Content Protection for Prerecorded Media Specification

Vmedia Video Book

Intel Corporation
International Business Machines Corporation
Panasonic Corporation
Toshiba Corporation

Revision 0.9
January 23, 2009

This page is intentionally left blank.

Preface

Notice

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

List of Figures

This page is intentionally left blank.

List of Tables

This page is intentionally left blank.

Chapter 1
Introduction

1. Introduction

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 *CPPM 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 *Vmedia Video Book*, specifies additional details for using CPPM technology to protect content distributed on read-only Vmedia disc.

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 Vmedia Video content.
- Chapter 3 describes the components of the physical level.
- Chapter 4 describes the components of the file system.
- Chapter 5 describes the mapping of CPPM to Vmedia Video Format.
- Chapter 6 describes the drive-host environment architecture.

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 When the publications are superceded by an approved revision, the revision shall apply.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 1.0*

4C Entity, LLC, *CPRM Specification: Introduction and Common Cryptographic Elements, Revision 1.01*

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

Vmedia Research, Inc, *Vmedia 32 mm Optical Disc Cartridge Specification 1.0*

Vmedia Research, Inc, *Vmedia-ROM File System Format Specification 1.2*

Vmedia Research, Inc, *Vmedia-ROM Video Disc Specifications 1.0*

1.4 Future Directions

This document currently provides details specific to using CPPM for the Vmedia Video format only. It is anticipated that CPPM technology may also be applied to other Vmedia 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 *CPPM 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, Panasonic, and Toshiba)
ASCII	American Standard Code for Information Interchange
C-CBC	Converted Cipher Block Chaining
C2	Cryptomeria Cipher
CCI	Copy Control Information
CGMS	Copy Generation Management System
CPACK	Control Package
CPPM	Content Protection for Prerecorded Media
CPPM_CI	Content Protection for Prerecorded Media Copy Information
CPRM	Content Protection for Recordable Media
Drive	Vmedia Optical Drive
Host	Vmedia Software Player
ID	Identifier
LLC	Limited Liability Company
lsb (LSB)	Least Significant Bit
MKB	Media Key Block
msb (MSB)	Most Significant Bit
PPACK	Presentation Package
RNG	Random Number Generator
Vmedia-ROM	Vmedia Disc – Read-Only Memory
VSPI	Vmedia Secure Platform Information

Chapter 2
CPPM for Vmedia Video

2. CPPM for Vmedia Video

This chapter specifies details for using CPPM technology to protect Vmedia Video content. The Vmedia Video format is defined by Vmedia Research, Inc. for storing high-quality video, audio, still images and subtitles on read-only Vmedia disc. The format is the subject of a license from Vmedia Research, Inc. which also publishes specifications describing the format in detail (see the corresponding references in Section 1.3):

- Vmedia Research, Inc., *Vmedia 32 mm Optical Disc Cartridge Specification*
- Vmedia Research, Inc., *Vmedia-ROM File System Format Specification*
- Vmedia Research, Inc., *Vmedia-ROM Video Disc Specifications*

This chapter assumes the reader is familiar with the Vmedia Video 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 Vmedia Video 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 *CPPM 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 Vmedia Video discs. Figure 2-1 gives an overview showing the locations of some of these components.

