Advanced Access Content System (AACS)

Blu-ray Disc Recordable Book

Intel Corporation
International Business Machines Corporation
Microsoft Corporation
Panasonic Corporation
Sony Corporation
Toshiba Corporation
The Walt Disney Company
Warner Bros.

Revision 0.951
Final
September 28, 2009

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, Microsoft Corporation, Panasonic 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

This page is intentionally left blank.

List of Figures

This page is intentionally left blank.

List of Tables

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 AACS Recordable 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), Blu-ray Disc Recordable Media (BD-R), CPRM compliant recordable media (DVD-R, DVD-RW and DVD-RAM), "Koninklijke Philips Electronics, DVD+R Part 1 Single Layer and Part 2 Dual Layer" (hereafter referred to as +R) and "Koninklijke Philips Electronics, DVD+RW Basic Format Specifications Part 1 and Part2" (hereafter referred to as +RW).

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 all kinds of physical media, i.e. Blu-ray Disc Rewritable Media (BD-RE), Blu-ray Disc Recordable Media (BD-R), CPRM compliant recordable media (DVD-R, DVD-RW and DVD-RAM), +R and +RW. BD-R has 2 recording modes that are defined as "Sequential Recording Mode with Logical Over Write (SRM with LOW)" and "Sequential Recording Mode without Logical Over Write (SRM without LOW)". Blu-ray Disc media types are categorized to the AACS "rewritable media" and "write once media" as follows:

- "rewritable media" described in the Recordable Video Book of this specification
  - BD-RE
  - BD-R initialized for SRM with LOW mode
  - DVD-RW of CPRM compliant recordable media
  - DVD-RAM of CPRM compliant recordable media
  - +RW
- "write once media" described in the Recordable Video Book of this specification
  - BD-R initialized for SRM without LOW mode
  - DVD-R of CPRM compliant recordable media
  - +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 Content on AACS Recordable Media.

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 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

AACS LA, Recordable Video Book

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 2.1

Blu-ray Disc Association, System Description Blu-ray Disc Rewritable Format, part 3: Audio Visual Basic Format Specifications, version 2.1

Blu-ray Disc Association, System Description Blu-ray Disc Rewritable Format, part 3: Audio Visual Basic Format Specifications, version 3.0

Blu-ray Disc Association, System Description Blu-ray Disc Recordable Format, part 1: Basic Format Specifications, version 1.2

Blu-ray Disc Association, System Description Blu-ray Disc Recordable Format, part 2: File System Specifications, version 1.1

DVD Forum, DVD Specifications for Rewritable Disc, Part 1 Physical Specifications Ver2.2 with Optional Specifications

DVD Forum, DVD Specifications for Rewritable Disc, Part 2 File System Specifications Ver2.0

DVD Forum, DVD Specifications for Re-recordable Disc, Part 1 Physical Specifications Ver1.2 with Optional Specifications

DVD Forum, DVD Specifications for Re-recordable Disc, Part 2 File System Specifications Ver1.0

DVD Forum, DVD Specifications for Re-recordable Disc for Dual Layer, Part 1 Physical Specifications Ver2.0

DVD Forum, DVD Specifications for Re-recordable Disc for Dual Layer, Part 2 File System Specifications Ver2.0

Koninklijke Philips Electronics, DVD+RW Basic Format Specifications Part 1: Single layer, Volume 1: 2.4x & 4x Version 1.3

Koninklijke Philips Electronics, DVD+RW Basic Format Specifications Part 1: Single layer, Volume 2: 8x Version 1.0

Koninklijke Philips Electronics, DVD+RW Basic Format Specifications Part 2: Dual layer, Volume 1: 2.4x Version 1.0

Blu-ray Disc Association, System Description AVCREC Recordable Format, part 2: File System Specifications (UDF®), version 1.0

Blu-ray Disc Association, System Description AVCREC Rewritable Format, part 2: File System Specifications (UDF®), version 1.0

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

DVD Forum, DVD Specifications for Recordable Disc for General, Part 1 Physical Specifications Ver2.1 with Optional Specifications

DVD Forum, DVD Specifications for Recordable Disc for General, Part 2 File System Specifications Ver2.1

DVD Forum, DVD Specifications for Recordable Disc for Dual Layer, Part 1 Physical Specifications Ver3.0 with Optional Specifications

DVD Forum, DVD Specifications for Recordable Disc for Dual Layer, Part 2 File System Specifications Ver3.0

Koninklijke Philips Electronics, DVD+R Part 1 Single Layer: DVD+R 4.7 Gbytes, Basic Format Specifications Version 1.3

Koninklijke Philips Electronics, DVD+R Part 2 Dual Layer: DVD+R 8.5 Gbytes, 8x Basic Format Specifications Version 1.1

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

4C Entity, LLC, *CPRM Specification: Introduction and Common Cryptographic Elements, Revision 1.0*

4C Entity, LLC, *CPRM Media Verification Book, Revision 0.9*

1.5 Document History

This document version 0.951 adds editorial errata to 0.95 which superseded version 0.921 dated August 5, 2008. It contained editorial improvements since the 0.921 version, plus the following changes:

- Red laser recording is supported.

1.6 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.

1.7 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. Unless otherwise specified, all the bits of reserved field in the syntax of data structure shall be set to 0_2. 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.

1.8 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
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

2.1.1 BD-R / RE

The Media ID shall be stored in the Burst Cutting Area (BCA) of BD-R / RE.

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

(Note) For the BD-R / RE, the Licensed 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-R / RE

Bit / 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 Licensed Player, Licensed Recorder or Licensed Drive 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 00000100_2.

Content Code field (6 bits) indicates the application identifier, and is set to 000001_2 for discs protected by AACS.

Data Unit sequence number field (2 bits) indicates the data unit sequence number, and is set to 00_2 for Media ID.

Content Sub Identifier field (4 bits) indicates sub application identifier in an AACS protected disc, and is set to 0001_2 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 E_{16}.

Category field (4 bits) contains the disc category, and is set to 0000_2 for Blu-ray Disc Rewritable Media (BD-RE) and set to 0001_2 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.

2.1.2 CPRM compliant recordable media

The detail of 64-bit Media Identifier on the CPRM compliant recordable media is specified in the *CPRM Media Verification Book.*

For AACS protection, the 64-bit CPRM Media Identifier on CPRM compliant recordable media is expanded to a 128-bit as follows:

128-bit Media ID =$25B946EBC0B36173_{16}$ || 64-bit CPRM Media Identifier

If AACS Drive Authentication, as specified in Chapter 4 of the *Introduction and Common Cryptographic Elements* book, is used for exchange of the Media ID, this expansion shall be done in the Licensed Drive side, so that the same command set, as specified in Chapter 4 of the *Introduction and Common Cryptographic Elements* book, is utilized.

Licensed Recorders, which support CPRM compliant recordable media, shall also have a “CPRM Device Key Set” and shall verify the correctness of the CPRM Media Key (derived from CPRM MKB) by using the Verification Data in the Verify Media Key Record in the CPRM MKB.

