Content Protection for Prerecorded Media Specification

DVD Book

Intel Corporation
International Business Machines Corporation
Matsushita Electric Industrial Co., Ltd.
Toshiba Corporation

Revision 0.93
January 31, 2001

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, MEI, and Toshiba 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 an intermediate draft and is subject to change without notice. Adopters and other users of this specification are cautioned that products based on it may not be interoperable with the final version or subsequent versions thereof.

Intellectual Property

Implementation of this specification requires a license from the 4C Entity, LLC.

Contact Information

Please address inquiries, feedback, and licensing requests to the 4C Entity, LLC:

- Licensing inquiries and requests should be addressed to cppm-licensing@4Centity.com.
- Feedback on this specification should be addressed to cppm-comment@4Centity.com.

The URL for the 4C Entity, LLC web site is http://www.4Centity.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

This page is intentionally left blank.

Chapter 1
Introduction

1.

1.1 Purpose and Scope

The *Content Protection for Prerecorded Media Specification* defines a robust and renewable method for protecting content distributed on prerecorded (read-only) media types. The specification is organized into several "books". The *Introduction and Common Cryptographic Elements* book provides a brief overview of Content Protection for Prerecorded Media (CPPM), and defines cryptographic procedures that are common among its different uses. This document (the *DVD Book*) specifies additional details for using CPPM technology to protect content distributed on read-only DVD media.

The use of this specification and access to the intellectual property and cryptographic materials required to implement it will be the subject of a license. A license authority referred to as the 4C Entity, LLC is responsible for establishing and administering the content protection system based in part on this specification.

1.2 Document Organization

This specification is organized as follows:

- Chapter 1 provides an introduction.
- Chapter 2 describes the use of CPPM to protect DVD-Audio content.

1.3 References

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 When the publications are superceded by an approved revision, the revision shall apply.

4C Entity, LLC, *CPPM license agreement*

4C Entity, LLC, *CPPM Specification: Introduction and Common Cryptographic Elements, Revision 0.93*

4C Entity, LLC, *CSS Compatible DVD Drive Authentication for CPPM, Revision 0.91*

4C Entity, LLC, *Content Protection System Architecture White Paper, Version 0.81*

DVD Forum, *DVD Specifications for Read-Only Disc, Part 1: Physical Specifications, Version 1.02*

DVD Forum, *DVD Specifications for Read-Only Disc, Part 2: File System Specifications, Version 1.02*

DVD Forum, *DVD Specifications for Read-Only Disc, Part 4: Audio Specifications, Version 1.1*

1.4 Future Directions

This document currently provides details specific to using CPPM for the DVD-Audio format only. It is anticipated that CPPM technology may also be applied to other DVD read-only formats under future extensions to this specification, as authorized by the 4C Entity, LLC.

1.5 Notation

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

1.6 Abbreviations and Acronyms

The following is an alphabetical list of abbreviations and acronyms used in this document:

4C	4 Companies (IBM, Intel, MEI, and Toshiba)
ACC	Authentication Control Code
AMGM_VOBS	Video Object Set for Audio Manager Menu
AOTT_AOBS	Audio Object Set for Audio Only Title
ASCII	American Standard Code for Information Interchange
ASV	Audio Still Video
ASVOBS	Audio Still Video Object Set
C-CBC	Converted Cipher Block Chaining
C2	Cryptomeria Cipher
CCI	Copy Control Information
CGMS	Copy Generation Management System
CPPM	Content Protection for Prerecorded Media
CPR_MAI	Copyright Management Information
CSS	Content Scramble System
DVD	Digital Versatile Disc
DVD-ROM	Digital Versatile Disc – Read-Only Memory
ID	Identifier
ISRC	International Standard Recording Code
LLC	Limited Liability Company
lsb	Least Significant Bit
MKB	Media Key Block
MPEG	Moving Picture Experts Group
msb	Most Significant Bit
PC	Personal Computer
PES	Packetized Elementary Stream

