

Advanced Access Content System (AACCS)

HD DVD and DVD Prepared Video Book

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

*Revision 0.95
Final
February 19, 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. Intel Corporation, International Business Machines Corporation, 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.

Copyright © 2006-2009 by Intel Corporation, International Business Machines Corporation, Microsoft Corporation, Panasonic 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

PREFACE	III
Notice	iii
Intellectual Property.....	iii
Contact Information.....	iii
1 INTRODUCTION.....	1
1.1 Purpose and Scope.....	1
1.2 Overview.....	1
1.3 Organization of this Document.....	1
1.4 References	1
1.5 Notation	3
1.6 Terminology	3
1.7 Abbreviations and Acronyms	3
2 AACCS COMPONENTS IN LEAD-IN AREA AND BURST CUTTING AREA ..5	
2.1 Introduction	5
2.2 AACCS Components on HD DVD-R/RW/RAM	7
2.2.1 Control Data.....	7
2.2.2 Media Key Block.....	9
2.2.3 Media Identifier	9
2.2.4 Prepared Video Volume Identifier	9
2.2.5 Prepared Video Serial Number	9
2.3 AACCS Components on DVD-R/RW/RAM	9
2.3.1 Control Data.....	9
2.3.2 Media Key Block.....	9
2.3.3 Media Identifier	10

2.3.4	Prepared Video Volume Identifier	10
2.3.5	Prepared Video Serial Number	10
2.3.6	Partial Media Key Block for Host Revocation List	10
3	AACS COMPONENTS IN DATA AREA.....	13
3.1	Introduction	13
3.2	Information in CPR_MAI.....	13
3.2.1	CPR_MAI for HD DVD-R/RW/RAM	13
3.2.2	CPR_MAI for DVD-R/RW/RAM	14
3.3	Media Key Block (MKB)	15
3.4	Sequence Key Block and Segment Key File	15
3.5	Title Key File.....	16
3.6	Title Usage File	16
3.7	Prepared Video Content Certificate	16
3.8	Content Hash	18
3.9	Content Revocation List.....	18
3.10	Prepared Video Token	18
3.11	Subsidiary Token File	20
3.12	Boot Sequence for Disc Application	22
3.13	Backup.....	22
4	PROTECTION OF HD DVD-VIDEO CONTENT ON RECORDABLE MEDIA	23
4.1	Introduction	23
4.2	Stored Data Values in CPI field	23
4.3	Protection for EVOB	23
4.3.1	Bus Encryption/Decryption	24
4.4	Protection for Advanced Resources.....	25
4.5	Secure Move	26
5	DOWNLOAD, STREAMING AND ONLINE-ENABLING	27
5.1	Introduction	27

5.2	Managed Copy	27
6	PROTECTION OF HD DVD-VIDEO CONTENT IN PERSISTENT STORAGE	29
7	SEQUENCE KEY	31
A	ADDITIONAL REQUIREMENT FOR CARRIAGE OF SRM	33
A.1	Introduction	33
A.2	SRM (System Renewability Message).....	33
A.2.1	SRM for DTCP	33
A.2.2	SRM for HDCP	33

List of Figures

Figure 2-1 – Physical Layout of AACS Components for storing HD DVD-Video content on HD DVD-R/RW/RAM Media.....	6
Figure 2-2 – Physical Layout of AACS Components for storing HD DVD-Video content on DVD-R/RW/RAM Media.....	6
Figure 2-3 – Structure of BCA and Lead-in Area of HD DVD-R/RW/RAM media.....	7
Figure 2-4 – Structure of a Control Data Zone	8
Figure 2-5 – Structure of a Data Segment in a Control Data Zone.....	8
Figure 2-6 Example of MKB for CPRM showing a Valid Order of Records.....	11
Figure 3-1 – Data frame configuration	14

This page is intentionally left blank.

List of Tables

Table 2-1 – Format of Copyright Protection Information.....	8
Table 3-1 – Protected Area in Data Area of HD DVD-R/RW/RAM	14
Table 3-2 – Protected Area in Data Area of DVD-R/RW	14
Table 3-3 Protected Area in Data Area of DVD-RAM	15
Table 3-4 – Format for Prepared Video Content Certificate on recordable media	16
Table 3-5 – Format for Prepared Video Token on Recordable Media.....	19
Table 3-6 – Format for Prepared Video Volume Identifier on recordable media.....	19
Table 3-7 – Encoding of Move Allowed Flag bit in Prepared Video Token.....	20
Table 3-8 – Format for Subsidiary Token	21
Table 4-1 – Bus Encryption Format	24

Chapter 1

Introduction

1 Introduction

1.1 Purpose and Scope

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

When there is a discrepancy between a format-independent book and this book then this book takes precedence.

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

1.2 Overview

In the *HD DVD and DVD Prepared Video Book*, the following procedures of Content Encryption and Decryption are described that are required to protect Prepared Video Content (PVC).

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

1.3 Organization of this Document

This document is organized as follows:

- Chapter 1 provides an introduction and overview.
- Chapter 2 describes the AACS Components in Lead-in Area and Burst Cutting Area on HD DVD-R/RW/RAM and DVD-R/RW/RAM media.
- Chapter 3 describes the AACS Components in Data Area on HD DVD-R/RW/RAM and DVD-R/RW/RAM media.
- Chapter 4 describes HD DVD-Video specific procedures for encryption and decryption of AACS Content on HD DVD-R/RW/RAM media and DVD-R/RW/RAM media.
- Chapter 5 describes HD DVD-Video specific functions and protocols which are required for online applications such as download, streaming and Online-Enabling.
- Chapter 6 describes HD DVD-Video specific scheme for content in Persistent Storages.
- Chapter 7 describes the implementation and realization of the Sequence Key for HD DVD-Video.

1.4 References

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

AACS LA, *License Agreement*
AACS LA, *AACS Introduction and Common Cryptographic Elements*
AACS LA, *AACS HD DVD and DVD Pre-recorded Book*
AACS LA, *AACS Pre-recorded Video Book*
AACS LA, *AACS Prepared Video Book*
DVD Forum, *DVD Specifications for High Density Rewritable Disc, Part 1: Physical Specifications Version 1.1*
DVD Forum, *DVD Specifications for High Density Rewritable Disc, Part 2: File System Specifications Version 1.0*
DVD Forum, *DVD Specifications for High Density Recordable Disc, Part 1: Physical Specifications Version 1.1*
DVD Forum, *DVD Specifications for High Density Recordable Disc, Part 2: File System Specifications Version 1.1*
DVD Forum, *DVD Specifications for High Density Recordable Disc for Dual Layer, Part 1: Physical Specifications Version 2.1*
DVD Forum, *DVD Specifications for High Density Recordable Disc for Dual Layer, Part 2: File System Specifications Version 2.0*
DVD Forum, *DVD Specifications for High Density Re-recordable Disc, Part 1: Physical Specifications Version 1.1*
DVD Forum, *DVD Specifications for High Density Re-recordable Disc, Part 2: File System Specifications Version 1.0*
DVD Forum, *DVD Specifications for High Density Re-Recordable Disc for Dual Layer, Part 1: Physical Specifications Version 2.1*
DVD Forum, *DVD Specifications for High Density Re-Recordable Disc for Dual Layer, Part 2: File System Specifications Version 2.0*
DVD Forum, *DVD Specifications for High Definition VIDEO, Version 1.1*
DVD Forum, *DVD Specifications for High Definition VIDEO, Optional Specifications, Multiple HD DVD-Video Contents Recording for DVD / HD DVD Writable Discs, Revision 1.0.*
DVD Forum, *DVD Specifications for Rewritable Disc, Part 1: Physical Specifications Version 2.2*
DVD Forum, *DVD Specifications for Rewritable Disc, Part 2: File System Specifications Version 2.0*
DVD Forum, *DVD Specifications for Recordable Disc for General, Part 1: Physical Specifications Version 2.1*
DVD Forum, *DVD Specifications for Recordable Disc for General, Part 2: File System Specifications Version 2.1*
DVD Forum, *DVD Specifications for Recordable Disc for Dual Layer, Part 1: Physical Specifications Version 3.0*
DVD Forum, *DVD Specifications for Recordable Disc for Dual Layer, Part 2: File System Specifications Version 3.0*
DVD Forum, *DVD Specifications for Re-recordable Disc, Part 1: Physical Specifications Version 1.2*
DVD Forum, *DVD Specifications for Re-recordable Disc, Part 2: File System Specifications Version 1.0*
DVD Forum, *DVD Specifications for Re-Recordable Disc for Dual Layer, Part 1: Physical Specifications Version 2.0*
DVD Forum, *DVD Specifications for Re-Recordable Disc for Dual Layer, Part 2: File System Specifications Version 2.0*
4C Entity, LLC, *CPRM Specification: Introduction and Common Cryptographic Elements, Revision 1.0*
4C Entity, LLC, *CPRM Specification: DVD Book, Revision 0.97*
4C Entity, LLC, *CPRM Media Verification Book*