(Note 1) The Licensed Drive shall handle the CPRM compliant recordable media as AACS compliant disc, if the 64-bit CPRM Media Identifier is recorded on the disc.

(Note 2) The 64-bit CPRM Media Identifier, which is read from CPRM compliant recordable media by use of READ DISC STRUCTURE Command with Format Code 06_{16}, shall not be used to calculate Media ID.

2.1.3 +R and +RW

The Media ID shall be calculated from the Disc ID 1 and the Disc ID 2 as follows:

128-bit Media ID = AES-H(Disc ID 1 || Disc ID 2)

If AACS Drive Authentication, as specified in Chapter 4 of the *Introduction and Common Cryptographic Elements* book, is used for exchange of the Media ID, this calculation shall be done in the Licensed Drive side, so that the same command set, as specified in Chapter 4 of the *Introduction and Common Cryptographic Elements* book, is utilized.

On +R media, Disc ID 1 represents the 256-bits Disc ID that is contained in the first Session Disc Control Block (SDCB) that is stored in the Inner Disc Identification Zone of the Lead-in. On +RW media, Disc ID 1 represents the 256-bits Disc ID that is contained in the Format Disc Control Block (FDCB) that is stored in the Inner Disc Identification Zone of the Lead-in.

Disc ID 2 consists of 40bits. The Licensed Player, Licensed Recorder or Licensed Drive shall regard the all zero value as an invalid Disc ID 2. Copies of Disc ID 2 shall be stored in the RSV field of Data Frames having

a Physical Sector Number in the ranges $2FE10_{16}..2FEEF_{16}$ and $2FF10_{16}..2FFEF_{16}$. Copies of Disc ID 2 may optionally be stored in the RSV field of Data Frames having a Physical Sector Number in the ranges $2FE00_{16}..2FE0F_{16}$, $2FEF0_{16}..2FF0F_{16}$, and $2FFF0_{16}..2FFFF_{16}$.

Table 2-2 shows the data format of the Disc ID 2 in the RSV field in specific sectors of Buffer Zone 2.

Disc ID 1 and Disc ID 2 shall be recorded on the disc as follows:

Blank +R media. When the host issues the READ DISC STRUCTURE Command (Format Code 82_{16}) to request the Media ID, the Licensed Drive behavior shall be as follows:

1. The Licensed Drive shall generate Disc ID 1 and Disc ID 2 as two non-zero pseudo random values.
2. The Licensed Drive shall open the first session and record the first SDCB (containing Disc ID 1).
3. The Licensed Drive shall record Buffer Zone 2 on the media, as well as the first ECC Block of the Data Zone.
4. The Licensed Drive shall return the Media ID calculated from Disc ID 1 and Disc ID 2 to the host.

If there is any error during recording of Buffer Zone 2 and the SDCB, the Licensed Drive shall terminate the READ DISC STRUCTURE Command with CHECK CONDITION Status, 5/6F/01 ILLEGAL REQUEST/COPY PROTECTION KEY EXCHANGE FAILURE - KEY NOT PRESENT.

+R media containing a Reserved Track. In this case, the first SCDB has previously been recorded (namely when the first session was opened). When the host issues the READ DISC STRUCTURE Command (Format Code 82_{16}) to request the Media ID, the Licensed Drive behavior shall be as follows:

1. The Licensed Drive shall read Disc ID 1 from the first SDCB.
2. The Licensed Drive shall generate Disc ID 2 as a non-zero pseudo random value.
3. The Licensed Drive shall record Buffer Zone 2 on the media, as well as the first ECC Block of the Data Zone.
4. The Licensed Drive shall return the Media ID calculated from Disc ID 1 and Disc ID 2 to the host.

If there is any error during recording of Buffer Zone 2, the Licensed Drive shall terminate the READ DISC STRUCTURE Command with CHECK CONDITION Status, 5/6F/01 ILLEGAL REQUEST/COPY PROTECTION KEY EXCHANGE FAILURE - KEY NOT PRESENT.

(Partially) formatted +RW media. When the host issues the READ DISC STRUCTURE Command (Format Code 82_{16}) to request the Media ID, the Licensed Drive behavior shall be as follows:

1. The Licensed Drive shall read Disc ID 1 from the FDCB.
2. The Licensed Drive shall read Disc ID 2 from Buffer Zone 2. If Disc ID 2 is invalid (i.e. the all-zero value), the Licensed Drive shall generate Disc ID 2 as a non-zero pseudo random value.
3. The Licensed Drive shall record Buffer Zone 2 on the media and update Physical format information in the Control Data Zone accordingly.
4. The Licensed Drive shall return the Media ID calculated from Disc ID 1 and Disc ID 2 to the host.

If there is any error during recording of Buffer Zone 2, the Licensed Drive shall terminate the READ DISC STRUCTURE Command with CHECK CONDITION Status, 5/6F/01 ILLEGAL REQUEST/COPY PROTECTION KEY EXCHANGE FAILURE - KEY NOT PRESENT.

Table 2-2 Data Format for Disc ID 2 in RSV field

Byte \ Bit	7	6	5	4	3	2	1	0
0	Reserved							
1	(msb)							
:	Disc ID 2							
5								(lsb)

(Note) The Licensed Drive shall handle all +R discs as AACS Recordable Media, except those discs that contain an invalid Disc ID 2. In addition, the Licensed Drive shall handle all formatted +RW discs as AACS Recordable Media. If the Licensed Drive has loaded an unformatted +RW disc, the AACS Feature shall not be active (i.e. the Current bit shall be set to zero). Once the +RW disc is at least partially formatted (such as when a Quick Start Formatting operation is in progress), it becomes AACS Recordable Media, and consequently the AACS Feature shall become active (i.e. the Current bit shall be set to one).

(Note) When Quick Start Formatting a +RW disc, the Licensed Drive shall record Disc ID 1 in the FDCB and Disc ID 2 in Buffer Zone 2 before the disc is ejected.

2.2 Binding Nonce

2.2.1 BD-R / RE

The Binding Nonce is stored in the Protected Area of the BD-R / RE, and is used to calculate the Protected Area Key as described in Section 3.2 of the *Recordable Video Book* of this specification. For BD-R / RE, the Binding Nonce shall be stored in the User Control Data associated with the first logical Sector of the CPS Unit Key File and shall be non-zero value. The details of the Protocol for Reading / Writing the Binding Nonce is described in Section 4.7 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-R / RE.

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)

(Note) The first bit of User Control Data is reserved for a Bus Encryption Flag (BEF). This bit is not used for this specification, although the same media may be used for AACS *Blu-ray Disc Prepared Video Book.* See

Section 3.5.1 of the AACS *Blu-ray Disc Prepared Video Book,* for the media incorporated with the AACS Content protected by AACS *Blu-ray Disc Prepared Video Book.*

2.2.2 CPRM compliant recordable media, +R and +RW

For CPRM compliant recordable media, +R and +RW, the all zero 128-bit value is used for Binding Nonce. Note that the host does not use REPORT Key command (Key Format 100000_2 and 100001_2) and uses all zero 128-bit value as Binding Nonce.