Chapter 2
CPPM for DVD-Audio

2. Introduction

This chapter specifies details for using CPPM technology to protect DVD-Audio content. The DVD-Audio format is defined by the DVD Forum for storing high-quality multi-channel audio with optional still and moving pictures on read-only DVD media. The format is the subject of a license from the DVD Forum, which also publishes specifications describing the format in detail (see the corresponding references in Section 1.3):

- DVD Specifications for Read-Only Disc, Part 1: Physical Specifications
- DVD Specifications for Read-Only Disc, Part 2: File System Specifications
- DVD Specifications for Read-Only Disc, Part 4: Audio Specifications

This chapter assumes the reader is familiar with the DVD-Audio format, and focuses on those aspects of the format that are relevant to CPPM protection.

2.1 Device Requirements

For the first generation, each CPPM compliant DVD-Audio Playback Device is given a set of 16 Device Keys, denoted K_{d_0},K_{d_1},…,K_{d_15}. These keys are provided by the 4C Entity, LLC, and are for use in processing the MKB to calculate the Media Key (K_m), as described in the *Introduction and Common Cryptographic Elements* book of this specification. Key sets may either be unique per device, or used commonly by multiple devices. The CPPM license agreement describes the details and requirements associated with these two alternatives. A device shall treat its Device Keys as highly confidential, and their associated Row values as confidential, as defined in the CPPM license agreement.

2.2 Format of CPPM Related Components

This section describes location and format details of CPPM related components stored on CPPM protected DVD-Audio discs. Figure 2-1 gives an overview showing the locations of some these components.

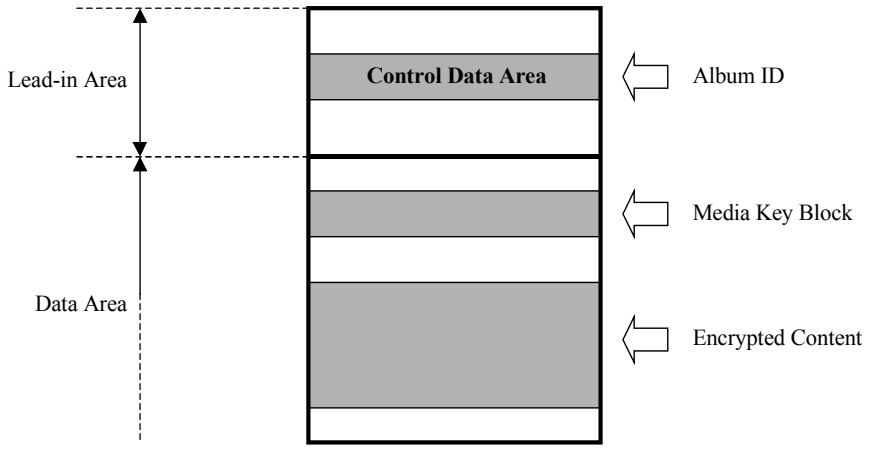

Figure 2-1 – Locations of CPPM Components on a DVD-Audio Disc

Each side of a disc with CPPM protected DVD-Audio content contains:

- An Album Identifier (ID_{album}) prerecorded in the Lead-in Area
- A Media Key Block (MKB) prerecorded as a specific file in the Data Area.
- Encrypted Content prerecorded as specific files in the Data Area.

The following subsections describe details regarding the location, format, and assignment method for these and other CPPM related components stored on a DVD-Audio disc. The descriptions are categorized according to the DVD Forum defined layer or "level" (physical, file system, or application) they correspond to.

2.2.1 Physical Level Components

2.2.1.1 Album Identifier

Each side of a disc with CPPM protected DVD-Audio content shall contain a 64-bit Album Identifier (ID_{album}), which is placed in the Lead-in Area by the disc manufacturer. Specifically, the Album Identifier is placed in bytes 80 through 87 of Control Data Area Sector #2, as shown in Table 2-1.