1.5 Notation

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

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

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

Content which would be protected by complying with this document is called HD DVD Portable Video content (HD DVD-PV content) in the DVD Forum specifications.

1.6 Terminology

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

1.7 Abbreviations and Acronyms

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

This page is intentionally left blank.

Chapter 2

AACS Components in Lead-in Area and Burst Cutting Area

2 AACS Components in Lead-in Area and Burst Cutting Area

2.1 Introduction

This chapter specifies the location and format details of the AACS common components to this *AACS HD DVD and DVD Prepared Video Book*. The HD DVD-R/RW/RAM formats and the DVD-R/RW/RAM formats are licensed by the DVD Forum. The DVD Forum publishes the concerned specifications¹:

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

This chapter assumes the reader is familiar with the HD DVD-R/RW/RAM formats and the DVD-R/RW/RAM format. This chapter focuses on those aspects of the format that are relevant to AACS protection. Figure 2-1 and Figure 2-2 give an overview of the locations of AACS related components on HD DVD-R/RW/RAM media and DVD-R/RW/RAM media. The structure of BCA and Lead-in area is the same as HD DVD-R/RW/RAM media and DVD-R/RW/RAM media described in *AACS HD DVD and DVD Recordable Book*.

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

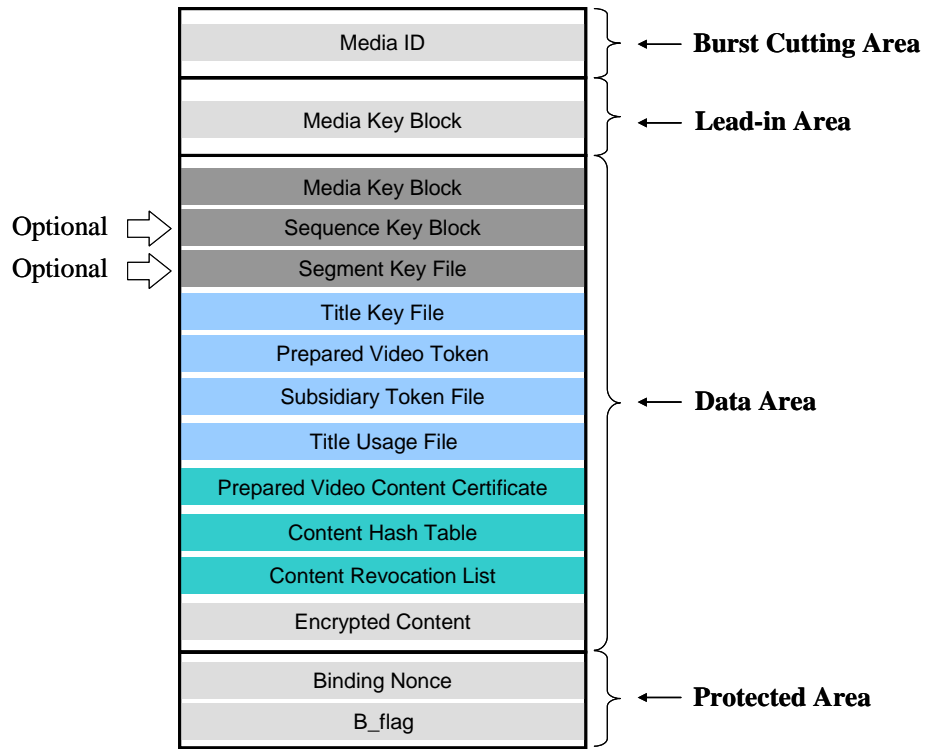


Figure 2-1 – Physical Layout of AACs Components for storing HD DVD-Video content on HD DVD-R/RW/RAM Media

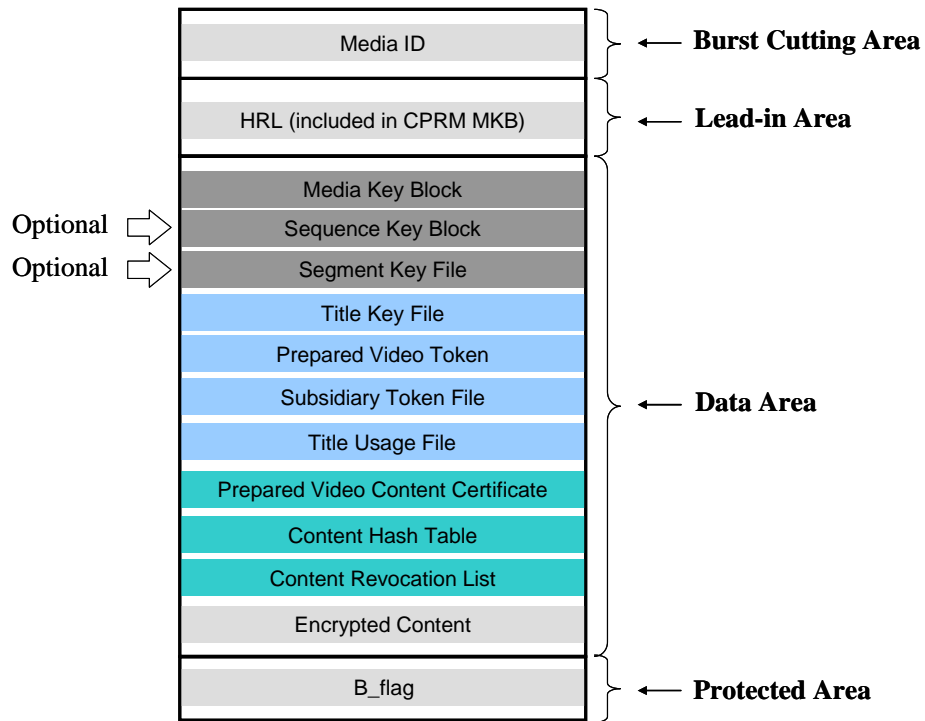


Figure 2-2 – Physical Layout of AACs Components for storing HD DVD-Video content on DVD-R/RW/RAM Media

2.2 AACS Components on HD DVD-R/RW/RAM

Locations and formats of the AACS components stored in the BCA or a System Lead-in Area of the HD DVD-R/RW/RAM media are described in this section. Figure 2-3 depicts the structure of the BCA and the Lead-in Area of the HD DVD-R/RW/RAM media. The details are provided in the following subsections.