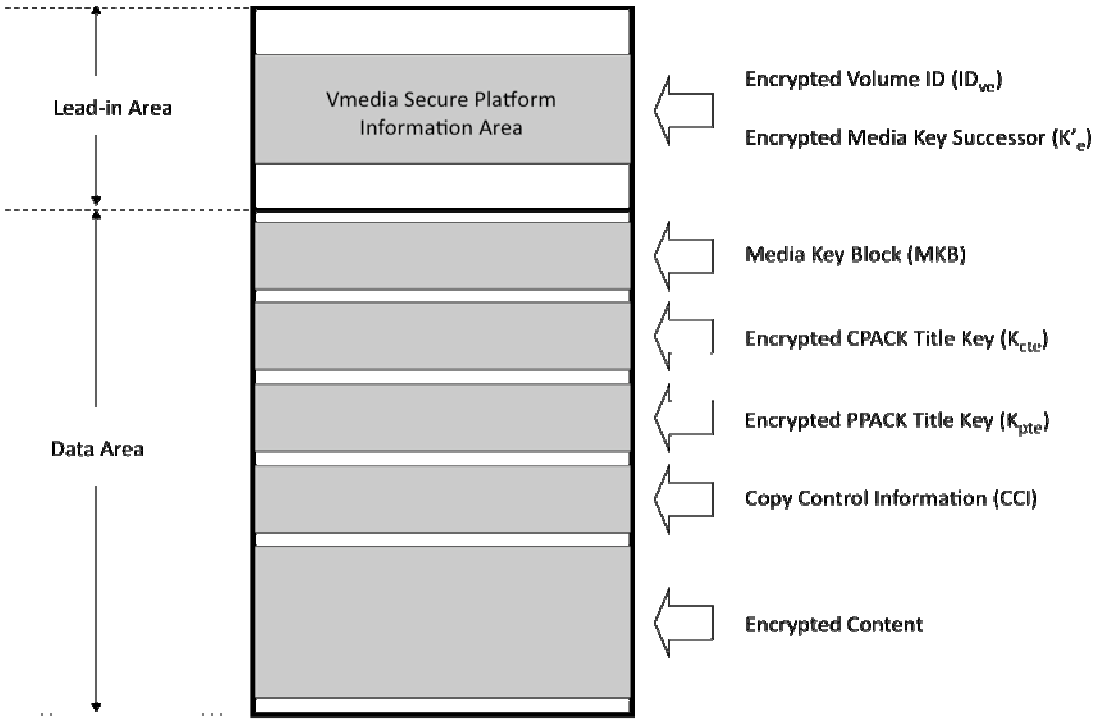

Figure 2-1 – Locations of CPPM Components on a Vmedia Video Disc

A disc with CPPM protected Vmedia Video content contains:

- An Encrypted Volume Identifier (ID_{ve}) and Encrypted Media Key Successor (K'_e) prerecorded in the Lead-in Area
- A Media Key Block (MKB) prerecorded as a specific file in the Data Area.
- An Encrypted Title Key for Control Data, the Encrypted CPACK Title Key (K_{cte}), prerecorded as a specific file in the Data Area.
- An Encrypted Title Key for Presentation Data, the Encrypted PPACK Title Key (K_{pte}), prerecorded as a specific file in the Data Area.
- Encrypted Content prerecorded as specific files in the Data Area.
- Copy Control Information (CCI) prerecorded as a specific file 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 Vmedia Video disc. The descriptions are categorized according to the Vmedia Research, Inc. defined layer or "level" (physical, file system, or application) they correspond to.

Chapter 3
Physical Level Components

3. Physical Level Components

3.1 Volume Identifier

A disc with CPPM protected Vmedia Video content shall contain a 64-bit Encrypted Volume Identifier ID_{ve}, which is placed in the Lead-in Area by the disc manufacturer. Specifically, the ID_{ve} is placed in the first eight bytes (byte 0 to byte 7) of the Vmedia Secure Platform Information (VSPI) Area within the Control Data Zone, as shown in Table 3-1.

The details on how to calculate the Encrypted Volume ID (ID_{ve}) and the Volume ID (ID_v) are described in a separate document, *CPPM Vmedia Video Book, Method to Secure Volume ID* book of this specification, a confidential document provided by the 4C Entity, LLC. The most significant 8 bits of the Volume Identifier 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.

Note that the role of the Volume Identifier is not that of individual media identification. Rather, it serves as a volume-specific value that is integrated into CPPM cryptographic key management

3.2 Calculation of Encrypted Media Key Successor (K'_e)

A disc with CPPM protected Vmedia Video content shall contain a 64-bit Encrypted Media Key Successor (K'_e) value, which is placed in the Lead-in Area by the disc manufacturer. Specifically, K'_e is placed in the last eight bytes (byte 2040 to byte 2047) of the Vmedia Secure Platform Information (VSPI) Area within the Control Data Zone, as shown in Table 3-1.

The disc manufacturer generates the Encrypted Media Key Successor value (K'_e) from the 56-bit Media Key (K_m) value and the 56-bit Drive Key (K_{drive}), both provided by the 4C Entity, LLC. The constant K_{drive} shall be treated as confidential value. The values K' and K'_e are calculated as follows:

$K' = C2\_G(K_m, 00_{16} \| K_m)$, and

$K'_e = C2\_E(K_{drive}, K')$

Table 3-1 – Components of the Vmedia Secure Platform Information Area

Bit / Byte	7	6	5	4	3	2	1	0
0	ID_{ve}							
:								
7								
8	(data defined in other specifications)							
:								
2039								
2040	Encrypted Media Key Successor (K'_e)							
:								
2047								

Chapter 4
File System Level Components

4. File System Level Components

4.1 Media Key Block (MKB)

A disc with CPPM protected Vmedia Video content shall contain a Media Key Block (MKB), which is provided by the 4C Entity, LLC. The MKB is stored in a file named VMEDIAVD.MKB, in the directory \VSPI. A duplicate backup file named VMEDIAVD.MKB is located in the subdirectory \VSPI\BACKUP in the Data Area of the disc. The \VSPI\VMEDIAVD.MKB and \VSPI\BACKUP\VMEDIAVD.MKB files contain identical data, so that if an error is encountered in one, the other may be used. Hereafter, the term MKB File refers to either one of these files. Table 4-1 shows the data structure of the MKB File.