Table 2-1 – Location of Album Identifier in Control Data Area Sector #2

Bit / Byte	7	6	5	4	3	2	1	0
0	(data defined in other specifications)							
:								
79								
80	*(reserved: 00_{16})*							
81	ID_{album}							
:								
87								
88	(data defined in other specifications)							
:								
2047								

The most significant 8 bits of the Album Identifier (stored in byte 80) are reserved for future use, and are currently defined to have a value of zero. For forward compatibility, a non-zero value in these 8 bits shall not be considered an error. For the remaining 56 bits, the content provider individually assigns a secret, unpredictable (e.g. random) value to each DVD-Audio album to be protected using CPPM. At the content provider's discretion, all pressings of a given album may contain the same ID_{album} value, or different values may be assigned for different pressings.

Note that the role of the Album Identifier is not that of individual media identification. Rather, it serves as an album-specific value that is integrated into CPPM cryptographic key management, and placed in a location that is not writable on compliant DVD recordable/rewritable media. In a PC system, it is accessed using the DVD drive authentication protocol, as described in Section 2.4. For consistency with the other (non-CPPM) uses of that protocol, the confidentiality of the data in Control Data Area Sector #2, including the Album Identifier value, must be maintained.

2.2.2 File System Level Components

2.2.2.1 Media Key Block (MKB)

Each side of a disc with CPPM protected DVD-Audio content shall contain a Media Key Block (MKB), which is provided by the 4C Entity, LLC. The MKB is stored in a file named DVDAUDIO.MKB, and also in a duplicate backup file named DVDAUDIO.BUP, both of which are located in the AUDIO_TS subdirectory in the Data Area of the disc. The DVDAUDIO.MKB and DVDAUDIO.BUP files contain identical data, so that if a data integrity error is encountered in one, the other may be used. Hereafter, the term MKB File refers to either one of these files. Table 2-2 shows the data structure of the MKB File.

Table 2-2 – Data Structure of the Media Key Block (MKB) File

Bit / Byte	7	6	5	4	3	2	1	0
0	File Identifier (“DVDAUDIO.MKB”)							
:								
11								
12	MKB Length (N)							
:								
15								
16	Media Key Block							
:								
15 + N								
16 + N	(unused bytes filled with zeros)							
:								
3,145,727								

The first byte of the MKB File shall coincide with the first byte of an ECC Block, and for the first generation, the MKB File shall have a fixed size of 3,145,728 bytes (96 ECC Blocks). The first 12 bytes of the file make up the File Identifier field, which shall contain a value corresponding to the ASCII string “DVDAUDIO.MKB” (this same value shall be used in both the DVDAUDIO.MKB and DVDAUDIO.BUP files). The next 4 bytes contain the MKB Length field, which shall indicate the length of the Media Key Block in bytes. Directly after the MKB Length field is the Media Key Block itself, which can vary in length as described below. Any unused bytes at the end of the file shall be filled with zeros.

The MKB itself shall be formatted as described in the *Introduction and Common Cryptographic Elements* book of this specification. The MKB can vary in size, with the maximum size for the first generation equal to 3,145,728 – 16 = 3,145,712 bytes. For the first-generation DVD-Audio MKB, 16 Device Key Columns are defined, and for a given Column there may be at most 65,536 Rows defined.

Individual Media Key Blocks shall be assigned to each DVD-Audio album to be protected using CPPM. At the content provider’s discretion, all pressings of a given album may contain the same MKB, or different MKBs may be used for different pressings.

2.2.3 Application Level Components

The Volume Space of a DVD-Audio disc can consist of several zones, of which the DVD-Audio Zone contains content to be protected by CPPM. Within the DVD-Audio zone, Video Objects and Audio Objects can be stored in several types of Video and Audio Object Sets:

- Video Object Set for Audio Manager Menu (AMGM_VOBS)
- Audio Still Video Object Set (ASVOBS)
- Audio Object Set for Audio Only Title (AOTT_AOBS).

Within these Object Sets, the content itself is structured as a sequence of 2048-byte Packs, each corresponding to a logical sector of the DVD-ROM disc. When the content in these Object Sets is protected by CPPM, certain Packs within the Object Sets are encrypted, as summarized in Figure 2-2.