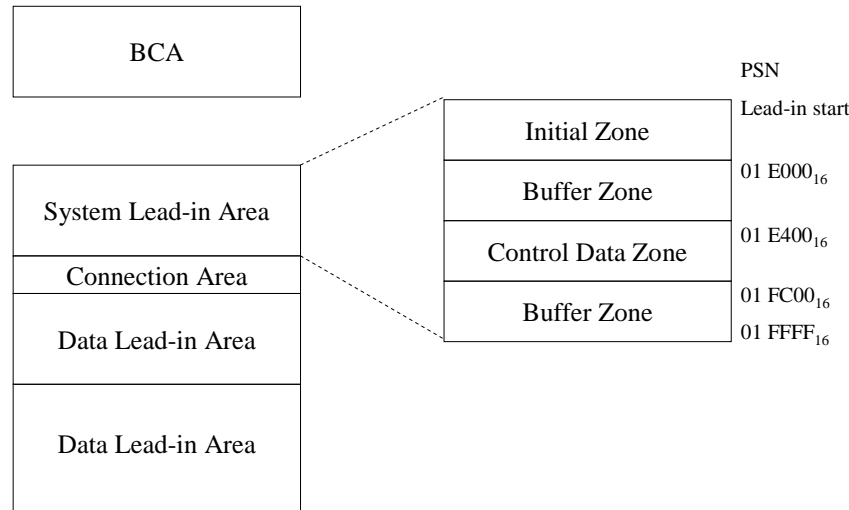


Figure 2-3 – Structure of BCA and Lead-in Area of HD DVD-R/RW/RAM media

2.2.1 Control Data

A Control Data indicating that AACS is applied to the media is stored in a Control Data Zone of the HD DVD-R/RW/RAM media. Figure 2-4 presents the structure of the Control Data Zone. The Control Data Zone has 2 Control Data Sections, 2 Copyright Data Sections, and a Copyright Protection System Use Section. Each Control Data Section is comprised of 16 Data Segments. The content of the first Data Segment in a Control Data Section or a Copyright Data Section are repeated 16 times. Figure 2-5 shows data structure of each Data Segment which is composed of 32 Physical Sectors. The third Physical Sector in each Data Segment of a Control Data Section contains the Copyright Protection Information. Table 2-1 shows the format of the Copyright Protection Information. A 1-byte Copyright Protection System Type value shall be set to 01₁₆ in order to indicate that AACS is applied to the media. The Read-Only MKB Packs field denotes information related with a Read-Only MKB recorded in the Lead-in Area as defined in *AACS HD DVD and DVD Recordable Book*. However, this information is not used for encrypting and decrypting the Prepared Video Content on the media. All bytes reserved for Copyright Protection System Use field shall be set to 00₁₆. The Copyright Data Section can contain copyright data or the data of the Copyright Data Section shall be set to 00₁₆.

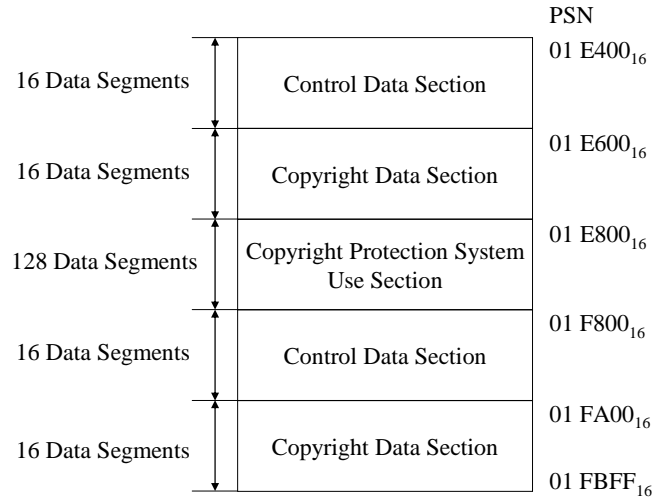


Figure 2-4 – Structure of a Control Data Zone

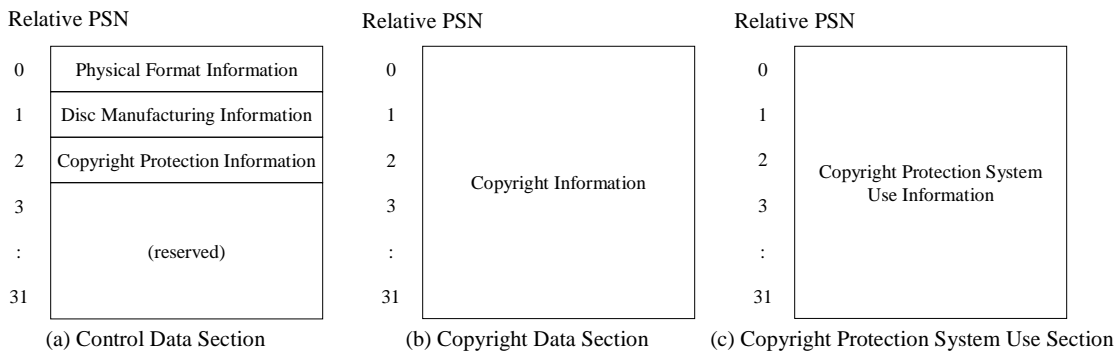


Figure 2-5 – Structure of a Data Segment in a Control Data Zone

Table 2-1 – Format of Copyright Protection Information

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

2.2.2 Media Key Block

A Read-Only MKB is recorded in Lead-in Area as defined in *AACS HD DVD and DVD Recordable Book*. However this adaptation book does not use the Read-Only MKB for encrypting and decrypting the Prepared Video Content on the media.

HD DVD-R/RW/RAM media may have a Read/Write MKB which is to encrypt and decrypt the Prepared Video Content and it shall be stored in the file “MKBPREPARED.AACS” located in the “/AACS” directory of the Data Area under the root directory if no Prepared Video Content (PVC) is recorded, or under the sub-directory specified in the DVD Forum specifications if a PVC is already recorded under the root directory. Licensed Player shall verify the signature of Read-Only MKB before calculating Media Key of Read/Write MKB. Details of the MKB and MKB process are described in the *Introduction and Common Cryptographic Elements* book. For clarification, it is not required to compare of the Version Number field in Read-Only MKB with Read/Write MKB. In other words, Licensed Player may continue to process even if the value of Version Number field in Read-Only MKB is larger than in Read/Write MKB.

For clarification, Media Key Delta defined in Prepared Video Token is used to calculate Media Key for Prepared Video Content. The detailed calculation method is described in Section 3.5 in this specification.

2.2.3 Media Identifier

AACS compliant HD DVD-R/RW/RAM media shall contain a 128-bit Media Identifier which is recorded in the Burst Cutting Area (BCA) by the media manufacturer as defined in *AACS HD DVD and DVD Recordable Book*.

2.2.4 Prepared Video Volume Identifier

Instead of Volume Identifier for HD DVD and DVD Pre-recorded Video, the Prepared Video Volume ID shall be stored in the Prepared Video Token defined in Section 3.10.

2.2.5 Prepared Video Serial Number

Instead of Pre-recorded Media Serial Number (PMSN), the Prepared Video Serial Number shall be stored in the Prepared Video Token defined in Section 3.10.

2.3 AACS Components on DVD-R/RW/RAM

For encryption and decryption of Prepared Video Content and recorded on DVD-R/RW/RAM media, CPRM Compliant DVD-R/RW/RAM media is required. The Media Identifier and some records of the Media Key Block (this MKB is completely different from the MKB for AACS and hereinafter referred to as CPRM MKB in the Lead-in Area) in the CPRM Compliant DVD-R/RW/RAM media are used for AACS protection. AACS Adopters who manufacture devices recording the AACS Content shall refer the CPRM Specifications.

