

Advanced Access Content System (AACCS)

Blu-ray Disc 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. IBM, Intel, 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.
- Feedback on this specification should be addressed to 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

Notice	3
Intellectual Property.....	3
Contact Information.....	3
CHAPTER 1 INTRODUCTION	1
1.1 Purpose and Scope.....	1
1.2 Overview.....	1
1.3 Organization of this Document.....	1
1.4 Reference	2
1.5 Notation	2
1.6 Terminology	2
1.7 Abbreviation and Acronyms.....	3
CHAPTER 2 FORMAT OF CPS FOR BD RECORDABLE DISC	5
2. INTRODUCTION.....	5
2.1 Media ID.....	5
2.2 Binding Nonce	6
2.3 Bus Encryption Flag.....	6
2.4 Media Key Block.....	7
2.5 Backup of Media Key Block	7
2.6 Partial Media Key Block for Host Revocation List	7
CHAPTER 3 DETAILS FOR CONTENT ENCRYPTION AND DECRYPTION	11
3. INTRODUCTION.....	11
3.1 CPS Unit and Application Format Structure.....	11
3.1.1 Format Structure of BDMV Application	11
3.1.1.1 Clip	12

3.1.1.2	PlayList	12
3.1.1.3	Movie Object	12
3.1.1.4	BD-J Object	12
3.1.1.5	Index Table	12
3.1.1.6	First Playback	12
3.1.1.7	Top Menu.....	13
3.1.1.8	Title.....	14
3.1.1.9	CPS Unit for BDMV Application.....	14
3.1.2	Format Structure of BDAV Application.....	16
3.1.2.1	Clip	17
3.1.2.2	PlayList.....	17
3.1.2.3	infoBDAV.....	17
3.1.2.4	menu.tidx and mark.tidx (Thumbnail Index File).....	17
3.1.2.5	menu.tdt1, menu.tdt2, mark.tdt1, and mark.tdt2 (Thumbnail Data File).....	17
3.1.2.6	CPS Unit for BDAV Application	17
3.1.2.6.1	CCI Sequence	19
3.2	CPS Key File and CPS Usage File.....	19
3.2.1	CPS Unit Key File (Unit_Key_RW.inf) for BDMV Application.....	19
3.2.2	CPS Unit Key File (Unit_Key_RW.inf) for BDAV Application.....	21
3.2.3	Backup of CPS Unit Key File.....	24
3.2.4	CPS Unit Usage File (CPSUnitXXXXX.cci)	25
3.2.4.1	CCI_and_other_info().....	27
3.2.4.2	Basic CCI for AACs.....	28
3.2.4.3	CCI Sequence Information	32
3.3	Encrypted Packs	33
3.3.1	Encryption Scheme for Clip AV Stream.....	33
3.3.1.1	Copy Permission Indicator.....	33
3.3.2	Encrypted Scheme for Thumbnail data.....	34
3.4	Embedded CCI in AV Contents	35
3.4.1	Embedded CCI for Self-Encoded Stream Format of BDAV Application	35
3.4.2	Embedded CCI for Digital Recording of BDAV Application	35
3.4.3	Embedded CCI for BDMV Application	35
3.4.4	Data Structure of Copy Status Descriptor.....	35
3.4.4.1.1	private_data_byte	37
ANNEX A.	TREATMENT OF EACH CCI	39
A.1	Cognizant Recording and Non-Cognizant Recording	39
A.1.1	Cognizant Recording	39
A.1.2	Non-Cognizant Recording	39
A.2	Cognizant Playback and Non-Cognizant Playback	40
A.2.3	Cognizant Playback	40
A.2.4	Non-Cognizant Playback	40
ANNEX B.	CARRIAGE OF SYSTEM RENEWABILITY MESSAGE	41
B.1	Introduction	41
B.2	SRM for DTCP	41

B.3 SRM for HDCP41

This page is intentionally left blank.

List of Figures

Figure 3-1	Application Format Structure and CPS Unit for BDMV Application.....	11
Figure 3-2	Directory structure for BDMV Application	15
Figure 3-3	Application Format Structure and CPS Unit for BDAV Application	16
Figure 3-4	Application Format Structure and CPS Unit for BDAV Application	16
Figure 3-5	Directory structure for BDAV Application.....	18
Figure 3-6	CBC chaining on “Aligned Unit” basis	33
Figure 3-7	Calculation method for the Block Key.....	33
Figure 3-8	Data Format for tn_block	34
Figure 3-9	CBC chaining on “tn_sub_block” basis.....	34

This page is intentionally left blank.

List of Tables

Table 2-1	Data Format for BCA Record for Media ID of BD Recordable Disc	5
Table 2-2	Data Format for Binding Nonce in User Control Data.....	6
Table 2-3	Data Format for Bus Encryption Flag in User Control Data	7
Table 2-4	BD HRL Record Format	8
Table 2-5	Partial Media Key Block Format.....	8
Table 3-1	Data Format of CPS Unit Key File for BDMV Application	19
Table 3-2	Data Format of Unit_Key_File_Header() for BDMV Application	20
Table 3-3	Data Format of Unit_Key_Block() for BDMV Application	21
Table 3-4	Data Format of CPS Unit Key File for BDAV Application	22
Table 3-5	Data Format of Unit_Key_File_Header() for BDAV Application	22
Table 3-6	Data Format of Unit_Key_Block() for BDAV Application	23
Table 3-7	Data Structure for the CPS Unit Usage File	25
Table 3-8	Syntax for the CPS Unit Usage File	26
Table 3-9	Syntax for CCI_and_other_info().....	27
Table 3-10	Bit assignment for CCI_and_other_info_type.....	27
Table 3-11	Syntax of Basic CCI for AACs.....	28
Table 3-12	EPN	29
Table 3-13	CCI.....	29
Table 3-14	Trusted_Input	30
Table 3-15	Image_Constraint_Token	30
Table 3-16	Digital_Only_Token.....	30
Table 3-17	APS	30
Table 3-18	Syntax of CCI Sequence Information.....	32
Table 3-19	TP_extra_header.....	33
Table 3-20	copy_status_descriptor	36
Table 3-21	private_data_byte	37
Table 3-22	EPN	37
Table 3-23	CCI.....	37
Table 3-24	Image_Constraint_Token	38

Table 3-25 APS38

Table A-1 The combination between CCI in CCI Sequence Information and Embedded CCI.....39

Chapter 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 defines cryptographic procedures that are common among the various defined uses of the protection system. 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 *Blu-ray Disc Recordable Book*) specifies additional details for using the system to protect audiovisual content distributed on Blu-ray Disc Rewritable Media (BD-RE) and Blu-ray Disc Recordable Media (BD-R).

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.

Note: In this specification the words “BD Recordable Disc” includes both Blu-ray Disc Rewritable Media (BD-RE) and Blu-ray Disc Recordable Media (BD-R).

1.2 Overview

In this Blu-ray Disc Recordable Book, procedures are described for Content Encryption and Decryption that are required to protect AACS recordable video content.

This document is provided as a detailed description of procedures and data structures that are specific for the use of the AACS technology on BD Recordable Disc.

1.3 Organization of this Document

This document is organized as follows:

- Chapter 1 provides an introduction and overview.
- Chapter 2 describes the Physical Level Format of BD Recordable Disc.
- Chapter 3 describes Blu-ray Disc specific procedures for encryption and decryption of AACS video content on BD Recordable Disc

1.4 Reference

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, Introduction and Common Cryptographic Elements, Revision 0.91

AACS LA, Recordable Video Book, Revision 0.91

Blu-ray Disc Association, System Description Blu-ray Disc Rewritable Format, part 1: Basic Format Specifications, version 2.1

Blu-ray Disc Association, System Description Blu-ray Disc Rewritable Format, part 2: File System Specifications, version 2.0

Blu-ray Disc Association, System Description Blu-ray Disc Rewritable Format, part 3: Audio Visual Basic Format Specifications, version 2.0

Blu-ray Disc Association, System Description Blu-ray Disc Recordable Format, part 1: Basic Format Specifications, version 1.11

Blu-ray Disc Association, System Description Blu-ray Disc Recordable Format, part 2: File System Specifications, version 1.0

Blu-ray Disc Association, System Description Blu-ray Disc Read-Only Format, part 3: Audio Visual Basic Format Specifications, version 1.0

Digital Transmission Licensing Administrator, Digital Transmission Content Protection Specification Volume 1 Revision 1.4

1.5 Notation

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

1.6 Terminology

Aligned Unit: An Aligned unit consists of a series of 32 Source Packets.

Block Key: A Block Key is a key to encrypt and decrypt each Aligned unit.

CPS Unit: A CPS Unit is a group of titles or clips, to which the same title key has been assigned.

CPS Unit Key: A CPS Unit Key is a Blu-ray Disc synonym for the Title Key.

CPS Unit Usage file: A CPS Unit Usage file is a Blu-ray Disc synonym for the Title Usage file

Logical Sector: A Logical Sector is a data field in a logical volume. All Logical Sectors in a logical volume shall have the same size.

Reserved: The term “Reserved”, when used to define the syntax of the data structure, indicates that the field may be used for future extensions. All the bits of reserved field in the syntax of data structure shall be set to 0₂. The term “Reserved”, when used to define the meaning of values, indicates that the reserved values may be used for future extensions. The reserved values shall never be used in this version.

Source Packet: A Source Packet consists of a Source Packet header and a subsequent MPEG-2 transport packet.

User Control Data: A User Control Data is a control data contained in a sector.

1.7 Abbreviation and Acronyms

BCA	Burst Cutting Area
BD	Blu-ray Disc
BDAV	Blu-ray Disc Audio Visual
BDMV	Blu-ray Disc Movie
BD-CPS	Content Protection System for Blu-ray Disc
BD-R	Blu-ray Disc Recordable Media
BD-RE	Blu-ray Disc Rewritable Media
BD-ROM	Blu-ray Disc Read-Only Media
CCI	Copy Control Information
CPS	Content Protection System
ECC	Error Correction Code
MPEG	Moving Picture Experts Group

This page is intentionally left blank.