Note that same fixed value shall be used as Binding Nonce, even if Title Key File is being modified. This also means that Secure Move of AACS Content, defined in Section 3.5.1 of the *Recordable Video Book* of this specification, is prohibited.

2.3 Media Key Block

Each BD Recordable Disc that contains AACS Content [using a CPS Unit Key that is provided in the AACS directory] includes Media Key Block (MKB) for BDAV Application and/or MKB for BDMV Application. The MKB is used to grant playback of AACS Content. Note that if a Licensed Recorder records AACS Content on a BD Recordable Disc without corresponding MKB for the Application, the Licensed Recorder shall write the MKB on the disc.

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" for BDAV Application shall be stored in the "\AACS" directory for BD-R/RE or in the "\AACS_bd" directory for CPRM compliant recordable media, +R and +RW. The MKB "MKB_RW_mv.inf" for BDMV Application shall be stored in the "\AACS_mv" directory. For BDAV Application, a Licensed Recorder is required to update "MKB_RW.inf" and corresponding CPS Unit Key File. Similarly, for BDMV Application, a Licensed Recorder is required to update "MKB_RW_mv.inf" and corresponding CPS Unit Key File. A Licensed Player without AACS recording function is not required to update the MKB.

A Licensed Recorder shall update the MKB stored in its non-volatile memory, if the Licensed Recorder encounters newer MKB on each supported media as listed below.

- BD-ROM with BDMV protected by AACS
- BD-R with BDAV or BDMV protected by AACS
- BD-RE with BDAV or BDMV protected by AACS
- CPRM compliant recordable media with BDAV protected by AACS
- +R and +RW with BDAV protected by AACS

In addition to the above, if a Licensed Recorder supports to record BDAV on CPRM compliant recordable media, +R and +RW protected by AACS and does not support to playback BDMV on BD-ROM, this Licensed Recorder shall update the MKB stored in its non-volatile memory, when the Licensed Recorder supports the playback of DVD-Video and encounters newer MKB on DVD-ROM with DVD-Video as the file "MKB.inf" under "\AACS" directory.

The MKB stored in rewritable media defined in Section 1.1 is updatable, while the MKB stored in write once media defined in Section 1.1 is not.

2.4 Backup of Media Key Block

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

The temporary MKB "BAK_MKB.inf" for BDAV Application shall be stored in the "\AACS" directory for BD-R/RE and in the "\AACS_bd" directory for CPRM compliant recordable media, +R and +RW. The temporary MKB "BAK_MKB.inf" for BDMV Application shall be stored in the "\AACS_mv" 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 temporary MKB is generated.

Details and the usage of the temporary 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.

2.5 Partial Media Key Block for Host Revocation List

The Licensed Drive shall update the Host Revocation List (HRL) stored in its non-volatile memory, if the Licensed Drive encounters newer HRL on each supported media as listed below.

- BD-ROM protected by AACS
- BD-R protected by AACS
- BD-RE protected by AACS
- CPRM compliant recordable media protected by AACS
- +R and +RW protected by AACS

Update process for each media is described in subsections.

2.5.1 BD-R / RE

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-R / RE, 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-R / RE 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-R / RE is one megabyte.

Table 2-3 shows the data format for the BD HRL Record which is recorded in the Lead-in area of BD-R / RE.

Table 2-3 BD HRL Record Format

Bit / Byte	7	6	5	4	3	2	1	0
0	Additional Record Type: 31_{16}							
1	Additional Record Length							
2								
3								
4	Partial Media Key Block							
5								
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, and excluding padding.

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

Table 2-4 shows the data format for the Partial Media Key Block which is included in the BD HRL Record.

Table 2-4 Partial Media Key Block Format

Bit / Byte	7	6	5	4	3	2	1	0
0	Type and Version Record							
…								
11								
12	Host Revocation List Record							
13								
14								
…								
X								

The Licensed Drive with BD-R/RE reading function is required to store only the Partial Media Key Block in its non-volatile memory. In other words, the Licensed 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 Licensed 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 3.2.5.1.2 of the *Introduction and Common Cryptographic Elements* book of this specification.

For the BD-R / RE which does not have the BD HRL Record in the Lead-in area, the Licensed 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 Licensed Drive with recording function. The Additional Record Type and the Additional Record Length shall be generated by the Licensed Drive with recording

function to form the BD HRL Record using the Partial Media Key Block stored in non-volatile memory of the Licensed 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 Licensed Drive with recording function, the Licensed 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 Licensed Drive with recording function.

The behavior for Licensed Drive is as follows:

In case that the Licensed Drive cannot verify the BD HRL Record on the media, the Licensed Drive shall read the Partial Media Key Block stored in non-volatile memory of the Licensed Drive and use it for the authentication process. In case that the Licensed 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 Licensed Drive and use it for the authentication process. Note that the Licensed 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 Licensed Drive with recording function. Notwithstanding the foregoing, the Licensed Drive with recording function might not update the BD HRL Record in the Lead-in area if the Licensed Drive cannot write it for some reason (e.g. media error).

2.5.2 CPRM compliant recordable media

CPRM MKB in the Lead-in Area may include the Type and Version Record and the Host Revocation List (HRL) Record. In the case that the CPRM MKB contains the Type and Version Record and the HRL Record, these two Records always follow the last Conditionally Calculate Media Key Record. If no Conditionally Calculate Media Key Records are present, then these two Records follow the Calculate Media Key Record. Both of the Type and Version Record as well as the HRL Record shall precede the End of Media Key Block Record. Implementations shall not assume fixed record positioning for the Type and Version Record and the HRL Record.

In case of CPRM compliant recordable media, the Partial Media Key Block may be pre-recorded in the media, and the Licensed Drive need not to update the HRL in the media by one in non-volatile memory, even if the HRL in non-volatile memory is newer than one in the media.

On the other hand, the Licensed Drive shall update the HRL in non-volatile memory by one in the media, if the HRL in the media is correctly verified and newer than one in the media.

The behavior for Licensed Drive is as follows:

In case that the Licensed Drive cannot find or verify HRL Record on the media, the Licensed Drive shall read the Partial Media Key Block stored in non-volatile memory of the Licensed Drive and use it for the authentication process. In case that the Licensed Drive cannot read the HRL Record on the media for some reason, it shall read the Partial Media Key Block stored in non-volatile memory of the Licensed Drive and use it for the authentication process.

2.5.3 +R and +RW

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 +R / +RW, the

original of BD HRL Record and the duplicate of BD HRL Record shall be stored in the Buffer Zone 2 of Lead-in. The same data is written twice and these data shall be recorded from PSN $02FE11_{16}$ and $02FF11_{16}$.

(Note) The maximum size of reserved area for BD HRL Record on +R / +RW is 446 kilobytes for each of the two copies.

For the data format of the BD HRL Record, refer Section 2.5.1 of this specification.

The Licensed Drive with +R / +RW reading function is required to store only the Partial Media Key Block in its non-volatile memory. In other words, the Licensed 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 Licensed 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 3.2.5.1.2 of the *Introduction and Common Cryptographic Elements* book of this specification.