2.3.1 Control Data

A Control Data indicating that AACS is applied to the media is stored in a Control Data Zone of the DVD-R/RW/RAM media. The details of the data stored in the Control Data are described in the *CPRM Media Verification Book* (name subject to change).

2.3.2 Media Key Block

DVD-R/RW/RAM media may have a Read/Write MKB which is to encrypt and decrypt the Prepared Video Content and it shall be stored in the file “MKBPREPARED.AACS” located in the “/AACSHD” directory of Data Area under the root directory if no Prepared Video Content (PVC) is recorded, or under the sub-directory

specified in the DVD Forum specifications if a PVC is already recorded under the root directory. Details of the MKB and MKB process are described in the *Introduction and Common Cryptographic Elements* book.

For clarification, Media Key Delta defined in Prepared Video Token is used to calculate Media Key for Prepared Video Content. The detailed calculation method is described in Section 3.5 in this specification.

The recording device shall have non-volatile storage for storing the AACS Read/Write MKB, and shall update that MKB in its storage if it receives one from any source listed in the Section 2.3 of the *AACS Recordable Video Book* or the MKB is stored in the file named “MKB.inf” located in the “/AACS” directory of the Data Area on DVD-Video disc if playing the AACS Content on the disc, where the received MKB is more recent than the MKB currently stored, and is small enough to fit in the device’s non-volatile storage.

2.3.3 Media Identifier

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 128 bits as follows:

$$\text{AACS Media ID} = 25\text{B946EBC0B36173}_{16} \parallel \text{64-bit CPRM Media Identifier}$$

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.

AACS Compliant recorders which support CPRM compliant recordable media shall also have a “CPRM Device Key Set”, shall process the CPRM MKB and shall verify the correctness of the Media Key derived from the 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 media as AACS compliant media if the 64-bit Media Identifier is recorded on the media.

(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 02₁₆, shall not be used to calculate Media ID.

2.3.4 Prepared Video Volume Identifier

Instead of Volume Identifier for HD DVD and DVD Pre-recorded Video, the Prepared Video Volume ID shall be stored in the Prepared Video Token defined in Section 3.10.

2.3.5 Prepared Video Serial Number

Instead of Pre-recorded Media Serial Number (PMSN), the Prepared Video Serial Number shall be stored in the Prepared Video Token defined in Section 3.10.

2.3.6 Partial Media Key Block for Host Revocation List

The 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 all Conditionally Calculate Media Key Record. If the Conditionally Calculate Media Key Record is not 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.

Figure 2-6 shows an example CPRM MKB stored in the Lead-in Area on DVD-R/RW/RAM.

Record Type: 81 ₁₆
Verify Media Key Record
Record Type: 01 ₁₆
Calculate Media Key Record
Record Type: 82 ₁₆
Conditionally Calculate Media Key Record
Record Type: 10₁₆
Type and Version Record
Record Type: 21₁₆
Host Revocation List Record
Record Type: 02 ₁₆
End of Media Key Block Record

Figure 2-6 Example of MKB for CPRM showing a Valid Order of Records

This page is intentionally left blank.

Chapter 3

AACS Components in Data Area

3 AACS Components in Data Area

3.1 Introduction

This chapter describes details of locations and/or formats of the AACS components defined in the *AACS Pre-recorded Video Book* and *AACS Prepared Video Book* which are stored in the Data Area of an HD DVD-R/RW/RAM formatted media and DVD-R/RW/RAM formatted media. The data format on the HD DVD-R/RW/RAM media and DVD-R/RW/RAM media is subject of a license from the DVD Forum, which also publishes a specification describing the format in detail (see the corresponding reference in Section 1.4). An overview of locations for storing the AACS components on a recordable media is shown in Figure 2-1 and Figure 2-2. The following data will be stored in the Data Area: a Media Key Block (MKB), a Sequence Key Block File (SKBF), Segment Key Files (SKFs), Title Key Files (TKFs), Prepared Video Token, Title Usage Files (TUFs), a Prepared Video Content Certificate, Content Hash Tables (CHTs), a Content Revocation List (CRL), AACS Content and content with MAC/hash. All data listed above except AACS Content and content with MAC/hash are stored in the “/AACS” directory on the HD DVD-R/RW/RAM media or “/AACSHD” directory on the DVD-R/RW/RAM media under the root directory if no Prepared Video Content (PVC) is recorded, or under the sub-directory specified in the DVD Forum specifications if a PVC is already recorded under the root directory. This means that each “/AACS” or “/AACSHD” directory explained in the following sections and chapters is made in either the root directory or the specific sub-directory when the Prepared Video Content is recorded according to the rules specified in the DVD Forum specifications. The encapsulation formats for Content and other HD DVD-Video specific data for copyright protection are mentioned in the following chapters. There are some reserved fields in data formats defined hereafter. Note that a reserved field shall be filled with 0₂ unless otherwise stated.

3.2 Information in CPR_MAI

3.2.1 CPR_MAI for HD DVD-R/RW/RAM

A Binding Nonce and a B_flag are stored in CPR_MAI field of a Data Area in HD DVD-R/RW/RAM media. The CPR_MAI field in HD DVD-R/RW/RAM media is denoted as Protected Area in the following sections of this book. Figure 3-1 depicts the configuration of Data Frame, which is the logical structure of one physical sector. Table 3-1 shows the Protected Area of a Data Frame in the Data Area. A Protected Area in the Data Area shall consist of the following fields:

- 4 bytes of a 16-byte Binding Nonce are defined in *AACS HD DVD and DVD Recordable Book*.
- A B_flag of 1 bit. This value indicates a sector to be Bus Encrypted or not:
 - 0₂: A sector not to be Bus Encrypted.
 - 1₂: A sector to be Bus Encrypted.
- A reserved field of 15 bits which shall be filled with 0₂.

Note that B_flag shall be 1₂ if and only if the Data Frame stores part of an EVOB file, provided that the Service Provider chooses to use Bus Encryption for the disc.

Details of format and location of Protected Area to store Binding Nonce are defined in *AACS HD DVD and DVD Recordable Book*. The location of Logical Sectors for storing a piece of a Binding Nonce is described in Section 3.11. For clarification, the first 4 bytes of Protected Area which does not contain a portion of Binding Nonce shall be set to 00₁₆.

Some clarifications and notes on Bus Encryption (BE) are provided here. BE is never applied to an S-EVOB in a Persistent Storage. An S-EVOB in a Persistent Storage may come from a Disc, where B_flags may be associated with the S-EVOB. If B_flags are set at 1₂ in the sector headers of the sectors which carry the S-EVOB, on a PC platform, the AACCS module in a Player shall intervene and perform Bus Decryption when the Player copies the S-EVOB into a Persistent Storage. An S-EVOB may be stored in an ACA file (an archive). No BE is required for such an S-EVOB.