Chapter 2

Format of CPS for BD Recordable Disc

2. Introduction

This chapter describes additional details of the Copy Protection System Format that is specific to the use of AACS encryption with BD Recordable Discs.

2.1 Media ID

The Media ID shall be stored in the Burst Cutting Area (BCA) of BD Recordable Discs.

Table 2-1 shows the data format of the Media ID (128 bits) in the BCA Record of BD Recordable Discs.

(Note) For the BD Recordable Disc, the drive shall handle the disc as AACS compliant disc if the Media ID is recorded on the disc.

Table 2-1 Data Format for BCA Record for Media ID of BD Recordable Disc

Byte	7	6	5	4	3	2	1	0
0	Content Code = 000001 ₂						Data Unit sequence number = 00 ₂	
1	Content Sub Identifier = 0001 ₂				Content Length = E ₁₆			
2	Category = 0000 ₂ or 0001 ₂				Disc Manufacturer Code [11...8]			
3	Disc Manufacturer Code [7...0]							
4	Serial Number							
:								
15								

Each device shall use a 128-bit value in a Data Unit from the Content Code to the Serial Number as the Media ID, where the first 8 bits of the value is set to 00000100₂.

Content Code field (6 bits) indicates the application identifier, and is set to 000001₂ for discs protected by AACS.

Data Unit sequence number field (2 bits) indicates the data unit sequence number, and is set to 00₂ for Media ID.

Content Sub Identifier field (4 bits) indicates sub application identifier in an AACS protected disc, and is set to 0001₂ for Media ID.

Content Length (4 bits) indicates the number of bytes immediately following this field and up to the end of this application data, and is set to E₁₆.

Category field (4 bits) contains the disc category, and is set to 0000₂ for Blu-ray Disc Rewritable Media (BD-RE) and set to 0001₂ for Blu-ray Disc Recordable Media (BD-R).

Disc Manufacturer Code field (12 bits) contains the disc manufacturer code assigned to each disc manufacturer by the Blu-ray Disc licensing organization.

Each disc manufacturer shall assign 12-byte values to the Serial Number field that is unique for each disc.

2.2 Binding Nonce

The Binding Nonce is stored in the Protected Area of the BD Recordable Disc, and is used to calculate the Protected Area Key as described in Section 3.2 of the *Recordable Video Book* of this specification. For BDRecordable Disc, the Binding Nonce shall be stored in the User Control Data associated with the first logical Sector of the CPS Unit Key File and should be non-zero value. The details of the Protocol for Reading / Writing the Binding Nonce is described in Section 4.5 of the *Introduction and Common Cryptographic Elements* of this specification.

Table 2-2 shows the data format for Binding Nonce (128 bits) which is recorded in User Control Data of BD Recordable Disc.

Table 2-2 Data Format for Binding Nonce in User Control Data

Byte	Bit	7	6	5	4	3	2	1	0
0		Reserved for BEF	Reserved						
1		Reserved							
2		(msb)	Binding Nonce						
:									
17									
		(lsb)							

2.3 Bus Encryption Flag

The Bus Encryption Flag (BEF) is used to indicate whether the sector data shall be encrypted in the interface bus between the PC Drive and the PC Host or not. For BD Recordable Disc, the Bus Encryption Flag shall be also stored in the User Control Data associated with the corresponding sector.

Table 2-3 shows the data format for the Bus Encryption Flag (1 bit) which is recorded in the User Control Data of BD Recordable Disc. BEF field is reserved for future use and shall be set to 0₂.

Table 2-3 Data Format for Bus Encryption Flag in User Control Data

Byte	Bit	7	6	5	4	3	2	1	0
0		BEF	(reserved)						
1		(reserved)							
2		reserved for Binding Nonce							
:									
17									

2.4 Media Key Block

Each BD Recordable Disc that contains content encrypted by AACS [using a CPS Unit Key that is provided in the AACS directory] shall include exactly one Media Key Block (MKB). The MKB is used to grant playback of AACS protected content.

BD Recordable Disc applies the Read/Write Media Key Block that is defined in the *Recordable Video Book* of this specification, and does not contain a Read-Only MKB. The MKB “MKB_RW.inf” shall be stored in the “\AACS” directory.

The MKB stored in BD-RE is updatable, while the MKB stored in BD-R is not (BD-R is “write once” media).

2.5 Backup of Media Key Block

According to section 2.4.1 of the *Recordable Video Book* of this specification, the backup MKB is recorded during updating MKB.

The backup MKB “BAK_MKB.inf” shall be stored in the “\AACS” directory. The syntax of “BAK_MKB.inf” is the same as “MKB_RW.inf”, and the contents of “BAK_MKB.inf” is exactly the same as the contents of “MKB_RW.inf” at the time when the backup MKB is generated.

Details and the usage of the backup MKB are defined in Section 2.4.1 of the *Recordable Video Book* of this specification and the BD Recordable Disc applies the recovery protocol described in Section 2.4.1.1 of the *Recordable Video Book* of this specification.

2.6 Partial Media Key Block for Host Revocation List

The Host Revocation List is stored as “BD HRL Record” in the Lead-in area of disc. BD HRL Record consists of “Additional Record Type”, “Additional Record Length” and “Partial Media Key Block”. For BD Recordable Disc, the original of BD HRL Record and the duplicate of BD HRL Record shall be stored as 64KB units with zero padding in the INFO2/Reserved5 and Reserved8 in Inner Zone 0 of the BD Recordable Disc respectively. The same data is written twice and these data shall be recorded from the beginning of the Reserved5 and Reserved8 without defect management.

(Note) The maximum size of reserved area for BD HRL Record on BD Recordable Disc is one megabyte.

Table 2-4 shows the data format for the BD HRL Record which is recorded in the Lead-in area of BD Recordable Disc.

Table 2-4 BD HRL Record Format

Byte	Bit	7	6	5	4	3	2	1	0
0	Additional Record Type: 31_{16}								
1	Additional Record Length								
2									
3									
4									
5	Partial Media Key Block								
6									
...									
Length – 1									
Length	(padding)								
...									
64K*X-1									

Additional Record Type shall be 31_{16} for the BD HRL Record.

Additional Record Length indicates the number of bytes in this Record, including the Additional Record Type and the Additional Record Length.

The Partial Media Key Block consists of “Type and Version Record” and “Host Revocation List Record” of the Media Key Block.

Table 2-5 shows the data format for the Partial Media Key Block which is included in the BD HRL Record.

Table 2-5 Partial Media Key Block Format

Byte	Bit	7	6	5	4	3	2	1	0
0	Type and Version Record								
...									
11									
12									
13									
14									
...									

The BD drive is required to store only the Partial Media Key Block in its non-volatile memory. In other words, the drive is not required to store the Additional Record Type and the Additional Record Length in its non-volatile memory. The Host Revocation List Record required to be stored in the non-volatile memory of the drive consists of the data being signed for the first signature block including the Signature for Block 1. The details of the Host Revocation List Record are defined in Section 3.2.5.2 of the *Introduction and Common Cryptographic Elements* book of this specification.

For the BD Recordable Disc which does not have the BD HRL Record in the Lead-in area, the BD drive with recording function shall write the BD HRL Record on the disc before it writes the Binding Nonce on the disc if the new Binding Nonce is written on the disc by the drive with recording function. The Additional Record Type and the Additional Record Length shall be generated by the drive with recording function to form the BD HRL Record using the Partial Media Key Block stored in non-volatile memory of the drive with recording function.

On the other hand, for the Blu-ray Disc Rewritable Media (BD-RE) which has the BD HRL Record in the Lead-in area, if the version-number of the BD HRL Record recorded on the media is lower than the version number of the Partial Media Key Block stored in the drive with recording function, the drive with recording function shall generate the BD HRL Record using its Partial Media Key Block and write it on the media before it writes the Binding Nonce on the disc if the new Binding Nonce is written on the disc by the drive with recording function.

The behavior for drive is as follows:

In case that the drive cannot verify the BD HRL Record on the media, the drive shall read the Partial Media Key Block stored in non-volatile memory of the drive and use it for the authentication process. Note that the drive with recording function shall update the BD HRL Record in the Lead-in area before it writes the Binding Nonce on the disc if the new Binding Nonce is written on the disc by the drive with recording function. In case that the drive cannot read the BD HRL Record on the media for some reason, it shall read the Partial Media Key Block stored in non-volatile memory of the drive and use it for the authentication process. Note that the drive with recording function may update the BD HRL Record in the Lead-in area before it writes the Binding Nonce on the disc if the new Binding Nonce is written on the disc by the drive with recording function.

This page is intentionally left blank.



Chapter 3

Details for Content Encryption and Decryption

3. 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 section describes additional details of that approach that are specific to the use of AACS encryption with BD Recordable Discs.

3.1 CPS Unit and Application Format Structure

3.1.1 Format Structure of BDMV Application

BDMV Application Format is defined in *Blu-ray Disc Association, System Description Blu-ray Disc Read-Only Format, part 3: Audio Visual Basic Format Specifications, version 1.xx*.

Figure 3-1 describes a simplified diagram of the BDMV application format. This application format has four layers for managing AV stream files: those are Index Table, Movie Object, PlayList and Clip.