For the +R / +RW media which does not have the BD HRL Record in the Lead-in area, the Licensed Drive with recording function shall write the BD HRL Record on the disc, when Media ID is requested. The Additional Record Type and the Additional Record Length shall be generated by the Licensed Drive with recording function to form the BD HRL Record using the Partial Media Key Block stored in non-volatile memory of the Licensed Drive with recording function.

On the other hand, for the +RW media 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 Licensed Drive with recording function, the Licensed Drive with recording function shall generate the BD HRL Record using its Partial Media Key Block and write it on the media, when Media ID is requested.

The behavior for Licensed Drive is as follows:

In case that the Licensed Drive cannot verify the BD HRL Record on the media, the Licensed Drive shall read the Partial Media Key Block stored in non-volatile memory of the Licensed Drive and use it for the authentication process. In case that the Licensed 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 Licensed Drive and use it for the authentication process. Note that the Licensed Drive with recording function shall update the BD HRL Record in the Lead-in area when Media ID is requested. Notwithstanding the foregoing, the Licensed Drive with recording function might not update the BD HRL Record in the Lead-in area if the Licensed Drive cannot write it for some reason (e.g. media error).

This page is intentionally left blank.

Chapter 3
Details for Content Encryption and Decryption

3. Introduction

The general approach for encryption and decryption of AACS Content 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 Rewritable Format, part 3: Audio Visual Basic Format Specifications, version 3.0*, which has a format for realtime recording and editing by using BDMV Application Format. AACS encryption specified in this book can be applied to only the format for realtime recording and editing.

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

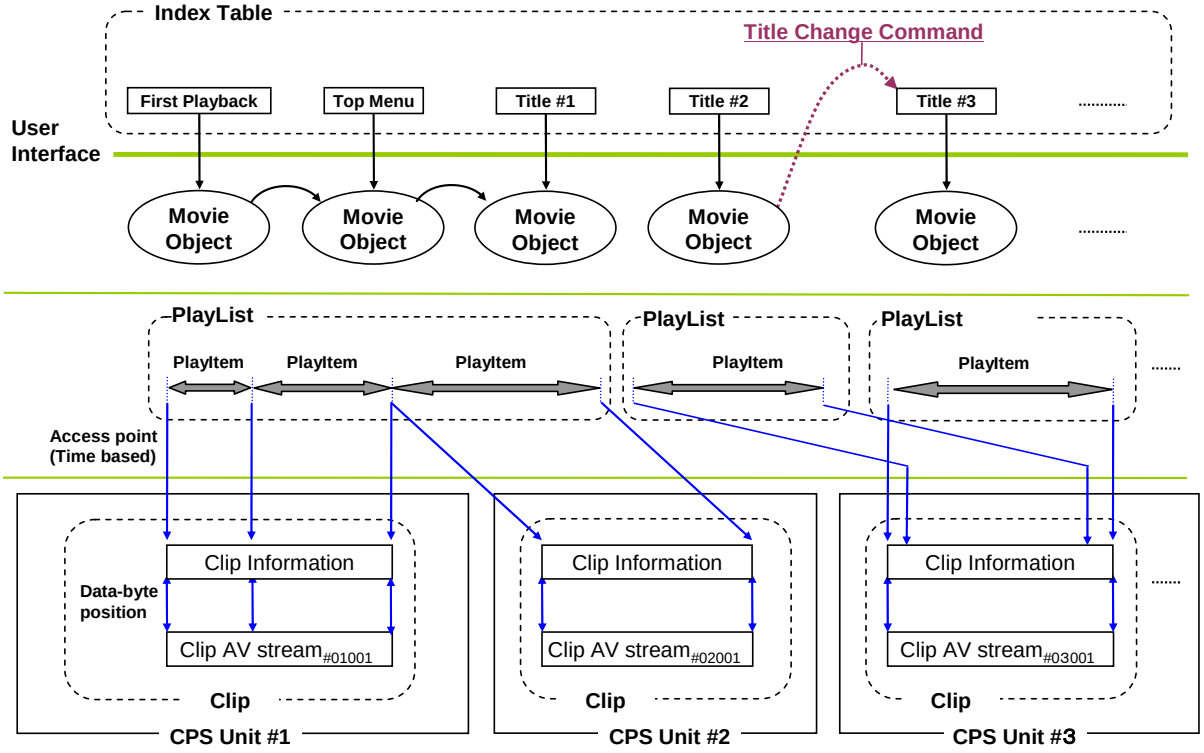

Figure 3-1 Application Format Structure and CPS Unit for BDMV Application

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 Rewritable Format, part 3: Audio Visual Basic Format Specifications, version 3.0*. 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 begins 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-point" 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 Move 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 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.

3.1.1.5 First Playback

First Playback may be optionally defined in the Index Table and points to a Movie 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. First Playback Movie Object is an optional function. A disc may or may not contain First Playback Movie Object.

3.1.1.6 Top Menu

Top Menu may be optionally defined in the Index Table and points to a Movie 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.

3.1.1.7 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. The 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.

3.1.1.8 CPS Unit for BDMV Application

A CPS Unit is assigned to each Clip, which is encrypted by using the CPS Unit Key (Kcu) associated to the CPS Unit. Two different Clips shall not belong to same CPS Unit. Each CPS Unit has its corresponding CPS Unit Usage file. Each CPS Unit has a CPS_Unit_number. CPS_Unit_number values shall be in the range of 1~200, and the Unit_Key_File_Header() in CPS Unit Key File defines the all CPS Unit number currently used for BDMV Application. CPS Unit Key File for BDMV Application is defined in Section 3.2.1 of this specification.

A Clip AV stream assigned as Main TS and a Clip AV stream assigned as Sub TS may coexist if IG stream is used as Sub TS for menu purpose. In this case, a Licensed Player shall apply a Usage Rule for Main TS to both Clip AV streams. Note that when encrypting/decrypting the CPS Unit Key for Main TS and Sub TS, the corresponding Usage Rule shall be used for each calculation of CPS Unit Key, i.e. AES-H(Usage Rules for Sub TS) shall be used for calculating of CPS Unit Key for Sub TS. Detailed information of Main TS, Sub TS and IG stream is described in *Blu-ray Disc Association, System Description Blu-ray Disc Rewritable Format, part 3: Audio Visual Basic Format Specifications, version 3.0.*

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 Rewritable Format, part 3: Audio Visual Basic Format Specifications, version 3.0.*