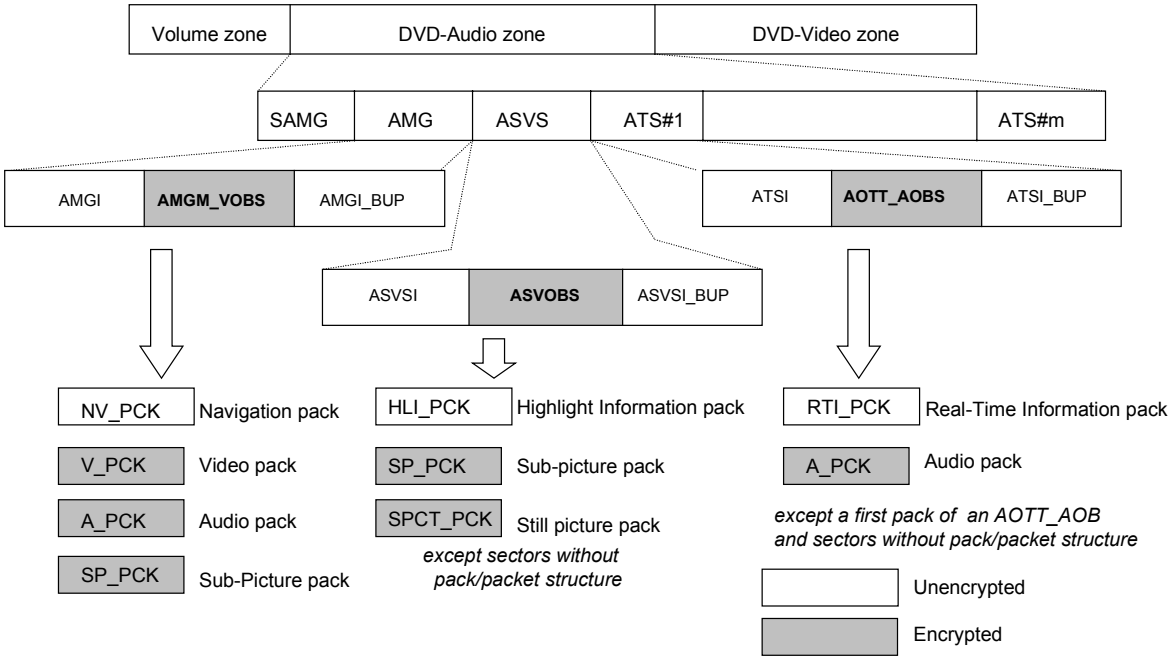

Figure 2-2 – CPPM Encryptable Packs in the DVD-Audio Zone

Packs of the types shown shaded in gray (with the indicated exceptions) are referred to collectively in this document as Encryptable Packs. The conditions under which CPPM encryption is actually applied to these Packs are described below. Table 2-3 shows the format of an Encryptable Pack, as it pertains to CPPM.

Table 2-3 – Format of Encryptable Pack

	Byte \ Bit	7	6	5	4	3	2	1	0	
Unencrypted Portion (128 bytes)	0 : 23	(data defined in DVD-Audio specification)								
	24 : 31	**Key Conversion Data 1 (D_{kc_1})**								CCI Related Portion (32 bytes)
	. .	. .								
	48 : 55	**Key Conversion Data 4 (D_{kc_4})**								
	56 : 83	(data defined in DVD-Audio specification)								
	84 : 91	**Key Conversion Data 5 (D_{kc_5})**								Variable Portion (8 bytes)
	92 : 127	(data defined in DVD-Audio specification)								
Encrypted Portion (1920 bytes)	128 : 2047	**Encrypted Data (D_e)**								

When CPPM encryption is applied to an Enryptable Pack, the final 1920 bytes, referred to as the Encrypted Data (D_e), are encrypted as described in Section 2.3. Before encryption (or after decryption), those same 1920 bytes are referred to as Unencrypted Data (D_u). Byte positions 24 through 55, labeled as the CCI Related Portion, and byte positions 84 through 91, labeled as the Variable Portion, are integrated into the CPPM cryptographic key management as described in Section 2.3. The 64-bit value D_{kc_5} in the Variable Portion contains DVD-Audio content data that varies significantly from one Pack to another, and is used to vary the CPPM encryption key from Pack to Pack. The CCI Related Portion is used for the purpose described below.