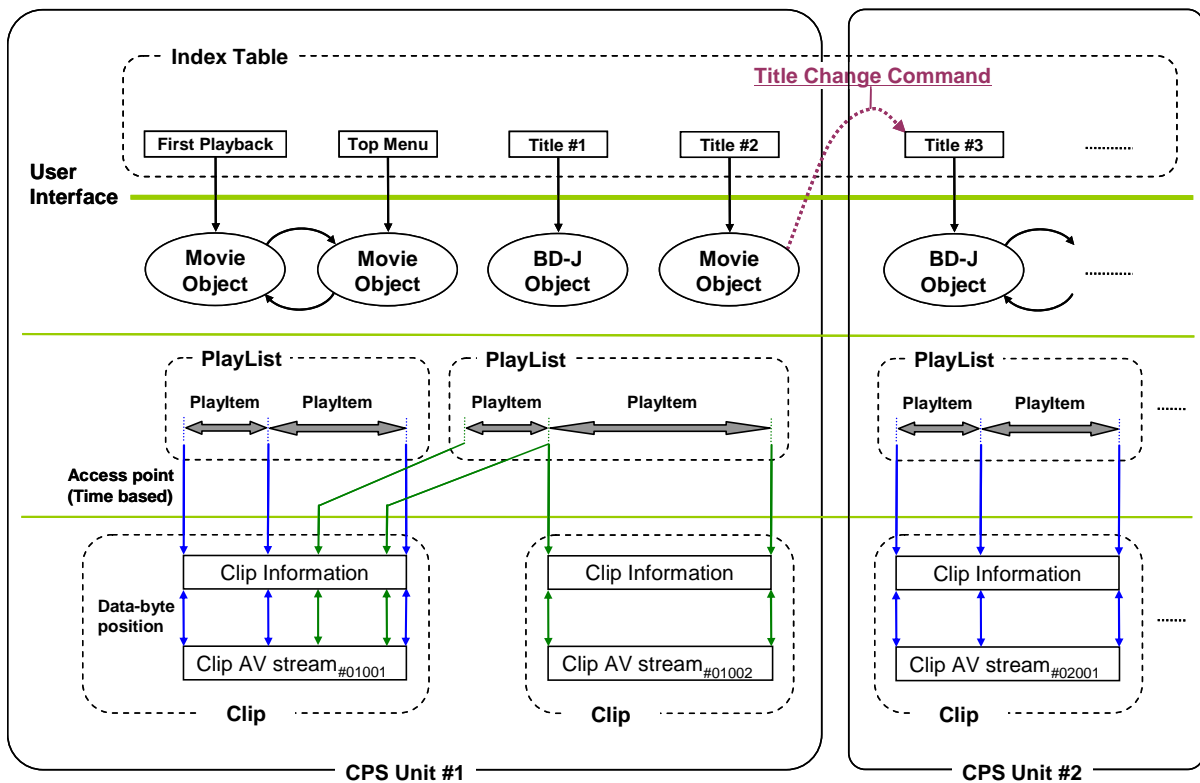


Figure 3-1 Application Format Structure and CPS Unit for BDMV Application

3.1.1.1 Clip

Each pair of an AV stream file and its attribute is considered to be one object. A Clip is an object consisting of a Clip AV stream file and its corresponding Clip information file. A Clip AV stream file stores data, which is basically an MPEG-2 transport stream defined in a structure conforming to *Blu-ray Disc Association, System Description Blu-ray Disc Read-Only Format, part 3: Audio Visual Basic Format Specifications, version 1.xx*. The Clip Information file stores the time stamps of the access point into the corresponding AV stream file. The Player reads the Clip Information to find out the position where it should begin to read the data from the AV stream file.

3.1.1.2 PlayList

A PlayList is a collection of playing intervals in the Clips. One such playing interval is called a PlayItem and consists of a pair of “IN-point and OUT-points” that point to positions on a time axis of the Clip. Therefore, a PlayList is a collection of PlayItems. Here the IN-point means a start point of a playing interval and the OUT-point means an end point of the playing interval.

3.1.1.3 Movie Object

A Movie Object consists of an executable navigation command program. This enables dynamic scenario description. Movie Objects are a layer above PlayLists. A navigation command in a Movie Object can launch a PlayList playback or a Movie Object can call another Movie Object so that a set of Movie Objects can manage playback of PlayLists in accordance with user’s interaction and preferences.

3.1.1.4 BD-J Object

A BD-J Object consists of a table of BD-J applications and indicates a set of BD-J Applications. This also enables dynamic scenario description and interactive contents playback by use of the Java programming environment. BD-J Objects are at the same layer of Movie Object, and selected per title basis. BD-J Applications in BD-J Object provides online functionality not only for the corresponding Title but also for the whole BD Recordable Disc.

3.1.1.5 Index Table

The Index Table is top-level information of the application format. This table contains entry points for all Titles, First Playback, and Top Menu. The Player references this table whenever a Title, First Playback, or Menu executing operation needs to be performed.

3.1.1.6 First Playback

First Playback may be optionally defined in the Index Table and points to a Movie Object or a BD-J Object, which then plays automatically. When the disc is loaded, the player refers to the entry of “First Playback” and obtains the corresponding Movie Object or a BD-J Object. First Playback Movie Object / BD-J Object is an optional function. A disc may or may not contain First Playback Movie Object / BD-J Object.

3.1.1.7 Top Menu

Top Menu may be optionally defined in the Index Table and points to a Movie Object or a BD-J Object. Top Menu can be called by a user operation such as “MenuCall”. A Movie Object indexed by Top Menu executes a Playlist whose PlayItem links a Clip having Button Objects. Each Button Object branches off to another Movie Object as a child Menu. Top Menu Movie Object is an optional function. A disc may or may not contain Top Menu Movie Object.

3.1.1.8 Title

Title is a logical unit for the user to recognize one playback group. The group may be one linear playback block or it may be a non-linear playback block with branching points. Each Title has a title_number. Title_number values are defined in ascending order, starting from one. All the values of the title_number shall be defined at least once on a disc.

3.1.1.9 CPS Unit for BDMV Application

A CPS Unit is a group of a First Playback, a Top Menu, and/or Titles, which are encrypted by using the same Unit Key (Kcu). Each CPS Unit has its corresponding CPS Unit CCI file. Each CPS Unit has a CPS_Unit_number. CPS_Unit_number values are defined in ascending order, starting from one. All the values of CPS_Unit_number shall be defined at least once on a disc.

All AV stream files that are referred to by First Playback are included in the same CPS Unit, i.e. they are encrypted by using the same Unit Key. All AV stream files that are referred to by Top Menu are included in the same CPS Unit: i.e. they are encrypted by using the same Unit Key. All AV stream files that are referred to by one Title are included in the same CPS Unit: i.e. they are encrypted by using the same Unit Key. If First Playback, Top Menu and/or a Title share one or more Clips, they shall be included in the same CPS Unit: i.e. the same Unit Key shall be assigned to First Playback, Top Menu and/or the Title. If multiple Titles share one or more Clips, these Titles shall be included in the same CPS Unit: i.e. the same Unit Key shall be assigned to these Titles. First Playback may or may not be included in the same CPS Unit with Top Menu, a Title, and/or Titles. Top Menu may or may not be included in the same CPS Unit with one or more Titles.

For example in Figure 3-1, since a First Playback, a Top Menu, and two Titles commonly refer to the same Clip AV stream_{#01001}, they belong to the same CPS Unit #1. Both Clip AV stream_{#01001} and Clip AV stream_{#01002} shall be encrypted by using the same key Kcu1.

To achieve higher security and future flexibility, different keys shall be assigned to different CPS Units. For example in Figure 3-1, different keys, Kcu1 and Kcu2, are assigned to CPS Unit #1 and CPS Unit #2. In this case, the switching between different CPS Units can be executed by some commands for Title change (e.g. Jump Title, Call Title, etc.) defined in *Blu-ray Disc Association, System Description Blu-ray Disc Read-Only Format, part 3: Audio Visual Basic Format Specifications, version 1.xx*.

Figure 3-2 shows the directory structure of BDMV application format. Detailed information is described in *Blu-ray Disc Association, System Description Blu-ray Disc Read-Only Format, part 3: Audio Visual Basic Format Specifications, version 1.xx*.

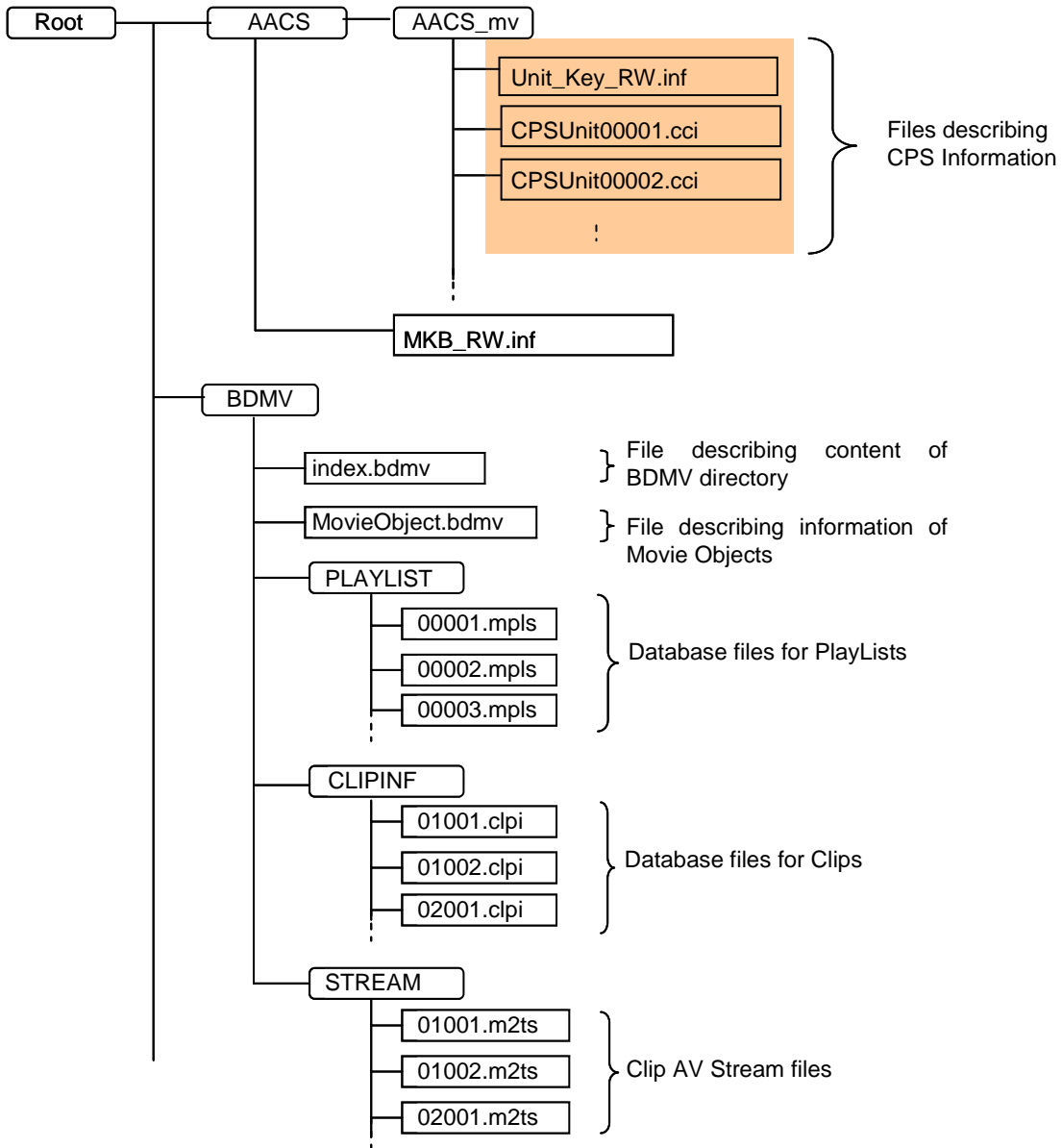


Figure 3-2 Directory structure for BDMV Application

All the AACS protected Clip AV stream files under “\BDMV\STREAM” directory shall be encrypted. Any other data under BDMV directory shall not be encrypted.