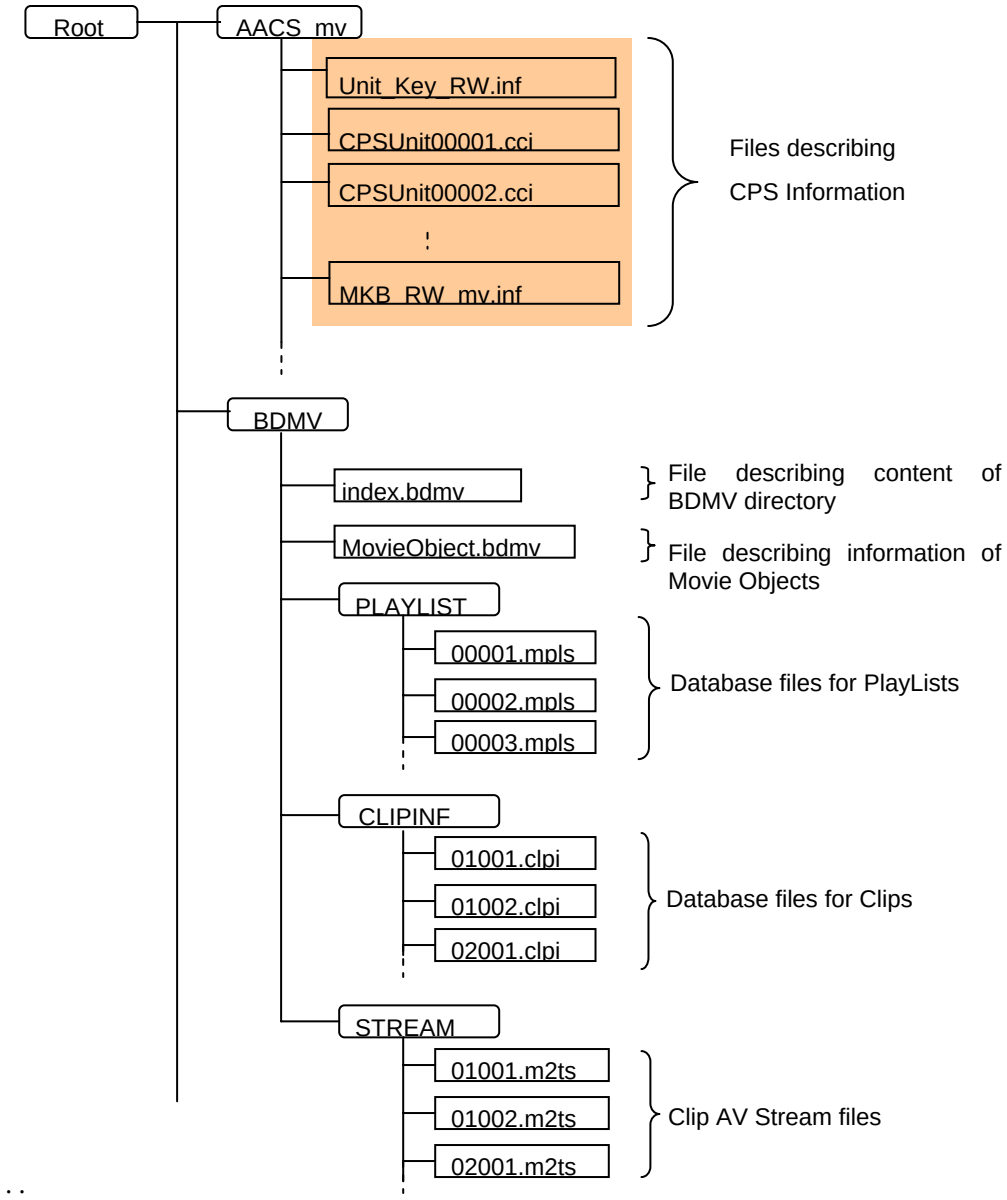

Figure 3-2 Directory structure for BDMV Application

Note that AACS shall be applied to only Clip AV stream files under "\BDMV\STREAM" directory. Any other data under BDMV directory shall not be encrypted. There may be both encrypted Clip AV stream files and unencrypted Clip AV stream files on a BD Recordable Disc.

3.1.1.8.1 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.

3.1.2 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 2.0*.

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

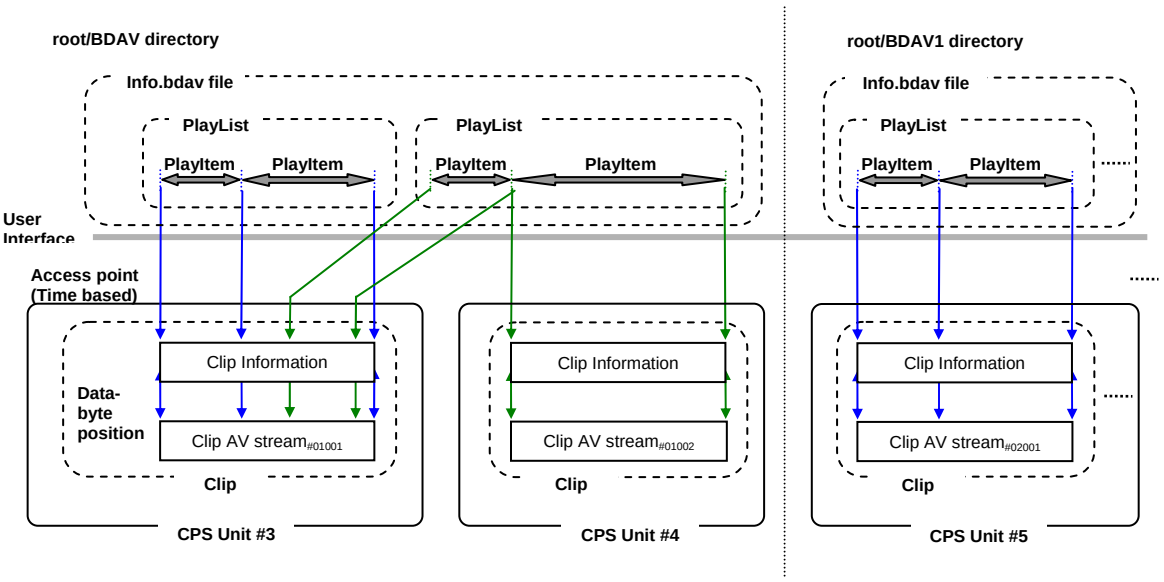

Figure 3-3 Application Format Structure and CPS Unit for BDAV Application

This application format has two layers for managing AV stream files: PlayList and Clip. BDAV Application files are stored in the "\BDAV" directory called "Basic BDAV" 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.

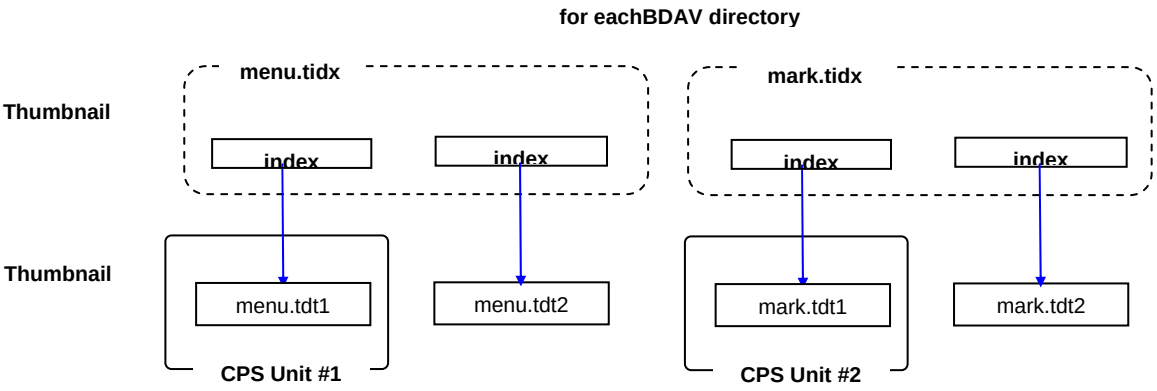

Figure 3-4 Application Format Structure and CPS Unit for BDAV Application

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 Rewritable Format, part 3: Audio Visual Basic Format Specifications, version 2.0.* 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 begins 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-point" 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 CPS Unit Key (Kcu) associated to the CPS Unit. Two different Clips shall not belong to same CPS Unit. Each CPS Unit has its corresponding CPS Unit Usage file. Each CPS Unit has a CPS_Unit_number. CPS_Unit_number values shall be in the range of 1~202, and the Unit_Key_File_Header() in CPS Unit Key File defines the all CPS Unit number currently used for BDAV Application. CPS Unit Key File for BDAV Application is defined in Section 3.2.2 of this specification.