Within an AOTT_AOBS, devices shall use the copy_control_information field contained in each Encryptable Pack to determine the copy control status of the content. If the UPC_EAN_ISRC_number and UPC_EAN_ISRC_data fields of the Encryptable Packs describe a valid International Standard Recording Code (ISRC), then that ISRC shall also be used. Devices shall periodically check the copy_control_information and ISRC values and use them to control copying as described in the CPPM license agreement. The Encryptable Packs of a Program shall be encrypted if and only if the audio_copy_permission sub-field of the copy_control_information field is other than 00_2 ("Copy Freely"). As a result of variable-length fields within the Pack format, the copy_control_information, UPC_EAN_ISRC_number, and UPC_EAN_ISRC_data fields' locations may vary from one Pack to another. Nevertheless, all of those fields shall be guaranteed to lie within byte positions 24 through 55, labeled collectively as the CCI Related Portion in the table above. To ensure the integrity of the CCI Related Portion, the 64-bit values D_{kc_1} through D_{kc_4} located in that range are integrated into the CPPM cryptographic key management, as described in Section 2.3. Note that in an AMGM_VOBS or ASVOBS, the CCI Related Portion will not contain data that is used to determine copy protection status. For consistency, however, the D_{kc_1} through D_{kc_4} values are always integrated into the CPPM cryptographic key management in the same way, regardless of which type of Object Set the Encryptable Pack is in.

Within an ASVOBS, devices shall determine the copy control status of the content based on whether it is encrypted. Encrypted content shall be treated as "Copy Never", and unencrypted content shall be treated as "Copy Freely". For a given ASV (picture) within the ASVOBS, the Encryptable Packs are either all encrypted or all unencrypted.

Within an AMGM_VOBS, devices shall determine the copy control status of the content based on whether it is encrypted. Encrypted content shall be treated as "Copy Never", and unencrypted content shall be treated as "Copy Freely". Within an AMGM_VOBS, the Encryptable Packs are either all encrypted or all unencrypted.

As will be described soon in updated revisions of the DVD Forum specifications referred to in Section 1.3, the encryption status of Encryptable Packs may be determined from several sources. These include the CP_SEC sub-field of the Copyright Management Information (CPR_MAI) field in the Data Area, as well as the PES_scrambling_control field of the Encryptable Pack itself. Furthermore, the copy control status of Encryptable Packs will be summarized in several locations, including CGMS fields stored both at the file system level and within sector headers in the Data Area. Such fields could also be used to determine the encryption status of Encryptable Packs to which they pertain. However, none of the fields just described are by themselves definitive with regard to the copy control status of the content. Devices shall determine the copy control status of content as described for each Object Set type in the paragraphs directly above.

2.3 Content Encryption and Decryption

Figure 2-3 illustrates the process for encryption and decryption of CPPM protected DVD-Audio content. The rest of this section describes the encryption and decryption processes in detail.