3.1.2 Format Structure of BDAV Application

BDAV Application Format is defined in *Blu-ray Disc Association, System Description Blu-ray Disc Rewritable Format, part 3: Audio Visual Basic Format Specifications, version 2.xx.*

Figure 3-3 describes a simplified diagram of the BDAV Application format.

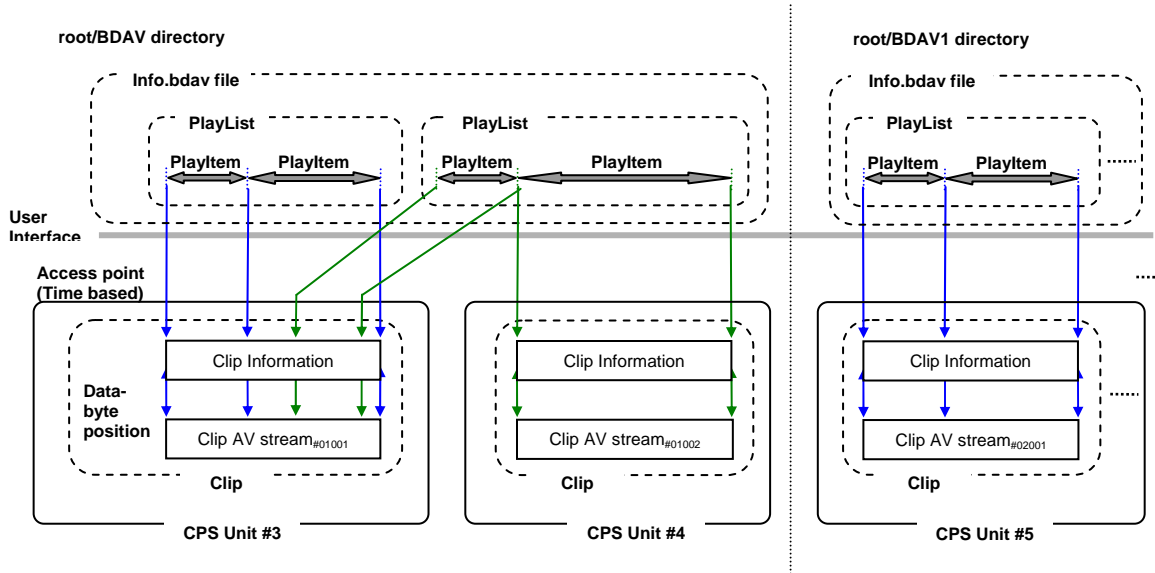


Figure 3-3 Application Format Structure and CPS Unit for BDAV Application

This application format has two layers for managing AV stream files: **PlayList** and **Clip**. BDAV Application files are stored in the “\BDAV” directory called “BasicBDAV” directory, and are also stored in “\BDAV1”, “\BDAV2”, “\BDAV3”, and “\BDAV4” directories called “Aux BDAV” directory.

In addition, BDAV Application Format has a function to store/display thumbnail pictures. Figure 3-4 describes the diagram of thumbnail files. Thumbnail files have two layers for managing pictures: **Thumbnail index** and **Thumbnail data**.

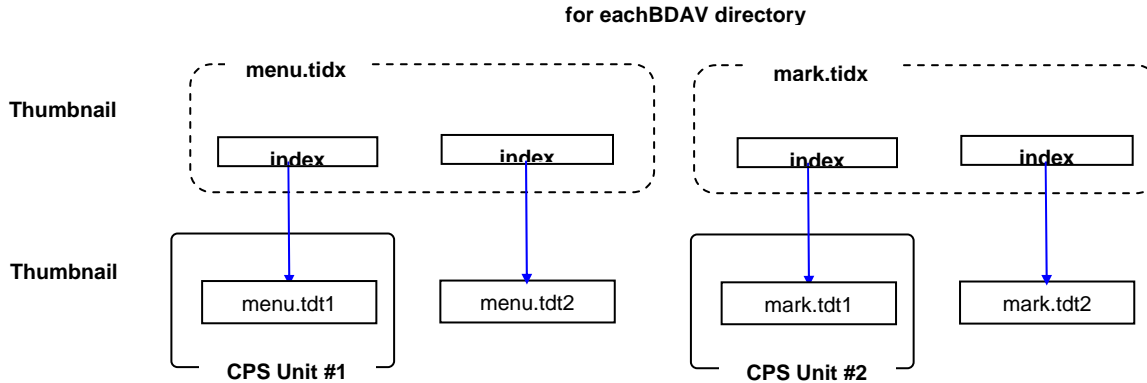


Figure 3-4 Application Format Structure and CPS Unit for BDAV Application

3.1.2.1 Clip

Each pair of an AV stream file and its attribute is considered to be one object. A Clip is an object consisting of a Clip AV stream file and its corresponding Clip information file. A Clip AV stream file stores data, which is basically an MPEG-2 transport stream defined in a structure conforming to *Blu-ray Disc Association, System Description Blu-ray Disc Read-Only Format, part 3: Audio Visual Basic Format Specifications, version 1.xx*. The Clip Information file stores the time stamps of the access point into the corresponding AV stream file. The Player reads the Clip Information to find out the position where it should begin to read the data from the AV stream file.

3.1.2.2 PlayList

A PlayList is a collection of playing intervals in the Clips. One such playing interval is called a PlayItem and consists of a pair of “IN-point and OUT-points” that point to positions on a time axis of the Clip. Therefore, a PlayList is a collection of PlayItems. Here the IN-point means a start point of a playing interval, and the OUT-point means an end point of the playing interval.

3.1.2.3 infoBDAV

Info.bdav file has the list of all PlayLists recorded in a BDAV directory.

3.1.2.4 menu.tidx and mark.tidx (Thumbnail Index File)

menu.tidx and mark.tidx has the index information for the thumbnail. menu.tidx includes the index information to the pictures used for the menu presentation. mark.tidx includes the index information to the pictures associated to the mark information assigned to the PlayLists and/or Clips.

3.1.2.5 menu.tdt1, menu.tdt2, mark.tdt1, and mark.tdt2 (Thumbnail Data File)

menu.tdt1 and menu.tdt2 contain the thumbnail picture data pointed to by the menu.tidx file. menu.tdt1 is encrypted by the Unit Key for the CPS_Unit associated to the menu thumbnail in a BDAV directory. menu.tdt2 is not encrypted.

mark.tdt1 and mark.tdt2 files contain the thumbnail picture data pointed to by the mark.tidx file. mark.tdt1 is encrypted by the Unit Key for the CPS_Unit associated to the mark thumbnail in a BDAV directory. mark.tdt2 is not encrypted.

3.1.2.6 CPS Unit for BDAV Application

A CPS Unit is assigned to each Clip, Menu Thumbnail, and Mark Thumbnail that are encrypted by using the Unit Key (Kcu) associated to the CPS Unit. Each CPS Unit has its corresponding CPS Unit CCI file. Each CPS Unit has a CPS_Unit_number. CPS_Unit_number values are defined in ascending order, starting from one. All the values of CPS_Unit_number shall be defined at least once on a disc.

Figure 3-5 shows the directory structure of BDAV application format. Detailed information is described in *Blu-ray Disc Association, System Description Blu-ray Disc Rewritable Format, part 3: Audio Visual Basic Format Specifications, version 2.xx*.