Table 4-1 – Data Structure of the Media Key Block (MKB) File

Bit / Byte	7	6	5	4	3	2	1	0
0	File Identifier (“VMEDIAVD.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 “VMEDIAVD.MKB” (this same value shall be used in both the \VSPI\VMEDIAVD.MKB and \VSPI\BACKUP\VMEDIAVD.MKB 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 *CPPM 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 Vmedia Video 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 Vmedia Video title to be protected using CPPM. At the content provider's discretion, all pressings of a given title may contain the same MKB, or alternatively different MKBs may be used for different pressings.

4.2 Encrypted CPACK Title Key, Encrypted PPACK Title Key and Copy Control Information Data File

A disc with CPPM protected Vmedia Video content shall contain an Encrypted CPACK Title Key (K_{cte}), Encypted PPACK Title Key (K_{pte}) and Copy Control Information (CCI) including Copy Generation Management System (CGMS). The CCI is used to indicate the CCI for the content stored on the Vmedia disc. All values, the K_{cte} , K_{pte} and the CCI are stored in a file named VMEDIAVD.TCD, in the directory \VSPI. A duplicate backup file named VMEDIAVD.TCD is located in the subdirectory \VSPI\BACKUP in the Data Area of the disc. Both files \VSPI\VMEDIAVD.TCD and \VSPI\BACKUP\VMEDIAVD.TCD contain identical data, so that if an error is encountered in one, the other may be used. Table 4-2 shows the data structure of the Encrypted CPACK Title Key (K_{cte})), the Encrypted PPACK Title Key (K_{cte}) and Copy Control Information (CCI) File.

Table 4-2 – Data Structure of the Encrypted Title Keys and Copy Control Information File

Bit / Byte	7	6	5	4	3	2	1	0
0	Encrypted CPACK Title Key (K_{te})							
:								
7								
8	Encrypted PPACKTitle Key (K_{pte})							
:								
15								
16	(Reserved: 00000000000000_{16})							
:								
22								
23	(Reserved: 000000_2)						CGMS	

In this specification the first 8–byte field of this file contains the Encrypted CPACK Title Key (K_{cte}). The next 8-byte field of this file contains the Encrypted PPACK Title Key (K_{pte}).The remaining bytes of this file contain the Copy Control Information and Reserved bits. The last 1-byte field of this file is called Copy Control Information field or CPPM Copy Information (CPPM_CI) which consists of 6-bit Reserved (000000_2) and 2-bit CGMS field. CPPM_CI is used for the calculation of encryption and decryption of Vmedia content. Table 4-3 shows the copy control status indicated by CGMS.

Table 4-3 – Copy control status indicated by CGMS

CGMS	Content Status
00_2	Copy freely
10_2	Copy One Generation
01_2	No more copies
11_2	Copy Never

Chapter 5
CPPM for Vmedia Video Format

5. CPPM for Vmedia Video Format

5.1 Application Level Components

The Volume Space of a Vmedia Video disc can consist of several zones, of which the Vmedia Video Zone contains content to be protected by CPPM. Within the Vmedia Video zone, video, audio, still image, fonts and subtitle content can be stored in two types of package files:

- Control Package files (CPACK) for video, audio and still images used in the menu system and fonts
- Presentation Package files (PPACK) for primary content video, audio and subtitles

These Package files are structured as a sequence of 2048-byte Blocks, each corresponding to a logical sector of the Vmedia-ROM disc. When the content in these Package files is protected by CPPM, a portion of each Block is encrypted, as summarized in Figure 5-1.