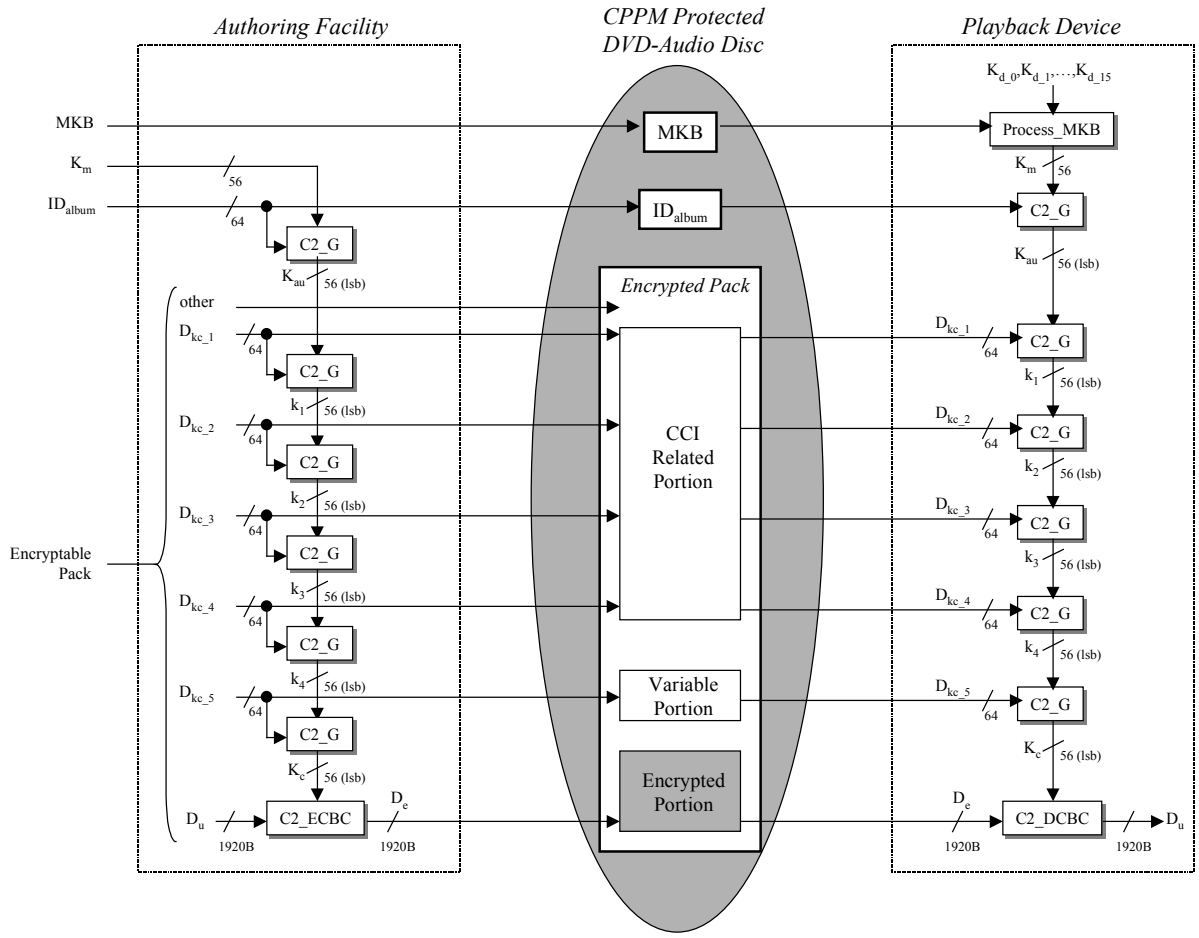

Figure 2-3 – Encryption and Decryption of CPPM Protected DVD-Audio Content

2.3.1 Content Encryption

The following steps are added to the authoring process for a DVD-Audio disc protected by CPPM.

1. Calculate Album Unique Key (K_{au}):

The MKB provided by the 4C Entity, LLC and the secret Album Identifier (ID_{album}) selected by the content provider are placed on the disc, as described in Section 2.2. The Authoring Facility uses the MKB's corresponding 56-bit Media Key (K_m) value, also provided by the 4C Entity, LLC, to calculate the 56-bit K_{au} as

$$K_{au} = [C2\_G(K_m, ID_{album})]_{lsb\_56},$$

where C2_G represents the C2 One-way Function defined in the *Introduction and Common Cryptographic Elements* book of this specification.