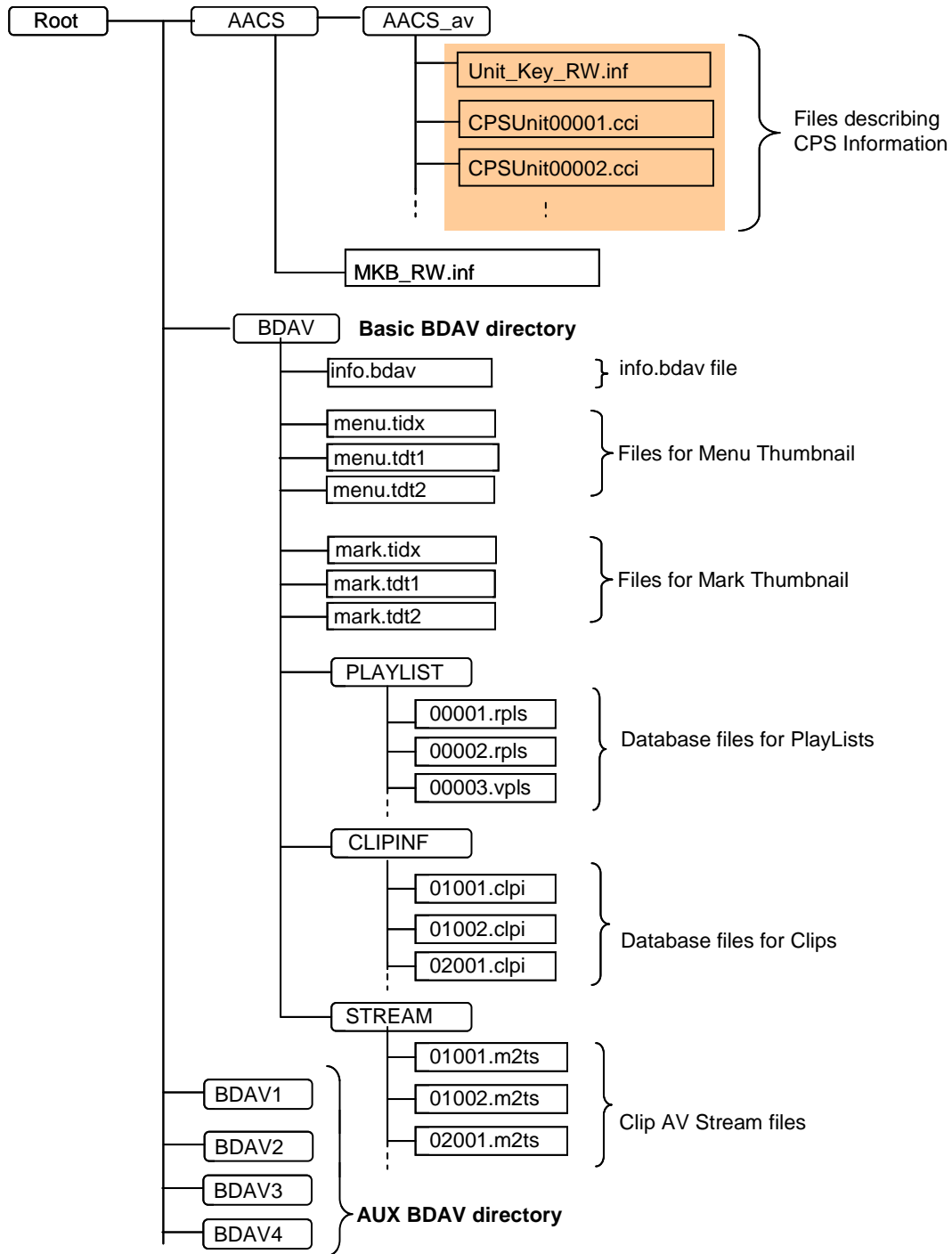


Figure 3-5 Directory structure for BDAV Application

All the AACS protected Clip AV stream files under “STREAM” directory, menu.tdt1, and mark.tdt1 files shall be encrypted in each BasicBDAV directory and AuxBDAV directory. Any other data under Basic BDAV directory and AuxBDAV directory shall not be encrypted.

3.1.2.6.1 CCI Sequence

In case of Clip AV stream file, CCI information corresponding to a specific segment of a CPS Unit may be different from each other. A sequence of source packets in which the status of copy control information (CCI) is constant is called a CCI sequence. A CPS Unit may contain one or more CCI sequences.

3.2 CPS Key File and CPS Usage File

3.2.1 CPS Unit Key File (Unit_Key_RW.inf) for BDMV Application

Each CPS_Unit on the BD Recordable Disc that is encrypted by AACS has a unique Unit Key. All Unit Keys on one disc shall be stored in the CPS Unit Key File “Unit_Key_RW.inf” in the “\AACS\AACS_mv” directory.

The following requirements are applied to the CPS Unit Key File to reserve enough size of continuous area for the CPS Unit Key File, and to avoid unexpected Read Modify Write operation to the ECC block that contains the CPS Unit Key File.

- The size of CPS Unit Key File shall be multiple of 65536 bytes.
- The CPS Unit Key File shall be allocated on an ECC block basis.

Table 3-1 shows the data structure for CPS Unit Key File for BDMV Application.

Table 3-1 Data Format of CPS Unit Key File for BDMV Application

Syntax	No. of bits	Mnemonic
CPS Unit Key File {		
Unit_Key_Block_start_address	32	uimsbf
reserved for future use	96	bslbf
Unit_Key_File_Header()		
For (I=0 ; I<X ; I++){	(*1)	
padding word#I	16	bslbf
}		
Unit_Key_Block()		
For (J=0 ; J<Y ; J++){	(*2)	
padding word#J	16	bslbf
}		
}		

(*1) X is used to align the start byte of Unit_Key_Block() to the 16 bytes boundary.

(*2) Y is used to align the end of CPS Unit Key File to the 65536 bytes boundary.

Unit_Key_Block_start_address field (32 bits) indicates the start address of Unit_Key_Block() in the relative byte number from the first byte of CPS Unit Key File. The value of Unit_Key_Block_start_address field shall be a multiple of 128.

Table 3-2 shows the data structure for Unit_Key_File_Header() of CPS Unit Key File for BDMV Application.

Table 3-2 Data Format of Unit_Key_File_Header() for BDMV Application

Syntax	No. of bits	Mnemonic
Unit_Key_File_Header(){		
Application_Type (= 01 ₁₆)	8	uimsbf
Num_of_BD_Directory (= 01 ₁₆)	8	uimsbf
(reserved)	16	bslbf
For(I=0; I < Num_of_BD_Directory; I++){		
CPS_Unit_number for First Playback#I	16	uimsbf
CPS_Unit_number for Top Menu#I	16	uimsbf
Num_of_Title#I	16	uimsbf
For(J=1; J < Num_of_Title+1; J++){		
(reserved)	16	bslbf
CPS_Unit_number for Title#J in Directory #I	16	uimsbf
}		
}		
}		

Application Type field (8 bits) indicates the type of AV Application that is used with the CPS Unit Key File. For BDMV Application, the value of Application Type shall be 1 to indicate that the CPS Unit Key File is associated to BDMV Application and the syntax complies with what is described in Table 3-2.

Num_of_BD_Directory field (8 bits) indicates the number of BD application directories recorded on the media. For BDMV Application, the value of Num_of_BD_Directory shall be 1, because BDMV Application uses only one directory (“\BDMV” directory).

CPS_Unit_number for First Playback#I field (16 bits) indicates the CPS Unit number that First Playback belongs to. If First Playback is not on the BD Recordable Disc, this field shall be set to 0000₁₆.

CPS_Unit_number for Top Menu#I field (16 bits) indicates the CPS Unit number that Top Menu belongs to. If Top Menu is not on the BD Recordable Disc, this field shall be set to 0000₁₆.

Num_of_Title#I field (16 bits) indicates the number of titles on the disc.

CPS_Unit_number for Title#J in Directory #I field (16 bits) indicates the CPS Unit number that each Title in the directory belongs to. If Title is not AACs encrypted, this field shall be set to 0000₁₆.

Table 3-3 shows the data structure for Unit_Key_Block() of CPS Unit Key File for BDMV Application.

Table 3-3 Data Format of Unit_Key_Block() for BDMV Application

Syntax	No. of bits	Mnemonic
Unit_Key_Block(){		
Num_of_CPS_Unit	16	uimsbf
(reserved)	112	bslbf
For(I=1; I < Num_of_CPS_Unit+1; I++){		
MAC of Media ID#I	128	bslbf
reserved for future use	128	bslbf
Encrypted CPS Unit Key for CPS Unit#I	128	bslbf
}		
}		

Num_of_CPS_Unit field (16 bits) indicates the number of CPS Units on the disc.

MAC of Media ID field contains the 128-bit MAC of Media ID by using CPS Unit Key for each CPS Unit. The Media ID MAC is generated as follows:

$$\text{CMAC}(K_{cu}, \text{Media ID}).$$

Encrypted CPS Unit Key field contains the 128 bits of the encrypted CPS Unit Key for each CPS Unit. The CPS Unit Key (K_{cu}) is encrypted as follows:

$$\text{AES-128E}(K_{pa}, K_{cu} \oplus \text{AES-H}(\text{CPS Unit Usage File}))$$

where K_{pa} denotes a Protected Area Key defined in Section 3.2 of the *Recordable Video Book* of this specification.

For Blu-ray Disc Recordable Media (BD-R), a recording device may insert additional Encrypted CPS Unit Key fields into the CPS Unit Key File when it first creates the CPS Unit Key File. These additional fields may be calculated using the same CPS Unit Key with different CPS Unit Usage Files. The CPS Unit Keys may be used for encrypting/decrypting content subsequently written on the media.

3.2.2 CPS Unit Key File (Unit_Key_RW.inf) for BDAV Application

Each CPS_Unit on the BD Recordable Disc that is encrypted by AACS has a unique Unit Key. All Unit Keys on one disc shall be stored in the CPS Unit Key File “Unit_Key_RW.inf” in the “\AACS\AACS_av” directory.

The following requirements are applied to the CPS Unit Key File to reserve enough size of continuous area for the CPS Unit Key File. This is to avoid unexpected Read Modify Write operations to the ECC block which contains the CPS Unit Key File.

- The size of CPS Unit Key File shall be a multiple of 65536 bytes.
- The CPS Unit Key File shall be allocated on an ECC block basis.

Table 3-4 shows the data structure for CPS Unit Key File for BDAV Application.

Table 3-4 Data Format of CPS Unit Key File for BDAV Application

Syntax	No. of bits	Mnemonic
CPS Unit Key File {		
Unit_Key_Block_start_address	32	uimbf
reserved for future use	96	bslbf
Unit_Key_File_Header()		
For (I=0 ; I<X ; I++){	(*1)	
padding word#I	16	bslbf
}		
Unit_Key_Block()		
For (J=0 ; J<Y ; J++){	(*2)	
padding word	16	bslbf
}		
}		

(*1) X is used to align the start byte of Unit_Key_Block() to the 16 bytes boundary.

(*2) Y is used to align the end of CPS Unit Key File to the 65536 bytes boundary.

Unit_Key_Block_start_address field (32 bits) indicates the start address of Unit_Key_Block() in the relative byte number from the first byte of CPS Unit Key File. The value of Unit_Key_Block_start_address field shall be a multiple of 128.