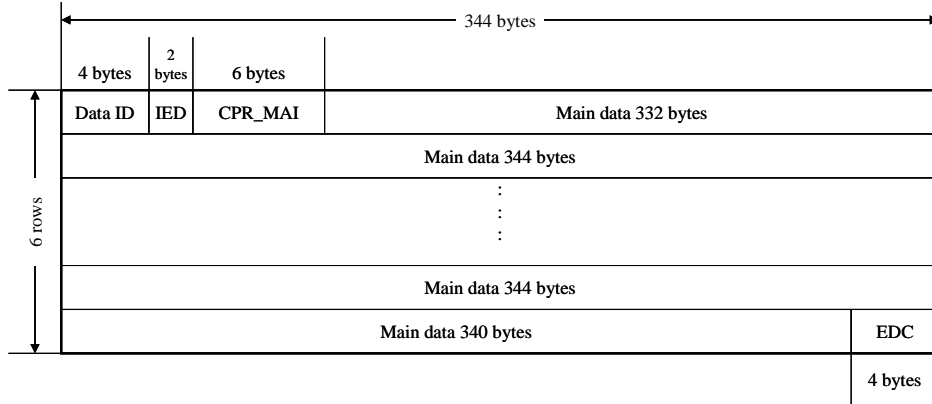


Figure 3-1 – Data frame configuration

Table 3-1 – Protected Area in Data Area of HD DVD-R/RW/RAM

Byte	Bit	7	6	5	4	3	2	1	0
0		4 bytes of a 16-byte Binding Nonce							
1									
2									
3									
4	B_flag	Reserved							
5		Reserved							

3.2.2 CPR_MAI for DVD-R/RW/RAM

The configuration of a Data Frame for the DVD-R/RW/RAM media is the same as for the HD DVD-R/RW/RAM media as shown in Figure 3-1. Table 3-2 and Table 3-3 show the CPR_MAI of a Data Frame in the Data Area of the DVD-R/RW and DVD-RAM media, respectively.

A CPR_MAI in Data Area on DVD-R/RW shall consist of the following fields:

- ADP_TY of 2 bits which shall be equal to 00₂
- A B_flag of 1 bit. This value indicates a sector to be Bus Encrypted or not:
 0₂: A sector not to be Bus Encrypted.
 1₂: A sector to be Bus Encrypted.
- Other fields denoted as “Reserved” shall be filled with 0₂.

Table 3-2 – Protected Area in Data Area of DVD-R/RW

Byte	Bit	7	6	5	4	3	2	1	0
0		Reserved				ADP_TY: 00 ₂		Reserved	

1	Reserved	
2		
3		
4	B_flag	Reserved
5	Reserved	

A CPR_MAI in Data Area on DVD-RAM shall consist of the following fields:

- A B_flag of 1 bit. This value indicates a sector to be Bus Encrypted or not:
 - 0₂: A sector not to be Bus Encrypted.
 - 1₂: A sector to be Bus Encrypted.
- Other fields denoted as “Reserved” shall be filled with 0₂.

Note that B_flag shall be 1₂ if and only if the Data Frame stores part of an EVOB file, provided that the Service Provider chooses to use Bus Encryption for the disc.

Some clarifications and notes on Bus Encryption (BE) are provided here. BE is never applied to an S-EVOB in a Persistent Storage. An S-EVOB in a Persistent Storage may come from a Disc, where B_flags may be associated with the S-EVOB. If B_flags are set at 1₂ in the sector headers of the sectors which carry the S-EVOB, on a PC platform, the AACS module in a Player shall intervene and perform Bus Decryption when the Player copies the S-EVOB into a Persistent Storage. An S-EVOB may be stored in an ACA file (an archive). No BE is required for such an S-EVOB.

Table 3-3 Protected Area in Data Area of DVD-RAM

Byte	Bit	7	6	5	4	3	2	1	0
0	Reserved								
1									
2									
3									
4	B_flag	Reserved							
5	Reserved								

3.3 Media Key Block (MKB)

A recordable media storing Prepared Video Content shall have Media Key Block (MKB) in the “/AACS” directory on HD DVD-R/RW/RAM media or the “/AACSHD” directory on DVD-R/RW/RAM media for decryption of AACS Content on the media. The MKB is stored as a file in the Data Area of the media, and the MKB file has the name “MKBPREPARED.AACS”.

3.4 Sequence Key Block and Segment Key File

A recordable media storing the AACS Prepared Video Content shall have at most one Sequence Key Block File (SKBF). SKBF shall be stored in the file “SKB.AACS” located in the “/AACS” directory on HD DVD-R/RW/RAM media or the “/AACSHD” directory on DVD-R/RW/RAM media. The format of SKBF on the recordable media is the same as the one defined in *AACS HD DVD and DVD Pre-recorded Book*. The SKBF contains six SKBs in it. Details of the SKB format and the SKB process are described in the *AACS Pre-recorded Video Book*.

The SKBF accompanies a Segment Key File (SKF). SKF shall be stored in the file “SKF.AACS” located in the “/AACS” directory on HD DVD-R/RW/RAM media or the “/AACSHD” directory on DVD-R/RW/RAM media.

The format of SKF on the recordable media is the same as the one defined in *AACS HD DVD and DVD Pre-recorded Book*.

A recordable media storing the AACS Prepared Video Content shall have an SKBF and an SKF if it contains a P-EVOB which has Sequence Key Sections.

3.5 Title Key File

A recordable media storing the AACS Prepared Video Content shall have at least one Title Key File (TKF) to store encrypted Title Key(s). Title Key File for Category 1 Disc which is defined in the *HD DVD-Video Specifications* shall be stored in the file “VTKF.AACS” located in the “/AACS” directory on HD DVD-R/RW/RAM media or the “/AACSHD” directory on DVD-R/RW/RAM media. Title Key File for a Category 2 Disc shall be stored in the file “VTKF%%.AACS” and “ATKF%%.AACS” located in the “/AACS” directory on HD DVD-R/RW/RAM media or the “/AACSHD” directory on DVD-R/RW/RAM media, where %% runs from 000 to 999. For a Category 2 Disc, a TKF is associated with a Playlist. Two or more Playlists are not allowed to share the same TKF. There is a name convention: “VPLST%%.XPL” shall be accompanied by “VTKF%%.AACS”. The format of Title Key File is the same as the one defined in *AACS HD DVD and DVD Pre-recorded Book*.

For clarification, because Binding Nonce is not stored in the Protected Area associated with Title Key File in case of AACS Prepared Video Content, it is also not necessary to mark with Non-relocatable attribute to the Logical Sectors even if Title Key File is written in HD DVD-R/RW/RAM media.

3.6 Title Usage File

Usage Rules are stored in a Title Usage File. Title Usage File for Category 1 Disc which is defined in the *HD DVD-Video Specifications* shall be stored in the file “VTUF.AACS” located in the “/AACS” directory on HD DVD-R/RW/RAM media or the “/AACSHD” directory on DVD-R/RW/RAM media. Title Usage File for a Category 2 Disc shall be stored in the file “VTUF%%.AACS” and “ATUF%%.AACS” located in the “/AACS” directory on HD DVD-R/RW/RAM media or the “/AACSHD” directory on DVD-R/RW/RAM media, where %% runs from 000 to 999. For a Category 2 Disc, a TUF accompanies a Playlist. Two or more Playlists are not allowed to share the same TUF. There is a name convention: “VPLST%%.XPL” shall be accompanied by “VTUF%%.AACS”. “APLST%%.XPL” shall be accompanied by “ATUF%%.AACS”. The format of Title Usage File is the same as the one defined in *AACS HD DVD and DVD Pre-recorded Book*.

3.7 Prepared Video Content Certificate

A recordable media storing the AACS protected Prepared Video Content shall have one Prepared Video Content Certificate file. The Prepared Video Content Certificate shall be stored in the file “PV_CONTENT_CERT.AACS” located in the “/AACS” directory on HD DVD-R/RW/RAM media or the “/AACSHD” directory on DVD-R/RW/RAM media. Table 3-4 shows the structure of Prepared Video Content Certificate.

The maximum size of the Prepared Video Content Certificate is 8Kbytes (8192 bytes).