2. Encrypt Packs:

The Authoring Facility encrypts any Encryptable Packs having copy control status other than "Copy Freely" before placing them in the Data Area of the disc. For each such Pack, the Authoring Facility first uses the Pack's Key Conversion Data values (D_{kc_1} through D_{kc_5}) to calculate a 56-bit Content Key (K_c) for the Pack using the following steps:

$$k_1 = [C2\_G(K_{au}, D_{kc\_1})]_{lsb\_56},$$

$$k_2 = [C2\_G(k_1, D_{kc\_2})]_{lsb\_56},$$

$$k_3 = [C2\_G(k_2, D_{kc\_3})]_{lsb\_56},$$

$$k_4 = [C2\_G(k_3, D_{kc\_4})]_{lsb\_56},$$

$$K_c = [C2\_G(k_4, D_{kc\_5})]_{lsb\_56}.$$

The resulting K_c value is then used to encrypt the corresponding Pack's 1920-byte Unencrypted Data (D_u) as follows:

$$D_e = C2\_ECBC(K_c, D_u),$$

where C2_ECBC represents encryption using the C2 cipher in C-CBC mode, as defined in the *Introduction and Common Cryptographic Elements* book of this specification. Note that the C-CBC cipher chain is reset after each 1920-byte D_u encryption.

2.3.2 Content Decryption

The process to decrypt CPPM protected DVD-Audio content is as follows:

1. Calculate Media Key (K_m).

The Playback Device reads the MKB from the disc, and uses its Device Keys (K_{d_0},K_{d_1},…,K_{d_15}) to calculate the 56-bit K_m as described in the *Introduction and Common Cryptographic Elements* book of this specification.

2. Calculate Album Unique Key (K_{au}):

The Playback Device reads the secret Album Identifier (ID_{album}) from the disc, and calculates the 56-bit K_{au} as

$$K_{au} = [C2\_G(K_m, ID_{album})]_{lsb\_56}.$$

3. Decrypt Packs:

For each Pack to be decrypted, the Playback Device reads the Pack from the disc, and uses the Pack's Key Conversion Data values (D_{kc_1} through D_{kc_5}) to calculate a 56-bit Content Key (K_c) for the Pack using to the following steps:

$$k_1 = [C2\_G(K_{au}, D_{kc\_1})]_{lsb\_56},$$

$$k_2 = [C2\_G(k_1, D_{kc\_2})]_{lsb\_56},$$

$$k_3 = [C2\_G(k_2, D_{kc\_3})]_{lsb\_56},$$

$k_4 = [C2\_G(k_3, D_{kc\_4})]_{lsb\_56}$,

$K_c = [C2\_G(k_4, D_{kc\_5})]_{lsb\_56}$.

The resulting K_c value is then used to decrypt that Pack's 1920-byte Encrypted Data (D_e) as follows:

$D_u = C2\_DCBC(K_c, D_e)$,

where C2_DCBC represents decryption using the C2 cipher in C-CBC mode, as defined in the *Introduction and Common Cryptographic Elements* book of this specification. Note that the C-CBC cipher chain is reset after each 1920-byte D_e decryption.

2.4 PC Based System Architecture

CPPM provides robust protection for DVD-Audio content in PC based systems. In such systems, a DVD drive and PC host can act together as the Playback Device for CPPM protected content. Note that such playback is possible using drives that support the Content Scramble System (CSS) for DVD-Video. The procedure for CPPM decryption is the same as described in Section 2.3.2, except for additional steps required to read the secret Album Identifier from the Lead-in Area, as depicted in Figure 2-4.