Table 3-5 shows the data structure for Unit_Key_File_Header() of CPS Unit Key File for BDAV Application.

Table 3-5 Data Format of Unit_Key_File_Header() for BDAV Application

Syntax	No. of bits	Mnemonic
Unit_Key_File_Header(){		
Application_Type (= 2 ₁₆)	8	uimsbf
Num_of_BD_Directory	8	uimsbf
(reserved)	16	bslbf
For(I=0; I < Num_of_BD_Directory; I++){		
CPS_Unit_number for Menu Thumbnail#I	16	uimsbf
CPS_Unit_number for Mark Thumbnail#I	16	uimsbf
Num_of_Clip#I	16	uimsbf
For(J=0; J < Num_of_Clip; J++){		
Clip_ID#J in Directory #I	16	uimsbf
CPS_Unit_number for Clip#J in Directory #I	16	uimsbf
}		
}		
}		

Application Type field (8 bits) indicates the type of AV Application that is used with the CPS Unit Key File. For the BDAV Application, the value of Application Type shall be 2, to indicate that the CPS Unit Key File is associated to the BDAV Application and the syntax complies with what is described in Table 3-5.

Num_of_BD_Directory field (8 bits) indicates the number of BD application directories recorded on the media. For the BDAV Application, the minimum value of Num_of_BD_Directory is 1. The maximum value of Num_of_BD_Directory is 5. This is because the BDAV Application uses one mandatory Basic BDAV directory (“\BDAV”) and 4 optional AuxBDAV Directories (“\BDAV1”, “\BDAV2”, “\BDAV3”, and “\BDAV4”).

CPS_Unit_number for Menu Thumbnail#I field (16 bits) indicates the CPS Unit number that the Menu Thumbnail of the associated BDAV directory belongs to. If Menu Thumbnail is not on the BD Recordable Disc, this field shall be set to 0000₁₆.

CPS_Unit_number for Mark Thumbnail#I field (16 bits) indicates the CPS Unit number that the Mark Thumbnail of the associated BDAV directory belongs to. If Mark Thumbnail is not on the BD Recordable Disc, this field shall be set to 0000₁₆.

Num_of_Clip#I field (16 bits) indicates the number of AACCS encrypted clips on the disc.

Clip_ID#J in Directory#I field (16 bits) indicates the number used in the file name of the AACCS encrypted Clip Information File. For example, Clip_ID#J in Directory #I = YYYYYY in decimal value for the Clip Information File of “YYYYYY.clpi”.

CPS_Unit_number for Clip#J in Directory #I field (16 bits) indicates the CPS Unit number that each AACCS encrypted Clip in the directory belongs to.

Table 3-6 shows the data structure for Unit_Key_Block() of CPS Unit Key File for BDAV Application.

Table 3-6 Data Format of Unit_Key_Block() for BDAV Application

Syntax	No. of bits	Mnemonic
Unit_Key_Block(){		
Num_of_CPS_Unit	16	uimsbf
(reserved)	112	bslbf
For(I=1; I < Num_of_CPS_Unit+1; I++){		
MAC of Media ID#I	128	bslbf
reserved for future use	128	bslbf
Encrypted CPS Unit Key for CPS Unit#I	128	bslbf
}		
}		

Num_of_CPS_Unit field (16 bits) indicates the number of CPS Units on the disc.

MAC of Media ID field contains the 128bit MAC of Media ID by using CPS Unit Key for each CPS Unit. The MAC of Media ID is generated as follows:

$$\text{CMAC}(K_{cu}, \text{Media ID}).$$

Encrypted CPS Unit Key field contains the 128 bits of the encrypted CPS Unit Key for each CPS Unit. The CPS Unit Key (K_{cu}) is encrypted as follows:

$$\text{AES-128E}(K_{pa}, K_{cu} \oplus \text{AES-H}(\text{CPS Unit Usage File}))$$

where K_{pa} denotes a Protected Area Key defined in Section 3.2 of the *Recordable Video Book* of this specification.

For Blu-ray Disc Recordable Media (BD-R), a recording device may insert additional Encrypted CPS Unit Key fields into the CPS Unit Key File when it first creates the CPS Unit Key File. These additional fields may be calculated using the same CPS Unit Key with different CPS Unit Usage Files. The CPS Unit Keys may be used for encrypting/decrypting content subsequently written on the media.

3.2.3 Backup of CPS Unit Key File

According to section 2.4.1 of the *Recordable Video Book* of this specification, the backup CPS Unit Key File is recorded during updating of the CPS Unit Key File.

The backup CPS Unit Key File “BAK_Unit_Key.inf” shall be stored in the “\AACS\AACS_mv” directory or in the “\AACS\AACS_av” directory. The syntax of backup CPS Unit Key File is the same as CPS Unit Key File, and the contents of backup CPS Unit Key File is exactly the same as the contents of CPS Unit Key File at the time when the backup encrypted CPS Unit Key File is generated.

Details and the usage of the backup encrypted CPS Unit Key File are defined in Section 2.4.1 of the *Recordable Video Book* of this specification,

3.2.4 CPS Unit Usage File (CPSUnitXXXXX.cci)

Each CPS_Unit on BD Recordable Discs that is encrypted by AACS has an associated CPS Unit Usage file. CPS Unit Usage file is the Usage Rules for the BD Recordable Disc and describes the CCI and related information of each CPS Unit. The details of the Usage Rules are described in Section 2.5 of the *Recordable Video Book* of this specification. Each CPS Unit Usage file “CPSUnitXXXXX.cci” associated to a CPS Unit shall be stored in the “\AACS\AACS_mv” directory or in the “\AACS\AACS_av” directory. Here, XXXXX shall be the 5-digit number. XXXXX shall be equal to the CPS Unit number to which the CCI file is associated. The extension shall be “cci”.

For Blu-ray Disc Recordable Media (BD-R), a recording device may store multiple CPS Unit Usage Files when the CPS Unit Key File is first created. Each CPS Unit Usage File may have different settings of Usage Rules.

Table 3-7 shows the data structure for the CPS Unit Usage File.

Table 3-7 Data Structure for the CPS Unit Usage File

Byte	Bit	7	6	5	4	3	2	1	0		
0	:	Primary Header								16 bytes	2048 bytes
15	:	Primary CCI Area								2032 bytes	
16	:	Secondary Header								16 bytes	(2048*N) bytes : Option
2047	:	Secondary CCI Area								(2048*N-16) bytes	
2048	:										
2064	:										
2065	:										
2048*N-1	:										

Primary Header (16 bytes) includes the number of CCI loops in the Primary CCI Area.

Primary CCI Area (2032 bytes) includes one or more CCI_and_other_info() blocks.

Secondary Header (16 bytes) includes the number of CCI loops in the Secondary CCI Area.

Secondary CCI Area (2048*N -16 bytes) includes one or more CCI_and_other_info() blocks.

(Note) The data structure after Byte 2048 is an Option. However, if a Secondary CCI Area is used, the structure in Table 3-7 shall be used. The player shall refer to the Primary CCI Area. If the Secondary CCI Area is on the disc, the player may refer to the both CCI Areas.

Table 3-8 shows the syntax for the CPS Unit Usage File.

Table 3-8 Syntax for the CPS Unit Usage File

Syntax	No. of bits	Mnemonics	Data Block
CPS Unit Usage File {			-
Number_of_Primary_CCI_loops	16	uimsbf	Primary Header
(reserved)	112	bslbf	
for(I=0; I< Number_of_Primary_CCI_loops; I++){			Primary CCI Area
CCI_and_other_info()			
}			
(reserved)	X (*1)	bslbf	
			-
Number_of_Secondary_CCI_loops	16	uimsbf	Secondary Header
(reserved)	112	bslbf	
for(I=0; I< Number_of_Secondary_CCI_loops; I++){			Secondary CCI Area
CCI_and_other_info()			
}			
(reserved)	Y (*2)	bslbf	
}			-

(*1) X is used to fill the Primary CCI Area (2032 bytes)

(*2) Y is used to fill the Secondary CCI Area (2048*N-16 bytes)

Number_of_Primary_CCI_loops indicates the number of CCI_and_other_info() blocks in the Primary CCI Area.

Number_of_Secondary_CCI_loops indicates the number of CCI_and_other_info() blocks in the Secondary CCI Area.

3.2.4.1 CCI_and_other_info()

CCI_and_other_info() contains CCI and title usage information for each CPS Unit.

Table 3-9 shows the data structure for CCI_and_other_info().

Table 3-9 Syntax for CCI_and_other_info()

Syntax	No. of bits	Mnemonic
CCI_and_other_info() {		
CCI_and_other_info_type	16	uimsbf
CCI_and_other_info_version	16	uimsbf
CCI_and_other_info_data_length	16	uimsbf
CCI_and_other_info_data()	L*8	
}		

CCI_and_other_info_type indicates what type of CCI and related information of a CPS Units is described in CCI_and_other_info_data(). CCI_and_other_info_type of each CCI_and_other_info() stored in the same CPS Unit Usage File shall be different values. Table 3-10 shows the bit assignment of CCI_and_other_info_type.

Table 3-10 Bit assignment for CCI_and_other_info_type

CCI_and_other_info_type	Meaning
0000 ₁₆	Reserved
0001 ₁₆	Reserved for Basic CCI for BD-CPS
0002 ₁₆ -0100 ₁₆	Reserved
0101 ₁₆	Basic CCI for AACS
0102 ₁₆	CCI Sequence Information
0103 ₁₆ -0110 ₁₆	Reserved
0111 ₁₆	Reserved for Basic Title Usage for AACS
0112 ₁₆	Reserved for Key Management Information for Network Transaction
0113 ₁₆ -FFFF ₁₆	Reserved

Basic CCI for AACS (CCI_and_other_info_type=0101₁₆) is used to describe the basic CCI information for AACS. CCI information corresponding to a specific segment of a CPS Unit may be different from each other. In this case, CCI information for the specific segment of a CPS Unit may be described as CCI Sequence Information. Basic CCI for AACS shall contain the most restrictive CCI information in each segment within a CPS Unit. Basic CCI for AACS shall be contained in the Primary CCI Area.