Table 3-4 – Format for Prepared Video Content Certificate on recordable media

Byte	Bit	7	6	5	4	3	2	1	0
0	Certificate Type: 07 ₁₆								
1	Reserved								
2	Total_Number_of_HashUnits								
:									
5									

6	Total_Number_of_Layers
7	Layer_Number
8 : 11	Reserved
12 13	Number_of_Digests
14 15	Applicant ID
16 ... 19	Content Sequence Number
20 21	Minimum CRL Version
22 23	Number of Prepared Video Authorizing Servers Entries (M)
24 25	Length_Format_Specific_Section
26 : 39	Reserved
40 : 59	Content Hash Table Digest #1
60 : 79	Content Hash Table Digest #2
80-119	Public Key of Authorizing Server #1
...	...
79+40*M	Public Key of Authorizing Server #M
80+40*M : 119+40*M	Signature Data

- Content Certificate ID is a combination of the 2-byte Applicant ID and the 4-byte Content Sequence Number. Refer the *AACS Pre-recorded Video Book* for Content Certificate ID and CRL. The meaning of the fields in the Prepared Video Content Certificate is described in the *AACS Prepared Video Book* except following fields.
- Total_Number_of_HashUnits field indicates the total number of hashes in CHT #1 and CHT #2 on the recordable media.

- Total_Number_of_Layers field indicates the total number of layers on the optical media. For an HD DVD-R/RW/RAM and DVD-R/RW/RAM media, this field shall be set to 01₁₆.
- Layer_Number field shall be set to 0000₁₆ for an HD DVD-R/RW/RAM and DVD-R/RW/RAM media.
- Number_of_Digests field shall be set to 0002₁₆.
- Length_Format_Specific_Section field shall be set to 000E₁₆.
- Content Hash Table Digest #1 contains the SHA-1 hash value of the Content Hash Table #1 (CHT #1). CHT #1 contains all the hash values of the Hash Units in the P/S-EVOBs for the corresponding protected Prepared Video Content on the recordable media. The details of CHT #1 are described in *AACS HD DVD and DVD Pre-recorded Book*.
- Content Hash Table Digest #2 contains the SHA-1 hash value of the Content Hash Table #2 (CHT #2). CHT #2 contains hash values of the navigation data, i.e. all the XML document files and all the ECMAScript files for the corresponding protected Prepared Video Content on the recordable media. In addition, CHT #2 contains the hash values of TKFs and TUFs. The details of CHT #2 are described in *AACS HD DVD and DVD Pre-recorded Book*.

Other fields in the Prepared Video Content Certificate are described in the *AACS Prepared Video Book*. All the reserved fields shall be filled with 00₁₆.

3.8 Content Hash

A recordable media storing the Prepared Video Content shall have two Content Hash Tables (CHTs): Content Hash Table #1 (CHT #1) and Content Hash Table #2 (CHT #2). Content Hash Table #1 shall be stored in the file “CONTENT_HASH_TABLE1.AACS” located in the “/AACS” directory on HD DVD-R/RW/RAM media or the “/AACSHD” directory on DVD-R/RW/RAM media. The format of Content Hash Table #1 is the same as the one defined in *AACS HD DVD and DVD Pre-recorded Book*. Content Hash Table #2 shall be stored in the file “CONTENT_HASH_TABLE2.AACS” located in the “/AACS” directory on HD DVD-R/RW/RAM media or the “/AACSHD” directory on DVD-R/RW/RAM media. The format of Content Hash Table #2 is the same as the one defined in *AACS HD DVD and DVD Pre-recorded Book*.

3.9 Content Revocation List

Recordable media storing AACS Prepared Video Content shall include a Content Revocation List (CRL). Content Revocation List shall be stored in the file “CONTENT_REVOCATION_LIST.AACS” located in the “/AACS” directory on HD DVD-R/RW/RAM media or the “/AACSHD” directory on DVD-R/RW/RAM media. The format of a CRL file is defined in the *AACS Pre-recorded Video Book*.

3.10 Prepared Video Token

A recordable media storing the Prepared Video Content shall have one and only one Prepared Video Token (PVT). PVT shall be stored in the file “PVT.AACS” located in the “/AACS” directory on HD DVD-R/RW/RAM media or the “/AACSHD” directory on DVD-R/RW/RAM media. The format of the PVT is defined as shown in Table 3-5.

Table 3-5 – Format for Prepared Video Token on Recordable Media

Byte	Bit	7	6	5	4	3	2	1	0
0 : 39		PVAS Public Key							
40 : 55		Prepared Video Volume ID							
56		PVSN Status	Move Allowed	BEE	Reserved				
57 : 59		Reserved							
60 : 75		Media Key Delta							
76 : 91		Prepared Video Serial Number (PVSN)							
92 : 131		Prepared Video Token Signature Data							

Each Prepared Video Content shall have one and only one Prepared Video Volume Identifier ($ID_{pvolume}$) of 128 bits. The format of the Prepared Video Volume ID is shown in Table 3-6.

Table 3-6 – Format for Prepared Video Volume Identifier on recordable media

Byte	Bit	7	6	5	4	3	2	1	0
0		Media Type: 80_{16}							
1		Reserved							
2 : 13		Unique Number							
14 : 15		Reserved							

When Prepared Video Content is for Electronic Sell Through or Manufacturing on Demand:

- Media Type shall be set to 80₁₆.
- Unique Number field shall be assigned by a Content Participant in order to identify a volume of HD DVD-Video content.

When Prepared Video Content is for Managed Copy, the value of the Unique Number field of Prepared Video Volume ID may be the same as Volume ID or Prepared Video Volume Identifier stored in source media of the Managed Copy.

Prepared Video Serial Number Status Flag indicates the status of Prepared Video Serial Number field. This flag shall be set to '1₂' if Prepared Video Serial Number has been defined, otherwise the flag shall be set to '0₂'. When this flag is set to '0₂', Prepared Video Serial Number field shall be filled with the '0₂'.

Move Allowed Flag indicates the status of whether the Prepared Video Content is allowed to be Moved, as shown in Table 3-7. When the Prepared Video Content is allowed to be Moved, this bit shall be set to '1₂.' Otherwise this bit shall be set to '0₂'. When the Prepared Video Content is a result of a Managed Copy and recorded on the HD DVD-RW/RAM media, the Move Allowed Flag shall be set to '1₂'. When the Prepared Video Content is a result of a Managed Copy and recorded on the HD DVD-R and DVD-R/RW/RAM media, the Move Allowed Flag shall be set to '0₂'

Table 3-7 – Encoding of Move Allowed Flag bit in Prepared Video Token

Move Allowed Flag	Status
0 ₂	Prepared Video Content is not allowed to be Moved
1 ₂	Prepared Video Content is allowed to be Moved

Bus Encryption Enabled (BEE) Flag indicates the status of whether Bus Encryption is enabled for the content in the P/S-EVOBs covered by this PV Token. When the AACS Content would be recorded by a Licensed Drive or an optical recorder which has the capability of setting the Bus Encryption Flag in the sector header and the Prepared Video Authorization Server (PVAS) requires using Bus Encryption between the Drive-Host Interface, the BEE Flag shall be set to '1₂'.

As clarification, Bus Encryption is never applied to an S-EVOB in a Persistent Storage.

Media Key Delta is used to calculate Media Key for Prepared Video Content. A Licensed Player shall XOR Media Key derived from Read/Write MKB with the value in this field and shall use the resulting value as Media Key for Prepared Video Content for processing the Sequence Key Block or decrypting Title Keys as defined in *AACS Prepared Video Book*.

Prepared Video Serial Number is defined instead of Pre-recorded Media Serial Number (PMSN) if it is defined.