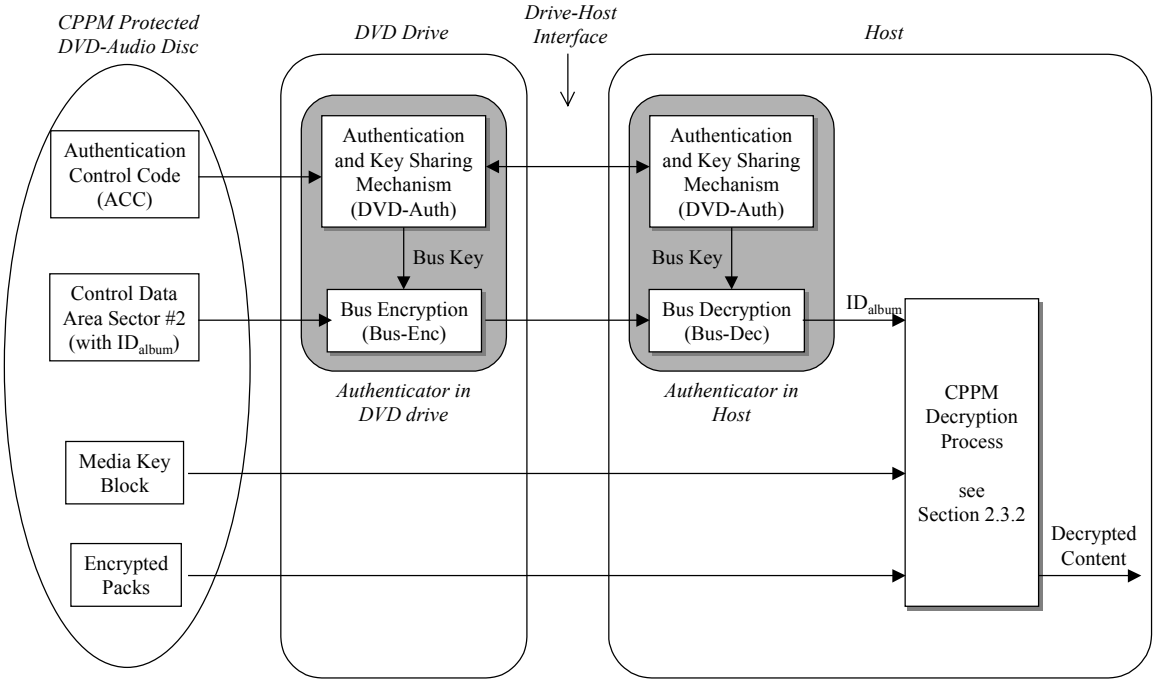

Figure 2-4 – Decryption of CPPM Protected DVD-Audio Content in a PC Based System

The same DVD drive authentication and bus encryption/decryption algorithms already defined for use with CSS for DVD-Video are used to acquire the Album Identifier from Control Data Area Sector #2. A description of those algorithms (shown in the gray shaded areas) is available separately in the *CSS Compatible DVD Drive Authentication for CPPM* document cited in Section 1.3. Both that document and the current document refer to those algorithms as:

- Authentication and Key Sharing (DVD-Auth)
- Bus Encryption (Bus-Enc)
- Bus Decryption (Bus-Dec)

The following subsection describes the use of those algorithms in the process of decrypting CPPM protected DVD-Audio content in a PC based system.

2.4.1 Content Decryption in a PC Based System

The following additional steps are used to acquire the secret Album Identifier value before decryption of CPPM protected DVD-Audio content in a PC based system.

1. Authentication and Key Sharing

   The drive and host carry out the Authentication and Key Sharing (DVD-Auth) procedure, as described in the *CSS Compatible DVD Drive Authentication for CPPM* document. One input to the DVD-Auth procedure is the Authentication Control Code (ACC). For CPPM protected DVD-Audio discs, the drive acquires this value from the ACC field, which is defined by the *CSS Compatible DVD Drive Authentication for CPPM* document. If the DVD-Auth procedure is successful, the drive and host calculate a shared Bus Key, and proceed with the remaining steps.

2. Encrypted Transfer of Control Data Area Sector #2

   Upon request from the host, the drive reads the Control Data Area Sector #2 from the disc, and encrypts it using the Bus Key and Bus Encryption (Bus-Enc) algorithm, as described in the *CSS Compatible DVD Drive Authentication for CPPM* document. The encrypted Sector #2 is transferred to the host.

3. Decryption and Extraction of the Album Identifier from the Encrypted Sector #2

   Upon receipt of the encrypted Sector #2 from the drive, the host decrypts it using the Bus Key and Bus Decryption (Bus-Dec) algorithm, as described in the *CSS Compatible DVD Drive Authentication for CPPM* document. Bytes 80 through 87 of the decrypted Sector #2 are then used as the Album Identifier (ID_{album}) value. Note that rather than decrypt all of Sector #2, some implementations may choose to only decrypt that portion that is necessary to produce the decrypted Album Identifier value.

Using the Album Identifier value acquired by these steps, the host decrypts the content according to the CPPM decryption procedure described previously in Section 2.3.2.