CCI Sequence Information (CCI_and_other_info_type=0102₁₆) is used to describe the CCI information for the specific segment of the CPS Unit. Note that the CCI Sequence Information is optional for the BD Recordable Disc. If the CCI Sequence Information is used, a compliant recorder shall record it according to CCI information of the recording source. A compliant player may use CCI Sequence Information. If the CPS_Unit is assigned for Thumbnail of BDAV Application, CCI Sequence Information shall not be recorded in this CPS Unit Usage File.

CCI_and_other_info_version indicates the version number of CCI_and_other_info_data() for each CCI_and_other_info_type. This value is defined for each CCI_and_other_info_type.

CCI_and_other_info_data_length indicates the byte length of CCI_and_other_info_data() for each CCI_and_other_info_type. This values is defined for each CCI_and_other_info_type.

CCI_and_other_info_data() is the description area for CCI and related information of a CSP Unit. The structure of this field is separately defined for each CCI_and_other_info_type.

The length of the CCI_and_other_info() field in the Primary CCI Area shall be less than or equal to 2012 bytes. The Primary CCI Area may contain multiple different types of CCI_and_other_info().

The Secondary CCI Area may also contain multiple different types of CCI_and_other_info(). The Secondary CCI Area can contain the CCI_and_other_info() that can not be stored in the Primary CCI Area. When the size of CCI_and_other_info() that is greater than 2012 bytes, the CCI_and_other_info() shall be stored in the Secondary CCI Area.

3.2.4.2 Basic CCI for AACs

Table 3-11 shows the data structure of CCI_and_other_info() for Basic CCI for AACs. Note that the Basic CCI for AACs is mandatory for the BD Recordable Disc.

Table 3-11 Syntax of Basic CCI for AACs

Syntax	No. of bits	Mnemonics
Basic CCI for AACCS {		
CCI_and_other_info_type (=0101 ₁₆)	16	uimsbf
CCI_and_other_info_version (=0100 ₁₆)	16	uimsbf
CCI_and_other_info_data_length (=0010 ₁₆)	16	uimsbf
(reserved)	5	bslbf
EPN	1	bslbf
CCI	2	bslbf
(reserved)	2	bslbf
Trusted_Input	1	bslbf
Image_Constraint_Token	1	bslbf
Digital_Only_Token	1	bslbf
APS	3	bslbf
(reserved)	112	bslbf
}		

CCI_and_other_info_type shall be 0002₁₆ for Basic CCI for AACCS.

CCI_and_other_info_version shall be 0100₁₆ for this version.

CCI_and_other_info_data_length shall be 0010₁₆ for Basic CCI for AACCS.

The EPN field indicates the value of the Encryption Plus Non-assertion (EPN). Table 3-12 shows the meaning of EPN.

Table 3-12 EPN

EPN	Meaning
0 ₂	EPN-asserted
1 ₂	EPN-unasserted

If the CPS_Unit is assigned for the Thumbnail of the BDAV Application, this EPN field shall be set to 0₂, and this field shall be ignored.

The CCI field indicates the value of the copy control information. Table 3-13 shows the meaning of CCI.

Table 3-13 CCI

CCI	Meaning
00 ₂	Copy Control Not Asserted
01 ₂	No More Copy
10 ₂	Reserved
11 ₂	Reserved

The Trusted_Input field indicates if the input is trusted. Table 3-14 shows the meaning of Trusted_Input. Details of the assertion and the use of this field is defined in the AACCS Compliance Rules.

Table 3-14 Trusted_Input

Trusted_Input	Meaning
0 ₂	Input may not be trusted.
1 ₂	Input is trusted.

The Image_Constraint-Token field indicates the value of Image Constraint Token. Table 3-15 shows the meaning of Image_Constraint-Token. If the CPS_Unit is assigned for Thumbnail of the BDAV Application, this Image_Constraint-Token field shall be set to 0₂, and this field shall be ignored.

Table 3-15 Image_Constraint-Token

Image_Constraint-Token	Meaning
0 ₂	High Definition Analog Output in the form of Constrained Image
1 ₂	High Definition Analog Output in High Definition Analog Form

The Digital_Only-Token field indicates the value of the Digital Only Token. Table 3-16 shows the meaning of the Digital_Only-Token.

Table 3-16 Digital_Only-Token

Digital_Only-Token	Meaning
0 ₂	Output of decrypted content is allowed for Analog/Digital Outputs
1 ₂	Output of decrypted content is allowed only for Digital Outputs

The APS field indicates the value of analog copy protection information. Table 3-17 shows the meaning of APS.

Table 3-17 APS

APS	Meaning
000 ₂	APS off
001 ₂	APS 1 on: type 1 (AGC)
010 ₂	APS 1 on: type 2 (AGC + 2L colourstripe)
011 ₂	APS 1 on: type 3 (AGC + 4L colourstripe)
100 ₂ -101 ₂	reserved
110 ₂ -111 ₂	APS2 on

3.2.4.3 CCI Sequence Information

Table 3-18 shows the data structure of CCI_and_other_info() for CCI Sequence Information.

Table 3-18 Syntax of CCI Sequence Information

Syntax	No. of bits	Mnemonics
CCI Sequence Information {		
CCI_and_other_info_type (=0102 ₁₆)	16	uimsbf
CCI_and_other_info_version (=0100 ₁₆)	16	uimsbf
CCI_and_other_info_data_length	16	uimsbf
(reserved)	3	
Number of CCI sequence	5	uimsbf
For (I = 0 ; I < Number of CCI sequence ; I++){		bslbf
(reserved)	2	
Start SPN for CCI Sequence	30	bslbf
(reserved)	5	
EPN	1	bslbf
CCI	2	bslbf
(reserved)	2	bslbf
Trusted_Input	1	bslbf
Image_Constraint_Token	1	bslbf
Digital_Only_Token	1	bslbf
APS	3	bslbf
(reserved)	80	bslbf
}		bslbf
}		

CCI_and_other_info_type shall be 0005₁₆ for CCI Sequence Information.

CCI_and_other_info_version shall be 0100₁₆ for this version.

CCI_and_other_info_data_length shall be the value of 2 plus 16 times “Number of CCI Sequence”.

Number of CCI Sequence indicates the number of the CCI Sequence in the corresponding CPS Unit. Number of CCI Sequence shall be equal to or less than 25.

Start SPN for CCI Sequence indicates the source packet number of where CCI information has been changed. Source packet number is defined in *Blu-ray Disc Association, System Description Blu-ray Disc Rewritable Format, part 3: Audio Visual Basic Format Specifications, version 2.xx*, and it is 32bits. Start PN for CCI Sequence is calculated as right 2bit shifted value of source packet number. Start SPN for CCI Sequence value in the first loop of this structure shall be 0. When the actual number of CCI-sequence is greater than 25, each

CCI and other information data for I = 24 shall indicate the most restrictive CCI from Start SPN for CCI Sequence for I = 24 to the last source packet of the Clip.

The semantics for EPN, CCI, Trusted_Input, Image_Constraint-Token, and APS is the same as Basic CCI for AACCS described in 3.2.4.2.

3.3 Encrypted Packs

3.3.1 Encryption Scheme for Clip AV Stream

When AACCS protection is applied to the Clip AV Stream files under the “\BDAV” or “\BDMV” directories, encryption is applied to every Aligned Unit in the file. An Aligned Unit consists of 32 MPEG source packets. Each MPEG source packet consists of the TP_extra_header(4 bytes) and an MPEG Transport packet(188 bytes). The total size of an Aligned Unit is 6144 bytes, which is equal to the size of 3 logical sectors.

The final 6128 bytes of each Aligned Unit are encrypted using the Block Key and AES-128CBCE. A new CBC cipher chain is started for each Aligned Unit. (see Figure 3-6).



Figure 3-6 CBC chaining on “Aligned Unit” basis

The Initialization Vector of CBC Mode used in this scheme is described in Section 2.1.2 of the Introduction and Common Cryptographic Elements of this specification.

The first 16 bytes of each Aligned Unit is used as the seed for calculating the Block Key. Calculation method for the Block key is described in Figure 3-7.

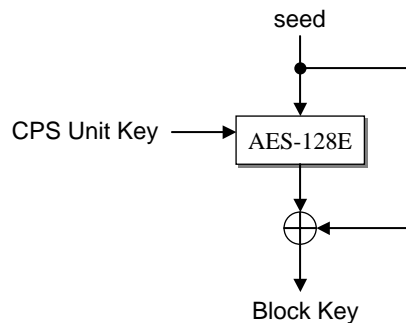


Figure 3-7 Calculation method for the Block Key

3.3.1.1 Copy Permission Indicator

MPEG source packet in Clip AV Stream file consists of the TP_extra_header(4 bytes) and an MPEG Transport packet(188 bytes). Table 3-19 shows the data structure for the TP_extra_header.

Table 3-19 TP_extra_header

Syntax	No. of bits	Mnemonic
--------	-------------	----------

TP_extra_header {		
Copy_permission_indicator	2	unimsbf
Arrival_time_stamp	30	unimsbf
}		

Copy_permission_indicator shall be set to 11b. Copy permission for each CPS Unit follows a corresponding Usage Rule described in CPS Unit Usage File.

3.3.2 Encrypted Scheme for Thumbnail data

The thumbnail file under “\BD\AV” directory is encrypted for each tn_sub_block. Data in the thumbnail file consists of tn_blocks (16384 bytes each). Each tn_block is composed of 8 tn_sub_blocks (2048 bytes each). And every tn_sub_block is composed of a 16-byte unencrypted portion and a 2032-byte encrypted portion. The 16-byte data in the unencrypted portion is used as the Block-Seed. Figure 3-8 illustrates the structure mentioned above.