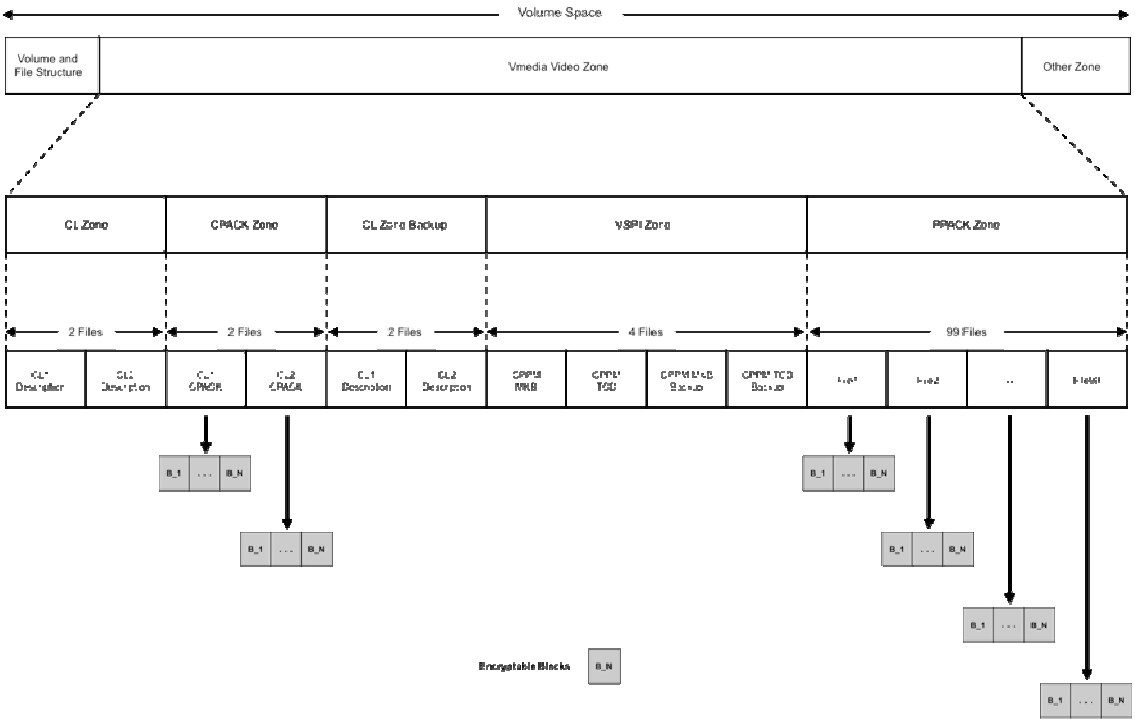

Figure 5-1 – CPPM Encryptable Blocks in the Vmedia Video Zone

Data of the types shown shaded in gray are referred to collectively in this document as Encryptable Blocks. The conditions under which CPPM encryption is actually applied to these Blocks are described below. Table 5-1 shows the format of an Encryptable Block, as it pertains to CPPM.

Table 5-1 – Format of Encryptable Block

	Bit / Byte	7	6	5	4	3	2	1	0
Unencrypted Portion (8 bytes)	0	**Key Conversion Data (D_{kt})**							
	…								
	7								
Encrypted Portion (2040 bytes)	8	**Encrypted Data (D_e)**							
	…								
	2047								

When CPPM encryption is applied to an Encryptable Block, the last 2040 bytes, referred to as the Encrypted Data (D_e), are encrypted as described in Section 5.2.1 Before and after encryption such 2040 bytes are referred to as Unencrypted Data (D_u) and Encrypted Data (D_e) respectively. Byte positions 0 through 7, labeled as the Unencrypted Portion are integrated into the CPPM cryptographic key management as described in Section 5.2. The 64-bit value D_{kt} in the Unencrypted Portion contains a value that varies significantly from one Block to another, and is used to vary the CPPM encryption key from Block to Block.