Prepared Video Token Signature Data is calculated using the PVAS Private Key. The detailed calculation method of the PVT Signature Data is described in Chapter 2 of the *AACS Prepared Video Book*.

3.11 Subsidiary Token File

When a Licensed Recorder first records the Prepared Video Token on to HD DVD-R/RW/RAM media, a Subsidiary Token File is also recorded, and all Logical Sectors for the Subsidiary Token File shall be marked with Non-relocatable attribute. Because available size of each Protected Area where the Binding Nonce is stored is 4 bytes, 4 Physical Sectors (8Kbytes) are necessary to store the Binding Nonce. The Binding Nonce

shall be sequentially stored in the Protected Area of the four continuous Logical Sectors where the Subsidiary Token File is written as described in Section 3.2.1.

When a Licensed Recorder first records the Prepared Video Token on to DVD-R/RW/RAM media, a Subsidiary Token File is also recorded, however all Logical Sectors for the Subsidiary Token File on DVD-R/RW/RAM media need not be marked with Non-relocatable attribute because the Binding Nonce is not stored in Sector Headers. The head of the Subsidiary Token File shall be arranged at the head of a Data Segment when the Subsidiary Token File is stored on HD DVD-RW/RAM and the Data Segment shall not contain any data other than data of the Subsidiary Token File.

The Subsidiary Token File shall be stored in the file “SUBTKN.AACS” located in the “/AACS” directory on HD DVD-R/RW/RAM media or the “/AACSHD” directory on DVD-R/RW/RAM media. The format of the Subsidiary Token is shown in Table 3-8.

The Binding Nonce that is used when signing the PVT is stored onto the media by associating it with one of two files, hereafter referred to as the “Subsidiary Token File” and the actual PVT is stored in a second file, hereafter referred to as the “PVT File”. The Download Client creates the Binding Nonce and ensures that it is successfully committed to the Subsidiary Token File before sending the Binding Nonce to the PVAS. The Download Client stores the PVT data in the PVT File when it is received from the PVAS.

During playback, the Licensed Player retrieves the PVT data from the PVT File and uses the Binding Nonce value from the Subsidiary Token File during the signature verification process of that PVT.

Table 3-8 – Format for Subsidiary Token

Bit Byte	7	6	5	4	3	2	1	0
0 : 11	(msb) TKN_ID (lsb)							
12 : 15	(msb) DVD_HD_PV_BN_EA (lsb)							
16 : 31	Reserved							
32 : 33	(msb) VERN (lsb)							
34 : 8191	Reserved							

TKN_ID field indicates the 12-byte value to identify this file. The value is set to “DVD_HD_PV_BN” with character set code of ISO/IEC 646:1983 (a-characters).

HD_DVD_PV_BN_EA field indicates the end address of the Binding Nonce File. Because the size of the Binding Nonce File is fixed to 8Kbytes, this field is filled with the value of ‘8191’.

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

3.12 Boot Sequence for Disc Application

In the Startup Sequence of Advanced Content, a Playlist shall have the name, “VPLST%%.XPL” or “APLST%%.XPL”, where %%% runs from 000 to 999. On the other hand, the *HD DVD-Video Specifications* do not specify a filename which may be used as a Playlist in a Soft Reset. However the same restriction on a Playlist filename for a Soft Reset defined in *AACS HD DVD and DVD Pre-recorded Book* shall be applied to this specification.

3.13 Backup

All the following AACS components shall have their backup image in the “/AACS_BAK” directory of the Data Area on HD DVD-R/RW/RAM and DVD-R/RW/RAM media which are provided by the PVAS. A Licensed Player uses any of the backup files if it cannot correctly read the original files. If the original file is updated, the corresponding backup file shall be updated. The following is a list of the backup components:

- /AACS_BAK/MKBPREPARED.AACS
- /AACS_BAK/SKB.AACS and /AACS_BAK/SKF.AACS (if original files exist)
- /AACS_BAK/PVT.AACS
- /AACS_BAK/VTKF.AACS (for the Standard Contents),
/AACS_BAK/VTKF%%.AACS, /AACS_BAK/ATKF%%.AACS (if the corresponding Playlist exists)
- /AACS_BAK/DKF.AACS
- /AACS_BAK/VTUF.AACS (for the Standard Contents),
/AACS_BAK/VTUF%%.AACS, /AACS_BAK/ATUF%%.AACS (if the corresponding Playlist exists)
- /AACS_BAK/PV_CONTENT_CERT.AACS
- /AACS_BAK/CONTENT_HASH_TABLE1.AACS
- /AACS_BAK/CONTENT_HASH_TABLE2.AACS
- /AACS_BAK/CONTENT_REVOCATION_LIST.AACS
- /AACS_BAK/MNGCPY_MANIFEST.XML

It is recommended that each original component and corresponding backup component is allocated in a different ECC block.

Chapter 4

Protection of HD DVD-Video Content on Recordable Media

4 Protection of HD DVD-Video Content on Recordable Media

4.1 Introduction

This chapter describes the details of encryption and decryption of HD DVD-Video content on a recordable media. In this chapter, recordable media indicates HD DVD-R/RW/RAM and DVD-R/RW/RAM media². The HD DVD-R/RW/RAM and DVD-R/RW/RAM format is subject of a license from the DVD Forum, which also publishes a specification describing the format in detail (see the corresponding reference in Section 1.4). The HD DVD-Video format is defined by the DVD Forum for storing Audiovisual Content not only on pre-recorded media but also on recordable media. The HD DVD-Video format is the subject of a license from the DVD Forum, which also publishes a specification describing the format in detail (see the corresponding reference in Section 1.4).

- DVD Specifications for High Definition VIDEO

The general approach for encryption and decryption of Prepared Video Content is specified in Chapter 3 of the *AACS Prepared Video Book*. This chapter describes the additional details of that approach that are specific to the use of AACS encryption and decryption with the HD DVD-Video Format on recordable media.

The elements of HD DVD-Video content which are targets of the Prepared Video Content are the same as the ones defined in the *AACS HD DVD and DVD Pre-recorded Book*. A Content Name file, a Thumbnail Picture file, a Content Metadata file and a Content Identifier file specified in the DVD Forum specifications are not targets of protection by this specification.

4.2 Stored Data Values in CPI field

A Content Protection Information (CPI) field is located in a GCI packet (GCI_PKT). The format and defined value is the same as the one defined in the *AACS HD DVD and DVD Pre-recorded Book*.

4.3 Protection for EVOB

An EVOB is protected by content encryption on a Pack basis using a Title Key. The protection format and the condition where Pack is prohibited or allowed to protect is the same as the ones defined in the *AACS HD DVD and DVD Pre-recorded Book*.

Pack encryption format, encryption method and decryption method are also the same as the ones defined in the *AACS HD DVD and DVD Pre-recorded Book*.

Before checking Content Hash of P-EVOBs for the Prepared Video Content on a recordable media, the integrity of Content Hash Table #1 shall be verified based on the Prepared Video Content Certificate File. The method of content hash checking and condition are the same as the ones defined in the *AACS HD DVD and DVD Pre-recorded Book*.

Before decrypting an EVOB, a Licensed Player shall verify the Prepared Video Content Certificate, the MAC of the Title Usage File and Content Hash Table according to the verification procedure defined in the *AACS HD*

DVD and DVD Pre-recorded Book. If the verification fails, the Licensed Player shall abort to playback. The Licensed Player shall also verify Prepared Video Token according to the verification procedure defined in Chapter 3 before decrypting an EVOB. If the verification fails, the Licensed Player shall abort to playback. Before using a Title Key, the Licensed Player shall verify the Binding MAC associated with the Title Key. Please refer to the example of decryption of an EVOB described in *AACS HD DVD and DVD Pre-recorded Book*.