Figure 3-5 shows the directory structure of BDAV Application Format for BD-R/RE media. In case of CPRM compliant recordable media, +R and +RW, the directory "\AACS_bd" is used instead of "\AACS". Detailed information is described in *Blu-ray Disc Association, System Description Blu-ray Disc Rewritable Format, part 3: Audio Visual Basic Format Specifications, version 2.0*.

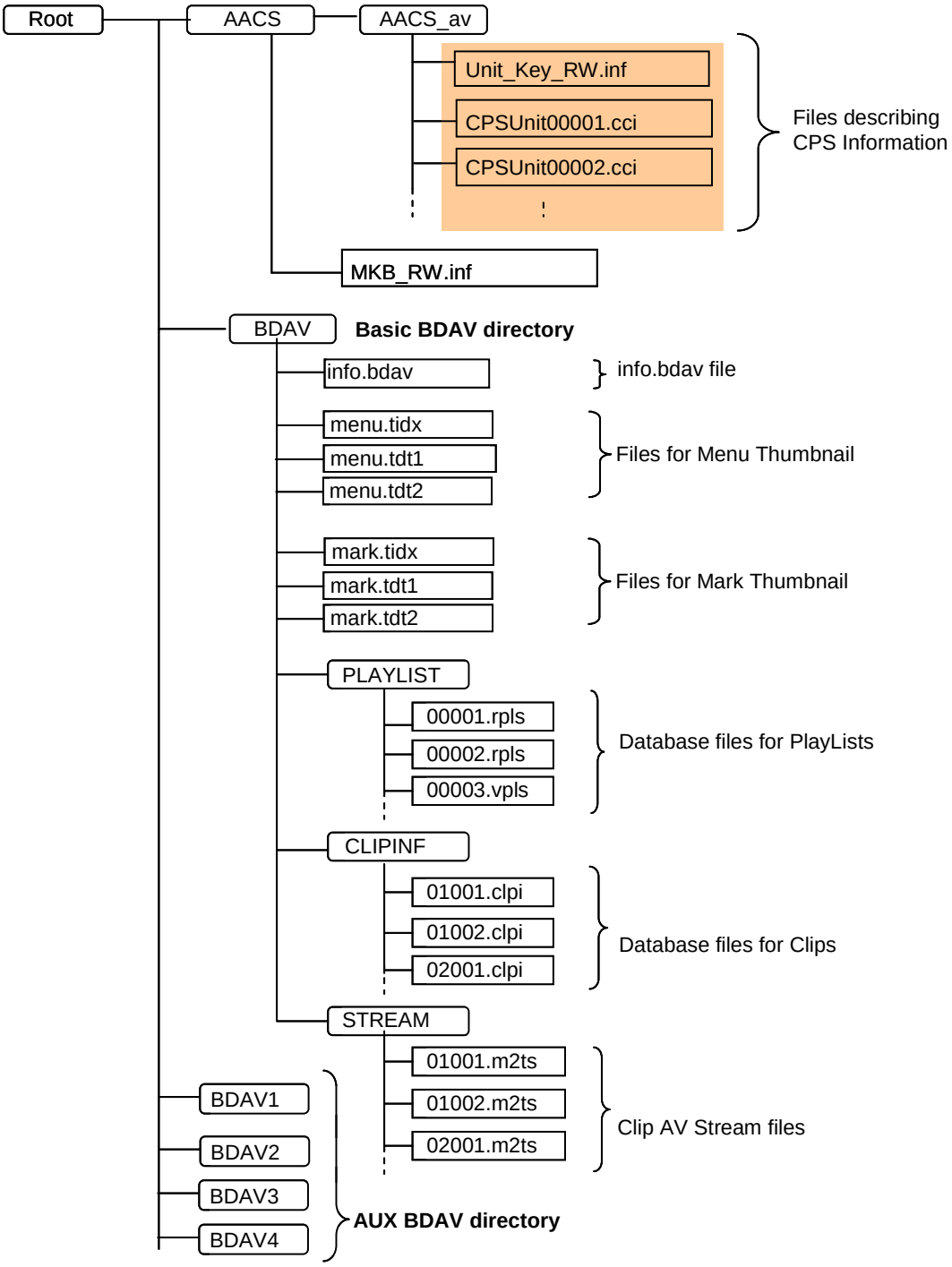

Figure 3-5 Directory structure for BDAV Application

Note that AACS shall be applied to only Clip AV stream files under “STREAM” directory, menu.tdt1, and mark.tdt1 files. Any other data under Basic BDAV directory and Aux BDAV directory shall not be encrypted. There may be both encrypted Clip AV stream files and unencrypted Clip AV stream files on a BD Recordable Disc.

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 CPS Unit Key. All Unit Keys on one disc shall be stored in the CPS Unit Key File “Unit_Key_RW.inf” in the “\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 (size of padding word) shall be such a value less than 8 that Unit_Key_Block() begins at 16-byte boundary.

(*2) Y (size of padding word) shall be such a value less than 32768 that the size of CPS Unit Key File becomes multiple of 65536-byte 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 16.

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 (= 03_{16})	8	uimsbf
Num_of_BD_Directory (= 01_{16})	8	uimsbf
(reserved)	16	bslbf
For(I=0; I < Num_of_BD_Directory; I++){		
(reserved)	16	uimsbf
(reserved)	16	uimsbf
Num_of_Clip#I	16	uimsbf
For(J=1; J < Num_of_Clip+1; J++){		
Clip_ID#J in Directory#I	16	bslbf
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 BDMV Application on the BD Recordable Disc, the value of Application Type shall be 3 to indicate that the CPS Unit Key File is associated to BDMV Application on the BD Recordable Disc 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).

Num_of_Clip#I field (16 bits) indicates the number of AACS encrypted Clips on the disc. The maximum number of AACS encrypted Clips on the disc is 200.

Clip_ID#J in Directory#I field (16 bits) indicates the number used in the file name of the AACS encrypted Clip. For the AACS encrypted Clip, this number shall be the value between 0 to 65535. For example, Clip_ID#J in Directory #I shall be set to 3039_{16} (12345 in decimal value) for the Clip Information file of "12345.clpi". If a Clip_ID of actually recorded Clip is not listed, the Licensed Player shall not treat the corresponding Clip as AACS encrypted Clip.