5.2 Content Encryption and Decryption

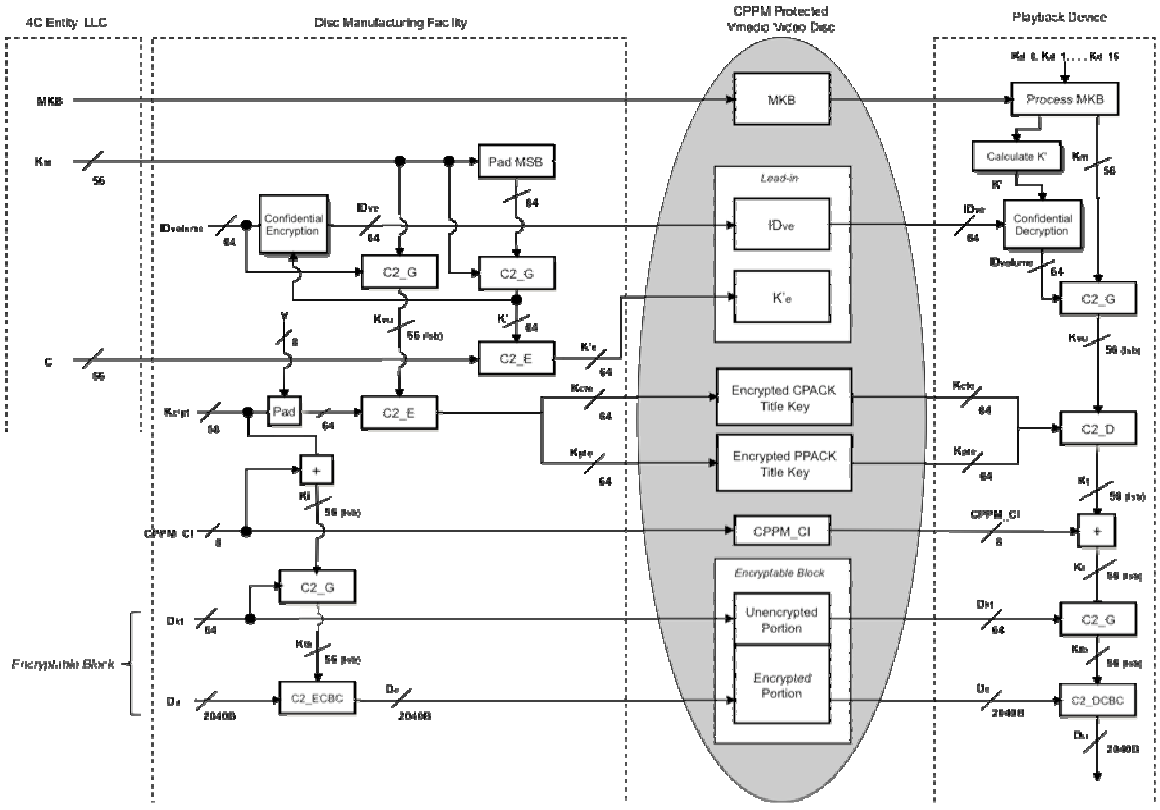

Figure 5-2 – Encryption and Decryption of CPPM protected Vmedia Video Content

Figure 5-2 illustrates the process for encryption and decryption of CPPM protected Vmedia Video content. The rest of this section describes the encryption and decryption processes in detail.

5.2.1 Content Encryption

The following steps are added to the pre-mastering process of a Vmedia Video disc protected by CPPM.

1. Calculate Volume Unique Key (K_{vu})

The MKB provided by the 4C Entity, LLC and the Encrypted Volume Identifier (ID_{ve}) generated by the disc manufacturer are placed on the disc, as described in Section 4.1 and Section 3.1 respectively. The generation of the ID_{ve} shall follow the calculations described in the "*CPPM Vmedia Video Book, Method to Secure Volume ID*" book of this specification, a confidential document provided by the 4C Entity, LLC. The disc manufacturer uses the Volume ID and the MKB's corresponding 56-bit Media Key (K_m) value, also provided by the 4C Entity, LLC, to calculate the 56-bit Volume Unique Key (K_{vu}) as

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

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

2. Calculate Media Key Successor (K')

The disc manufacturer uses the 56-bit Media Key (K_m) to calculate the 64-bit Media Key Successor (K') as follows.

$$K' = C2\_G(K_m, 00_{16} \,||\, K_m)$$

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

3. Calculate Encrypted Media Key Successor (K'_e)

The disc manufacturer uses the 56-bit Drive Key (K_{drive}), provided by the 4C Entity, LLC, and the Media Key Successor (K') to calculate the 64-bit Encrypted Media Key Successor (K'_e) as

$$K'_e = C2\_E(K_{drive}, K')$$

where C2_E represents encryption using the C2 cipher in ECB mode, as defined in the *CPPM Introduction and Common Cryptographic Elements* book of this specification. The Encrypted Media Key Successor (K'_e) is placed on the disc, as described in Section 3.2.

4. Generate CPACK Title Key (K_{ct})

The disc manufacturer generates a 56-bit random number to be the CPACK Title Key (K_{ct}). The random number is generated according to Section 2.4 in the *CPRM Introduction and Common Cryptographic Elements* book of this specification.

5. Calculate Encrypted CPACK Title Key (K_{te})

The disc manufacturer uses the Title CPACK Key (K_{ct}) from step 4, the Volume Unique Key K_{vu} from step 1 and an arbitrary 8-bit value (v) to calculate the 64-bit Encrypted Title Key value as follows

$$K_{cte} = C2\_E(K_{vu,}\ v \,||\, K_{ct})$$

where C2_E represents encryption using the C2 cipher in ECB mode, as defined in the *CPPM Introduction and Common Cryptographic Elements* book of this specification.

6. Calculate intermediate value K_i for CPACK file encryption

The disc manufacturer uses the Title CPACK Key from step 4 and CPPM_CI stored in the Vmedia disc described in Section 4.2 to calculate the intermediate 56-bit value K_i by taking

$$K_i = K_{ct} + (000000000000_{16} \,||\, CPPM\_CI)$$

where '+' represents addition modulo 2^{56}.