4.3.1 Bus Encryption/Decryption

See the *AACS Introduction and Common Cryptographic Elements* book for Bus Encryption/Decryption. Table 4-1 shows the Bus Encryption format for a Pack. If B_flag in a sector is set, Main Data (See the *AACS HD DVD and DVD Pre-recorded Book*) shall be encrypted by a Licensed Drive as shown in Table 4-1. When recording a sector that is required, the Main Data shall be encrypted by host in the same manner as Note that Main Data of a sector is identical to the data in a Pack. For each Pack, the first 128 bytes are unencrypted (the Unencrypted Portion) and the remaining 1920 bytes are called Bus Encrypted (the Encrypted Portion). Main Data is transferred to a PC host in this Bus Encryption format.

Each Bus Encrypted Pack is encrypted by a 128-bit BE Key (K_{be}).

On sector reads, the BE Key (K_{be}) is calculated with a 128-bit Read Data Key (K_{rd}), a 32-bit BE Key Data (D_{be}) and a 96-bit constant value as follows:

$$K_{be} = \text{AES-G}(K_{rd}, D_{be} \parallel \text{DEADBEEFDEADBEEFDEADBEEF}_{16}),$$

On sector writes, the BE Key (K_{be}) is calculated with a 128-bit Write Data Key (K_{wd}) and a 32-bit BE Key Data (D_{be}) and a 96-bit constant value as follows:

$$K_{be} = \text{AES-G}(K_{wd}, D_{be} \parallel \text{DEADBEEFDEADBEEFDEADBEEF}_{16}),$$

Note that BE Key Data (D_{be}) is just data between the 15th byte and the 18th byte of a Pack, inclusive.

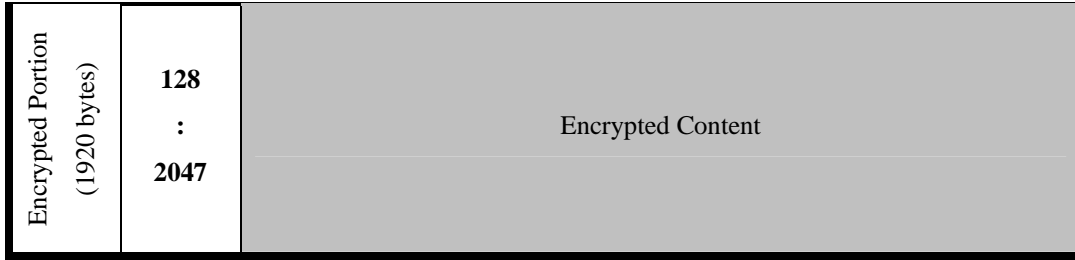
The Encrypted Portion (C_e) is encrypted as follows:

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

where C is the data in the Main Data.

Table 4-1 – Bus Encryption Format

	Bit	7	6	5	4	3	2	1	0
	Byte								
Unencrypted Portion (128 bytes)	0	Data defined in the <i>HD DVD-Video specification</i>							
	:								
	13								
	14	BE Key Data (D_{be})							
	:								
	17								
	18	Data defined in the <i>HD DVD-Video specification</i>							
	:								
	127								



A PC host shall perform Bus Decryption when it reads an EVOB (a P-EVOB or an S-EVOB) on a Disc. The following is an example of Bus Decryption by the PC host:

Step 1: Calculate the BE Key. When a PC Player reads an EVOB, the Player calculates a 128-bit BE Key (K_{be}) using Read Data Key (K_{rd}) and BE Key Data (D_{be}) as follows:

$$K_{be} = \text{AES-G}(K_{rd}, D_{be}).$$

Step 2: Decrypt the Pack. The Encrypted Portion (C_e) of the current Bus Encrypted Pack is decrypted as follows:

$$C = \text{AES-128CBCD}(K_{be}, C_e).$$

A Licensed Drive shall perform Bus Decryption when a PC host writes an EVOB (a P-EVOB or an S-EVOB) on a Disc. The following is an example of Bus Decryption by the Licensed Drive:

Step 1: Calculate the BE Key. When an EVOB is written, the Licensed Drive calculates a 128-bit BE Key (K_{be}) using Write Data Key (K_{wd}) and BE Key Data (D_{be}) as follows:

$$K_{be} = \text{AES-G}(K_{wd}, D_{be}).$$

Step 2: Decrypt the sector. Each sector of the Encrypted Portion (C_e) of the current Bus Encrypted Pack is decrypted as follows:

$$C = \text{AES-128CBCD}(K_{be}, C_e).$$

Step 3: Write the sector with setting the B_flag in the sector header to “1₂” on to the disc.

Note here that a BE Key for an ADV_PCK or for a NV_PCK is not AACS confidential information and need not be securely protected in a robust environment.

(Note) Other adaptation books of this specification may define a flag, like the B_flag in this book, and also encryption scheme for the bus encryption. However, if the Licensed Drive is not designed to be compliant to such books, the Licensed Drive is not required to recognize the flag defined in such books, nor to encrypt the sector data associated with the flag.

4.4 Protection for Advanced Resources

The encapsulation format and the condition where Advanced Resource is prohibited or allowed to encapsulate are the same as the ones defined in the *AACS HD DVD and DVD Pre-recorded Book*.

Encryption method and calculation of MAC are also the same as the ones defined in the *AACS HD DVD and DVD Pre-recorded Book*.

Before verification of the hashes, the Prepared Video Content Certificate file shall be at first verified. The condition of verification of Prepared Video Content Certificate is the same as the one defined in the *AACS HD DVD and DVD Pre-recorded Book*.

Before using an ARF encapsulated in Encapsulation Format for Hash or in Encapsulation Format for Encryption and Hash, the AACS module in the Licensed Player shall check the integrity by means of the content hash.

4.5 Secure Move

The detailed method for Secure Move of Prepared Video Content on a recordable media is described in Chapter 3 of the *AACS Prepared Video Book*.

Chapter 5

Download, Streaming and Online-Enabling

5 Download, Streaming and Online-Enabling

5.1 Introduction

The binding mechanism and API of Download, Streaming and Online-Enabling are identical to that for pre-recorded content. Refer to Chapter 5 of the *AACS HD DVD and DVD Pre-recorded Book* for details.

5.2 Managed Copy

When the source content for a Managed Copy is the Prepared Video Content recorded on a recordable media, Managed Copy mechanism is identical to that for pre-recorded content. Refer to Chapter 5 of the *AACS HD DVD and DVD Pre-recorded Book* for details.

When the MCOT destination is the recordable media, refer *AACS Prepared Video Book* for the details.

This page is intentionally left blank.

Chapter 6

Protection of HD DVD-Video Content in Persistent Storage

6 Protection of HD DVD-Video Content in Persistent Storage

The Protection mechanism of HD DVD-Video content in Persistent Storages is identical to that for pre-recorded content. Refer to Chapter 6 of the *AACS HD DVD and DVD Pre-recorded Book* for details.

This page is intentionally left blank.

Chapter 7

Sequence Key

7 Sequence Key

The Sequence Key mechanism for Prepared Video Content is identical to that for pre-recorded content. Refer to Chapter 4 of the *AACS Pre-recorded Video Book* and Chapter 7 of the *AACS HD DVD and DVD Pre-recorded Book* for details.

This page is intentionally left blank.

Appendix A

Additional requirements for carriage of SRM

A Additional requirement for carriage of SRM

A.1 Introduction

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

A.2 SRM (System Renewability Message)

A.2.1 SRM for DTCP

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

A.2.2 SRM for HDCP

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