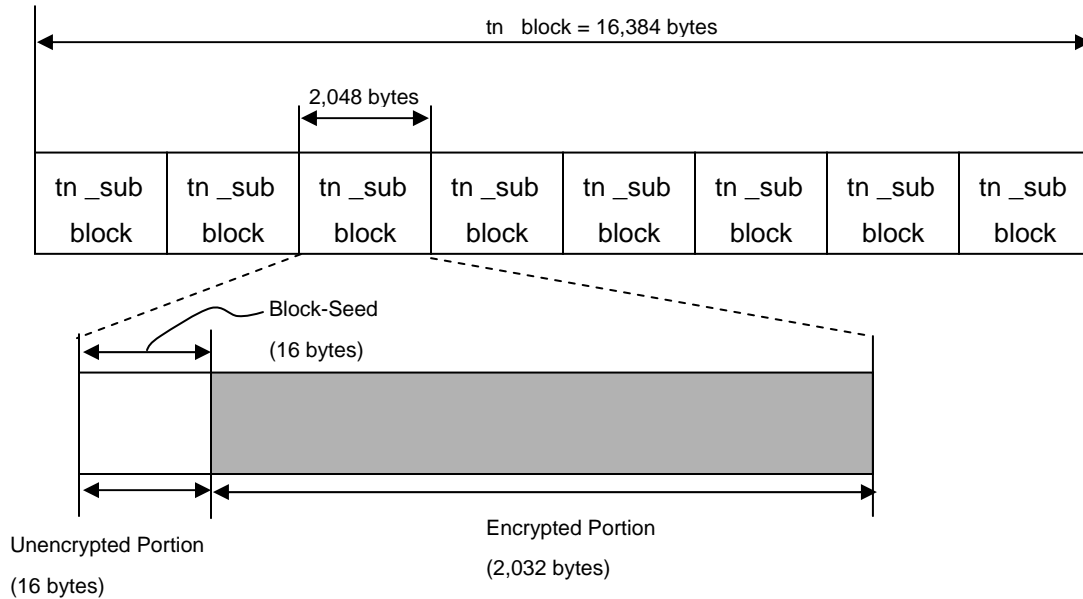


Figure 3-8 Data Format for tn_block

When AACS protection is applied to thumbnail files under the “\BD\AV” directory, encryption is applied to every `tn_sub_block` in the file. The final 2032 bytes of each `tn_sub_block` is encrypted using the Block Key and AES-128CBCE. A new CBC cipher chain is started for each `tn_sub_block` (see Figure 3-9).



Figure 3-9 CBC chaining on “tn_sub_block” basis

The Initialization Vector of CBC Mode used in this scheme is described in Section 2.1.2 of *Introduction and Common Cryptographic Elements* of this specification.

The first 16 bytes of each `tn_sub_block` is used as the seed for calculating the Block Key. Calculation method for the Block key is described in Figure 3-7.

3.4 Embedded CCI in AV Contents

3.4.1 Embedded CCI for Self-Encoded Stream Format of BDAV Application

The Self-Encoded Stream Format (SESF) shall contain the `SESF_copy_control_descriptor` in order to carry the up-dated CCI status and its related information as Embedded CCI.

The position of `SESF_copy_control_descriptor` in AV Contents is defined in *Blu-ray Disc Association, System Description Blu-ray Disc Rewritable Format, part 3: Audio Visual Basic Format Specifications, version 2.xx*.

Data Structure of `SESF_copy_control_descriptor` is same as `copy_status_descriptor` which is described in Table 3-20.

3.4.2 Embedded CCI for Digital Recording of BDAV Application

In order to carry the updated CCI status and its related information for Digital Broadcasting Streams, this specification applies `ATSC_CA_descriptor` specified by ATSC, document A/70.

This descriptor is called the “`copy_status_descriptor`” in this specification. The Data Structure of `copy_status_descriptor` is described in Table 3-20.

3.4.3 Embedded CCI for BDMV Application

As specified in *Blu-ray Disc Association, System Description Blu-ray Disc Read-Only Format, part 3: Audio Visual Basic Format Specification, version 1.xx*, `HDMV_copy_control_descriptor` shall be embedded in AV Contents.

The `HDMV_copy_control_descriptor` is used for the DTCP and contains the same fields and the same meaning defined in accordance with the `DTCP_descriptor` specified in *Digital Transmission Content Protection Specification Volume 1 Revision 1.4*.

Data Structure of `HDMV_copy_control_descriptor` is same as `copy_status_descriptor` which is described in Table 3-20. The information recorded in the CPS Unit Usage File defined in 3.2.4 and this `HDMV_copy_control_descriptor` shall be consistent.

3.4.4 Data Structure of Copy Status Descriptor

The `copy_status_descriptor` is used in the recording, as mentioned in 3.4.1, 3.4.2 and 3.4.3, and contain the same fields and the same meaning defined in accordance with the `DTCP_descriptor` specified in *Digital Transmission Content Protection Specification Volume 1 Revision 1.4*. Table 3-20 presents the syntax. For AACS compliant player and recorder implementation, the information recorded in the CPS Unit Usage File defined in 3.2.4 has priority rather than the information recorded in Embedded CCI.

Table 3-20 copy_status_descriptor

Syntax	No. of bits	Mnemonics
copy_status_descriptor {		
descriptor_tag	8	uimsbf
descriptor_length	8	uimsbf
CA_System_ID	16	uimsbf
for (I = 0 ; I < descriptor_length - 2 ; I++){		
private_data_byte	8	bslbf
}		
}		

Descriptor_tag field (1 byte) shall be set to 88_{16} . Descriptor_length (1 byte) indicates the number of bytes immediately following this field and up to the end of this descriptor. CA_System_ID (2 bytes) shall be set to $0FFF_{16}$.

3.4.4.1.1 private_data_byte

Table 3-21 shows the data format for private_data_byte.

Table 3-21 private_data_byte

Syntax	No. of bits	Mnemonics
private_data_byte {		
(reserved)	1	bslbf
Retention_Move_Mode	1	bslbf
Retention_State	3	bslbf
EPN	1	bslbf
CCI	2	bslbf
(reserved)	5	bslbf
Image_Constraint-Token	1	bslbf
APS	2	bslbf
}		

Retention_Move_mode and Retention_State are defined in the DTCP_descriptor, but these fields are not used in this specification.

EPN field indicates the value of the Encryption Plus Non-assertion (EPN) as shown in Table 3-22.

Table 3-22 EPN

EPN	Meaning
0 ₂	EPN-asserted
1 ₂	EPN-unasserted

CCI field indicates the value of the copy control information as shown as Table 3-23.

Table 3-23 CCI

CCI	Meaning
00 ₂	Copy Control Not Asserted
01 ₂	No More Copy
10 ₂	Copy One Generation
11 ₂	Reserved

Image_Constraint-Token field indicates the value of the Image_Constraint-Token as shown in Table 3-24.

Table 3-24 Image_Constraint_Token

Image_Constraint_Token	Meaning
0 ₂	High Definition Analog Output in the form of Constrained Image
1 ₂	High Definition Analog Output in High Definition Analog Form

APS field indicates the value of the analog copy protection information as shown in Table 3-25

Table 3-25 APS

APS	Meaning
00 ₂	copy control not asserted
01 ₂	APS on: type 1 (AGC)
10 ₂	APS on: type 2 (AGC + 2L colourstripe)
11 ₂	APS on: type 3 (AGC + 4L colourstripe)

Reserved bits are reserved for future definition and currently defined to have a value of one.

Annex A. Treatment of each CCI

A.1 Cognizant Recording and Non-Cognizant Recording

A.1.1 Cognizant Recording

In the case of Cognizant Recording, Embedded CCI shall be recognized by a recording device and updated before recording. This means that Embedded CCI and CCI Sequence Information in the CPS Unit Usage File shall be identical.

A.1.2 Non-Cognizant Recording

In the case of Non-Cognizant Recording, Embedded CCI may not be recognized and may not be updated before recording. Table A-1 shows the allowable and prohibited combination of CCI in CCI Sequence Information and Embedded CCI on the Recordable media. Note that Image_Constraint_Token of CCI Sequence Information in the CPS Unit Usage File shall be set to 0₂, And APS of CCI Sequence Information in the CPS Unit Usage File shall not be set to 00₂.

Table A-1 The combination between CCI in CCI Sequence Information and Embedded CCI

CCI in CCI Sequence Information		Embedded CCI				
		Copy Control Not Asserted 00 ₂		No More Copy 01 ₂	Copy One Generation 10 ₂	Copy Never 11 ₂
		EPN unasserted 1 ₂	EPN asserted 0 ₂			
Copy Control Not Asserted 00 ₂	EPN unasserted 1 ₂	Allowed	Prohibited [1]	Prohibited [1]	Prohibited [1]	Prohibited [2]
No More Copy 01 ₂	Don't care	Allowed	Allowed	Prohibited [3]	Allowed [4]	Prohibited [2]

[1] The CCI or EPN in CCI Sequence Information shall not indicate a situation which is less severe than the Embedded CCI.

[2] “Copy Never” content shall not be allowed on Recordable media.

[3] “No More Copy” content shall not be allowed to copy any more.

[4] This combination is allowable for only Non-Cognizant recording. In the case of Cognizant recording; Embedded CCI shall be updated before recording.

A.2 Cognizant Playback and Non-Cognizant Playback

A.2.3 Cognizant Playback

In the case of Cognizant Playback, each source packet can be processed according to the Embedded CCI except for the combination of: Embedded CCI is “Copy One Generation” and CCI in CCI Sequence Information is “No More Copy”. The source packet with the above combination will be processed as “No More Copy”.

A.2.4 Non-Cognizant Playback

In case of Non-Cognizant Playback, each source packet will be processed according to CCI in CCI Sequence Information or CCI in Basic CCI for AACCS.

Annex B. Carriage of System Renewability Message

B.1 Introduction

This chapter describes the method to store the System Renewability Message (SRM) on the BD Recordable Disc in the case where an SRM is to be stored on the BD Recordable Disc.

B.2 SRM for DTCP

SRM for DTCP “DTCP.srm” shall be stored in the root directory.

B.3 SRM for HDCP

SRM for HDCP “HDCP.srm” shall be stored in the root directory.