7. Encrypt CPACK Blocks

The disc manufacturer encrypts each encryptable Block of the CPACK and PPACK files before placing them in the Data Area of the disc. For each such Block, the disc manufacturer uses the intermediate 56-bit value (K_i) and the Block's Key Conversion Data value (D_{kt}) to calculate a 56-bit Block-Specific Title Key (K_{tb}) as follows:

$K_{tb} = C2\_G(K_i, D_{kt})$

The Block-Specific Title Key (K_{tb}) value is used to encrypt the corresponding Block's 2040-byte Unencrypted Data (D_u) as follows:

$D_e = C2\_ECBC(K_{tb}, D_u)$

where C2_ECBC represents encryption using the C2 cipher in C-CBC mode, as defined in the *CPPM Introduction and Common Cryptographic Elements* book of this specification. Note that the C-CBC cipher chain is reset after each 2040-byte D_u encryption.

8. Generate PPACK Title Key (K_{pt})

The disc manufacturer generates a 56-bit random number to be the PPACK Title Key (K_{pt}). The random number is generated according to Section 2.4 in the *CPRM Introduction and Common Cryptographic Elements* book of this specification.

9. Calculate Encrypted PPACK Title Key (K_{pte})

The disc manufacturer uses the PPACK Title Key (K_{pt}) from step 8, the Volume Unique Key K_{vu} from step 1 and an arbitrary 8-bit value (v) to calculate the 64-bit Encrypted Title Key value as follows

$K_{pte} = C2\_E(K_{vu,}\ v \parallel K_{pt})$

where C2_E represents encryption using the C2 cipher in ECB mode, as defined in the *CPPM Introduction and Common Cryptographic Elements* book of this specification.

10. Calculate intermediate value K_i for PPACK file encryption

The disc manufacturer uses the PPACK Title Key from step 8 and CPPM_CI stored in the Vmedia disc described in Section 4.2 to calculate the intermediate 56-bit value K_i by taking

$K_i = K_{pt} + (000000000000_{16} \parallel CPPM\_CI)$

where '+' represents addition modulo 2^{56}.

11. Encrypt PPACK Blocks

The disc manufacturer encrypts each encryptable Block of the PPACK files before placing them in the Data Area of the disc. For each such Block, the disc manufacturer uses the intermediate 56-bit value (K_i) and the Block's Key Conversion Data value (D_{kt}) to calculate a 56-bit Block-Specific Title Key (K_{tb}) as follows:

$K_{tb} = C2\_G(K_i, D_{kt})$

The Block-Specific Title Key (K_{tb}) value is used to encrypt the corresponding Block's 2040-byte Unencrypted Data (D_u) as follows:

$D_e = C2\_ECBC(K_{tb}, D_u)$

where C2_ECBC represents encryption using the C2 cipher in C-CBC mode, as defined in the *CPPM Introduction and Common Cryptographic Elements* book of this specification. Note that the C-CBC cipher chain is reset after each 2040-byte D_u encryption.

Steps 4 through 7 in this section describe encryption steps involving the CPACK Title Key (K_{ct}) while steps 8 through 11 describe the analogous encryption steps involving the PPACK Title Key (K_{pt}). These two sets of encryption steps are independent. Hence, steps 4 through 7 can be computed in parallel to steps 8 through 11.

5.2.2 Content Decryption

The process to decrypt CPPM protected Vmedia Video 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 *CPPM Introduction and Common Cryptographic Elements* book of this specification.

2. Calculate Volume Unique Key (K_{vu})

The Playback Device reads the Encrypted Volume Identifier, $ID_{ve,}$ from the disc. The details on the confidential additional steps to calculate the Volume Identifier are described in the *CPPM Vmedia Video Book, Method to Secure Volume ID* book of this specification which is a confidential document provided by the 4C Entity, LLC. The Playback Device uses the ID_{volume} and the Media Key (K_m) to calculate the 56-bit K_{vu} as follows:

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

3. Calculate CPACK Title Key (K_{ct})

The Playback Device uses the Encrypted CPACK Title Key (K_{cte}), the Volume Unique Key (K_{vu}) from step 2 as follows:

$K_{ct} = [C2\_D(K_{vu,} K_{cte})]_{lsb\_56}$

where C2_E represents encryption using the C2 cipher in ECB mode, as defined in the *CPPM Introduction and Common Cryptographic Elements* book of this specification.

4. Calculate intermediate value (K_i) for CPACK file decryption

The Playback Device uses the CPACK Title Key from step 3 and CPPM_CI stored in the Vmedia disc described in Section 4.2 to calculate the intermediate 56-bit value K_i by taking

$K_i = K_{ct} + (000000000000_{16} \,||\, CPPM\_CI)$

where '+' represents addition modulo 2^{56}.

5. Decrypt CPACK Blocks:

For each Block of the CPACK files to be decrypted, the Playback Device reads the Block from the disc, and uses the Block's Key Conversion Data values (D_{kt}) to calculate a 56-bit Block-Specific Title Key (K_{tb}) using the following steps:

$K_{tb} = C2\_G(K_i, D_{kt})$.