CPS_Unit_number for Clip#J in Directory #I field (16 bits) indicates the CPS Unit number that each AACS encrypted Clip in the directory belongs to. The value of this field shall be in the range of 1~200.

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. The maximum number of CPS Units on the disc is 200.

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:

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

In case of a PC-based system, this Media ID for AACS use shall be retrieved from the disc by use of the procedure as defined in the Section 4.6 of *Introduction and Common Cryptographic Elements* book of this specification.

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:

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

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

For write once media defined in Section 1.1, a Licensed Recorder 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 shall be calculated using the same CPS Unit Key with different CPS Unit Usage Files. The CPS Unit Keys may be used for encrypting/decrypting AACS Content subsequently written on the media.

Note: In the case that the CPS Unit number is not recorded in Unit_Key_File_Header() but Unit_Key_Block() has the information for that unused CPS Unit, MAC of Media ID#I and Encrypted CPS Unit Key for CPS Unit#I for the unused CPS Unit is not used and treated as invalid data. For example, if the Licensed Recorder deleted one Clip and associated CPS Unit became unused, the data space for that CPS Unit in Unit_Key_Block() shall remain as invalid data.

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 for BD-R/RE and "\AACS_bd\AACS_av" directory for CPRM compliant media, +R and +RW.

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	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	16	bslbf
}		
}		

(*1) X (size of padding word) shall be such a value less than 8 that Unit_Key_Block() begins at 16-byte boundary.

(*2) Y (size of padding word) shall be such a value less than 32768 that the size of CPS Unit Key File becomes multiple of 65536-byte 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 16.

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 (= 02_{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 Aux BDAV 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 0000_{16}.

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 0000_{16}.

Num_of_Clip#I field (16 bits) indicates the number of AACS encrypted Clips on the disc. The maximum number of Clips in BDAV directory is limited to 200, and the maximum number of AACS encrypted Clips on the disc is also 200.

Clip_ID#J in Directory#I field (16 bits) indicates the number used in the file name of the AACS encrypted Clip Information file. For the AACS encrypted Clip Information file, this number shall be the value between 0 to 65535. For example, Clip_ID#J in Directory #I shall be set to 3039_{16} (12345 in decimal value) for the Clip Information file of "12345.clpi". If a Clip_ID of actually recorded Clip is not listed, the Licensed Player shall not treat the corresponding Clip as AACS encrypted Clip.

CPS_Unit_number for Clip#J in Directory #I field (16 bits) indicates the CPS Unit number that each AACS encrypted Clip in the directory belongs to. The value of this field shall be in the range of 1~202.

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. The maximum number of CPS Units on the disc is 202.

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:

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

In case of a PC-based system, this Media ID for AACS use shall be retrieved from the disc by use of the procedure as defined in the Section 4.6 of *Introduction and Common Cryptographic Elements* book of this specification.

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:

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

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

For write once media defined in Section 1.1, a Licensed Recorder 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 shall be calculated using the same CPS Unit Key with different CPS Unit Usage Files. The CPS Unit Keys may be used for encrypting/decrypting AACS Content subsequently written on the media.

Note: In the case that the CPS Unit number is not recorded in Unit_Key_File_Header() but Unit_Key_Block() has the information for that unused CPS Unit, MAC of Media ID#I and Encrypted CPS Unit Key for CPS Unit#I for the unused CPS Unit is not used and treated as invalid data. For example, if the Licensed Recorder deleted one Clip and associated CPS Unit became unused, the data space for that CPS Unit in Unit_Key_Block() shall remain as invalid data.

3.2.3 Backup of CPS Unit Key File

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

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

Details and the usage of the temporary 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_mv" directory, in the "\AACS\AACS_av" directory or in the "\AACS_bd\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 write once media defined in Section 1.1, a Licensed Recorder 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 **:** **15**	Primary Header								16 bytes	2048 bytes
16 **:** **2047**	Primary CCI Area								2032 bytes	
2048 **:** **2064**	Secondary Header								16 bytes	(2048*N) bytes : Option
2065 **:** **2048*(N+1)-1**	Secondary CCI Area								(2048*N-16) bytes	

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 Licensed Player shall refer to the Primary CCI Area. If the Secondary CCI Area is on the disc, the Licensed 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=0101_{16}) 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=0102_{16}) 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 Licensed Recorder shall record it according to CCI information of the recording source. A Licensed Player shall use the most restrictive CCI information or 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.

If there is an unknown (Reserved) CCI_and_other_info_type, Licensed Player shall ignore this CCI_and_other_info( ).

If there is a higher version of CCI_and_other_info_version than the version supported by Licensed Player, Licensed Player shall ignore this CCI_and_other_info( ).

If reserved bits in each CC_and_other_info_data( ) are not set to zero, Licensed Player shall ignore these bits and only use non-reserved bits.

Note: If the Licensed Player cannot find the supporting version of Basic CCI for AACS, the Licensed Player shall not start playback of the AACS Content.

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 AACS {		
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)	1	bslbf
Move_Not_Allowed	1	bslbf
Trusted_Source_Mark_Screening_Required	1	bslbf
Image_Constraint_Token	1	bslbf
Digital_Only_Token	1	bslbf
APSTB	3	bslbf
(reserved)	112	bslbf
}		

CCI_and_other_info_type shall be 0101_{16} for Basic CCI for AACS.

CCI_and_other_info_version shall be 0100_{16} for this version.

CCI_and_other_info_data_length shall be 0010_{16} for Basic CCI for AACS.

The EPN field indicates the value of the Encryption Plus Non-assertion (EPN). Table 3-12 shows the meaning of EPN. Note that a Licensed Player refers to this field only if CCI is set to 00_2 (Copy Control Not Asserted). Otherwise, a Licensed Player shall ignore this field.

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 0_2, 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	Copy One Generation
11_2	Never Copy

Note that the EPN field and the CCI field are together referred to as the CGMS field in the AACS License Agreement.

Unless otherwise specified in the AACS specifications or in the AACS License Agreement, the CCI field shall be set in accordance with the following rule when the content received from the upstream technology is recorded. Input CGMS value shall be properly updated when the associated stream is recorded. When the content stream with "Copy One Generation" is input, the CCI field shall be updated to "No More Copy".

Any content stream with "No More Copy" shall not be recorded.

The Move_Not_Allowed field indicates if the Move is allowed. The Table 3-14 shows the meaning of Move_Not_Allowed field. Note that a Licensed Copier refers to this field only if CCI is set to either 01_2 (No More Copy) or 11_2 (Never Copy). Otherwise, the Move is not allowed.

Unless otherwise specified in the AACS License Agreement or by the upstream technology, the Move_Not_Allowed field shall be set to 0_2 (Move is allowed) when the content received from the upstream technology is recorded.

Table 3-14 Move_Not_Allowed

Move_Not_Allowed	Meaning
0_2	Move is allowed
1_2	Move is not allowed

The Trusted_Source_Mark_Screening_Required field indicates if Trusted Source Mark Screening is required. Table 3-15 shows the meaning of Trusted_Source_Mark_Screening_Required field. Details of the use of this field are defined in the AACS Compliance Rules.

