encrypted Title Key from VOB Title Key File corresponding to the Advanced Resources

2. Decrypt the Encrypted Title Key

The Title Key is decrypted as described in Section 3.3.2.

3. Decrypt the Advanced Resources

The Resource File Name (D_{RFN}) and ARF data (D_{RD}) are decrypted as follows:

D_{RFN} || D_{RD} = AES-128CBCD(K_t, D_e),

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

If the length of ARF data is not a multiple of 16 bytes, the residual of data shall not be decrypted.

Before the Licensed Player uses an encapsulated ARF, it shall verify the Resource File Name field is identical to the filename of the encapsulated ARF. If they are not identical, the Licensed Player shall not use the encapsulated ARF and the Licensed Player shall behave as if the file does not exist. The Licensed Player will throw the exception of HDDVD_E_FILENOTFOUND or set error info of FILE_NOT_FOUND for the callback, etc. as defined in the *HD DVD-Video Specifications*. If the exception is not caught, it makes the Licensed Player immediately go to Stop State.

This page is intentionally left blank.

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.