The resulting K_{tb} value is then used to decrypt that Block's 2040-byte Encrypted Data (D_e) as follows:

$D_u = C2\_DCBC(K_{tb}, D_e)$,

where C2_DCBC represents decryption using the C2 cipher in C-CBC mode, as defined in the *CPPM Introduction and Common Cryptographic Elements* book of this specification. Note that the C-CBC cipher chain is reset after each 2040-byte D_e decryption.

6. Calculate PPACK Title Key (K_{ct})

The Playback Device uses the Encrypted PPACK Title Key (K_{pte}), the Volume Unique Key (K_{vu}) from step 2 as follows:

$K_{pt} = [C2\_D(K_{vu,} K_{pte})]_{lsb\_56}$

where C2_E represents encryption using the C2 cipher in ECB mode, as defined in the *CPPM Introduction and Common Cryptographic Elements* book of this specification.

7. Calculate intermediate value (K_i) for PPACK file decryption

The Playback Device uses the PPACK Title Key from step 6 and CPPM_CI stored in the Vmedia disc described in Section 4.2 to calculate the intermediate 56-bit value K_i by taking

$K_i = K_{pt} + (000000000000_{16} \,||\, CPPM\_CI)$

where '+' represents addition modulo 2^{56}.

8. Decrypt PPACK Blocks:

For each Block of the PPACK files to be decrypted, the Playback Device reads the Block from the disc, and uses the Block's Key Conversion Data values (D_{kt}) to calculate a 56-bit Block-Specific Title Key (K_{tb}) using the following steps:

$K_{tb} = C2\_G(K_i, D_{kt})$.

The resulting K_{tb} value is then used to decrypt that Block's 2040-byte Encrypted Data (D_e) as follows:

$D_u = C2\_DCBC(K_{tb}, D_e)$,

where C2_DCBC represents decryption using the C2 cipher in C-CBC mode, as defined in the *CPPM Introduction and Common Cryptographic Elements* book of this specification. Note that the C-CBC cipher chain is reset after each 2040-byte D_e decryption.

Steps 3 through 5 in this section describe decryption steps involving the CPACK Title Key (K_{ct}) while steps 6 through 8 describe the analogous encryption steps involving the PPACK Title Key (K_{pt}). These two sets of decryption steps are independent. Hence, steps 3 through 5 can be computed in parallel to steps 6 through 8.

This page is intentionally left blank.

Chapter 6
Drive-Host Environment Architecture

6. Drive-Host Environment Architecture

CPPM provides robust protection for Vmedia Video content in Drive-Host based systems. In such systems, a Vmedia Optical Drive (Drive) and Vmedia Video Software Player (Host) can act together as the Playback Device for CPPM protected content. The procedure for CPPM decryption is the same as described in Section 5.2.2, except for additional steps required to read the Encrypted Volume Identifier (ID_{ve}) from the Lead-in Area, as depicted in Figure 6-1. The details on such confidential additional steps to calculate the Volume Identifier are described in the *CPPM Vmedia Video Book, Method to Secure Volume Identifier* book of this specification, a confidential document provided by the 4C Entity, LLC.