Table 3-15 Trusted_Source_Mark_Screening_Required

Trusted_Source_Mark_Screening_Required	Meaning
0_2	Trusted Source Mark Screening is required.
1_2	Trusted Source Mark Screening is not required.

The Image_Constraint_Token field indicates the value of Image Constraint Token. Table 3-16 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 0_2, and this field shall be ignored.

Table 3-16 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 3-17 shows the meaning of the Digital_Only_Token.

Table 3-17 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 APSTB field indicates the value of analog copy protection information. Table 3-18 shows the meaning of APS.

Table 3-18 APS

APSTB	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 3-19 shows the data structure of CCI_and_other_info( ) for CCI Sequence Information.

Table 3-19 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)	1	bslbf
Move_Not_Allowed	1	bslbf
Trusted_Source_Mark_Screening_Required	1	bslbf
Image_Constraint_Token	1	bslbf
Digital_Only_Token	1	bslbf
APSTB	3	bslbf
(reserved)	80	bslbf
}		bslbf
}		

CCI_and_other_info_type shall be 0102_{16} for CCI Sequence Information.

CCI_and_other_info_version shall be 0100_{16} for this version.

CCI_and_other_info_data_length shall be the value of 1 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 2.0,* and it is 32bits. Start SPN 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, Move_Not_Allowed, Trusted_Source_Mark_Screening_Required, Image_Constraint_Token, and APSTB is the same as Basic CCI for AACS described in 3.2.4.2.

A Licensed Player may ignore the Move_Not_Allowed field and the Trusted_Source_Mark_Screening_Required field in CCI Sequence Information.

3.3 Encrypted Packs

3.3.1 Encryption Scheme for Clip AV stream

When AACS 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.

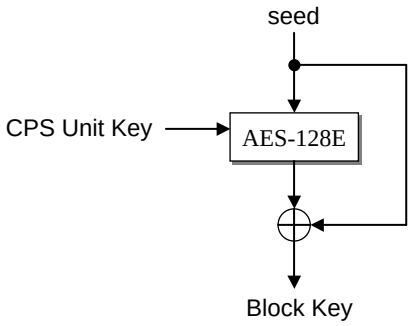

Figure 3-7 Calculation method for the Block Key

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 3-20 shows the data structure for the TP_extra_header.

Table 3-20 TP_extra_header

Syntax	No. of bits	Mnemonic
TP_extra_header {		
Copy_permission_indicator	2	uimsbf
Arrival_time_stamp	30	uimsbf
}		

For the encrypted Aligned Unit of Clip AV stream file, 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.

There may be both encrypted Aligned Unit and unencrypted Aligned Unit recorded in one Clip AV stream file. For example, in the case CCI information changed during the recording of one Clip AV stream file, the Licensed Recorder applies the encryption to the Aligned Units that need to be encrypted.

The change of CCI information may be recorded in CPS Unit Usage File as CCI Sequence Information.

3.3.2 Encrypted Scheme for Thumbnail data

The thumbnail file under "\BDAV" 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.

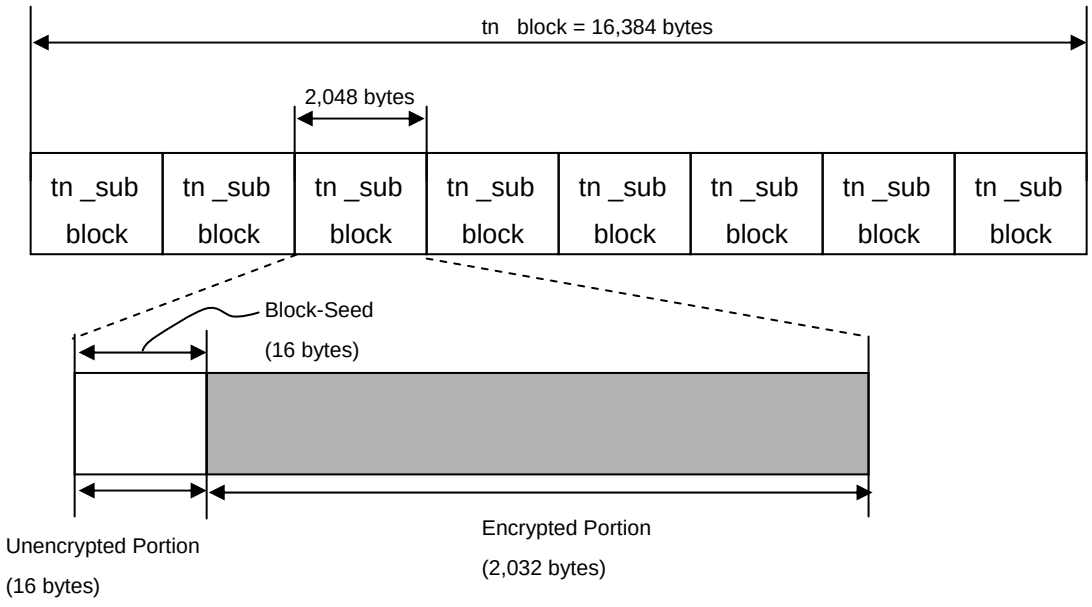

Figure 3-8 Data Format for tn_block

When AACS protection is applied to thumbnail files under the "\BDAV" 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 2.0.*

Data Structure of SESF_copy_control_descriptor is same as copy_status_descriptor which is described in Table 3-21.

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 3-21.

3.4.3 Embedded CCI for BDMV Application

As specified in *Blu-ray Disc Association, System Description Blu-ray Disc Rewritable Format, part 3: Audio Visual Basic Format Specification, version 3.0*, 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 3-21. 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 3-21 presents the syntax. For Licensed Player and Licensed 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 3-21 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 3-22 shows the data format for private_data_byte.

Table 3-22 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 3-23.

Table 3-23 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 3-24.

Table 3-24 CCI

CCI	**Meaning**
00_2	Copy Control Not Asserted
01_2	No More Copy
10_2	Copy One Generation
11_2	Never Copy

Image_Constraint_Token field indicates the value of the Image_Constraint_Token as shown in Table 3-25.

Table 3-25 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 3-26

Table 3-26 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.

This page is intentionally left blank.

Annex A. Treatment of each CCI

A Licensed Recorder and a Licensed Player may not recognize CCI setting embedded on an input stream. In this case, CCI setting in CPS Unit Usage File and CCI setting embedded on a stream may be inconsistent. This annex describes a relation between CCI setting in CPS Unit Usage File and CCI setting embedded on a stream. Note that this rule is applied for broadcast recording and DTCP. For recording from other upstream technologies, refer to the relevant documents, e.g. compliance rules, of the technologies.

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 Licensed Recorder 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 AACS Recordable Media. Note that Image_Constraint_Token and APSTB of CCI Sequence Information in the CPS Unit Usage File shall indicate the most restrictive value in the associated CCI Sequence.

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]
	EPN asserted 0_2	Allowed	Allowed	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 AACS 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 AACS.

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.