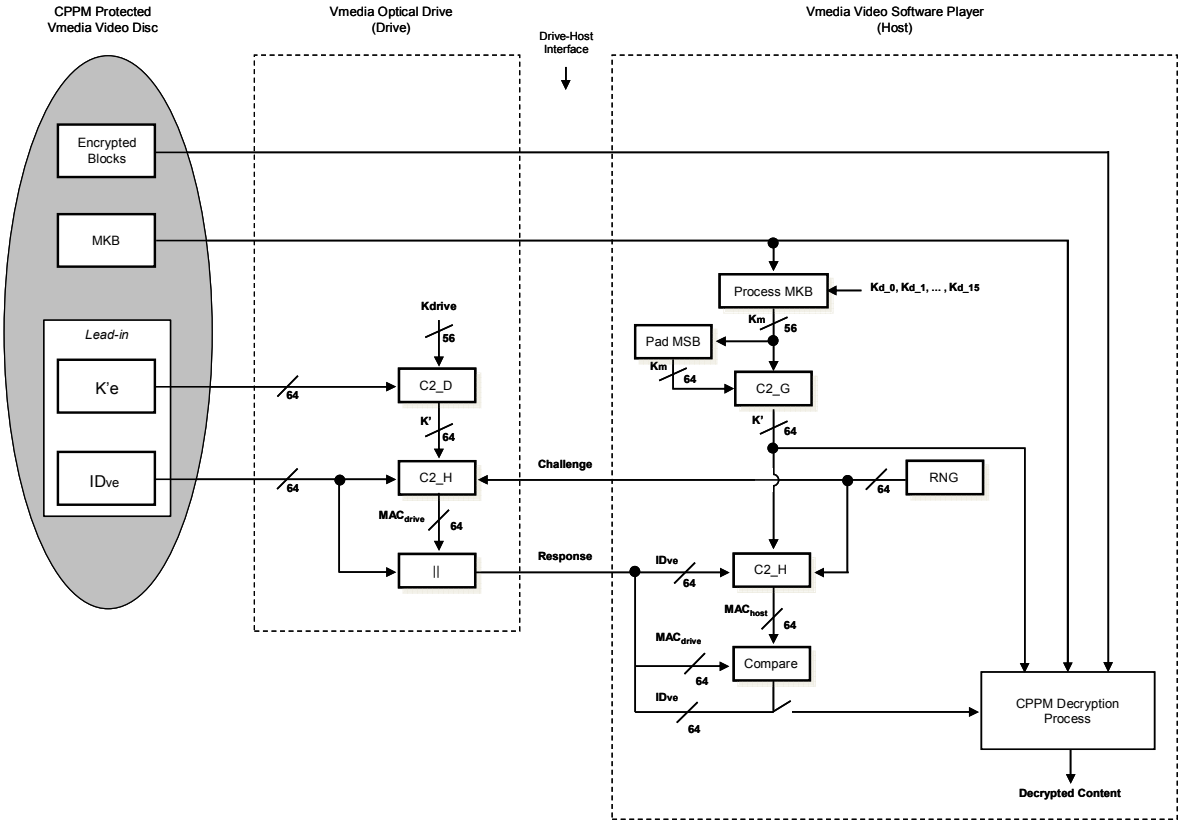

Figure 6-1 – Decryption of CPPM Protected Vmedia Video Content in a Drive-Host Environment

6.1 Content Decryption in a Drive-Host Environment

The following additional steps are used to acquire the Volume Identifier value before decryption of CPPM protected Vmedia Video content in a Drive-Host Environment. For the purpose of these additional steps, the Drive shall have the Drive Key which is given from 4C Entity, LLC. The Drive Key shall be treated as a 4C Confidential value.

1. Host Sends Challenge

   The Host generates a 64-bit random number and sends it to the Vmedia Optical Drive. The random number is generated according to Section 2.4 in the *CPRM Introduction and Common Cryptographic Elements* book of this specification.

2. Drive Calculates Media Key Successor (K')

   The Drive reads the Encrypted Media Key Successor (K'_e) from the Vmedia disc and uses it with the 56-bit Drive Key (K_{drive}) to calculate Media Key Successor (K') as

   $K' = C2\_D(K_{drive}, K'_e)$

   where C2_D represents decryption using the C2 cipher in ECB mode, as defined in the *CPPM Introduction and Common Cryptographic Elements* book of this specification.

3. Drive Generates Message Authentication Code (MAC_{drive})

   The Drive reads the Encrypted Volume Identifier (ID_{ve}) from the disc and uses it to calculate the MAC as

   $MAC_{drive} = C2\_H\ (K' \parallel Challenge \parallel ID_{ve}\ )$

   where C2_H represents the C2 Hash Function defined in the *CPRM Introduction and Common Cryptographic Elements* book of this specification.

4. Drive Generates Response

   The Drive appends the MAC_{drive} to the ID_{ve} and sends it to the Host.

5. Host Calculates Media Key (K_m)

   The Host 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 *CPPM Introduction and Common Cryptographic Elements* book of this specification.

6. Host Calculates Media Key Successor (K')

   The Host uses the 56-bit Media Key (K_m) to calculate the 56-bit Media Key Successor K' as follows:

   $K' = C2\_G(K_m, 00_{16} \parallel K_m)$

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

7. Host Generates Message Authentication Code (MAC_{host})

   The first 64-bits of the Response issued by the Drive is the ID_{ve} which the Host uses with the Challenge it generated in step 1 and the K' it generated in step 6 to calculate a MAC as

   $MAC_{host} = C2\_H(K' \parallel Challenge \parallel ID_{ve}\ )$

   where C2_H represents the C2 Hash Function defined in the *CPRM Introduction and Common Cryptographic Elements* book of this specification.

8. Host Authenticates Encrypted Volume Identifier (ID_{ve})

   The Host verifies that the MAC_{drive} from the Response issued by the Drive matches the MAC_{host} generated in step 7. If the verification fails, that is, the MAC_{drive} is not equal to the MAC_{host}, the Host shall not playback the content on the disc.

Using the Encrypted Volume Identifier value acquired by these steps, the Host decrypts the content according to the CPPM decryption procedure described previously in Section 5.2.2.