

# Advanced Access Content System (AACCS)

## *Recordable Video Book*

*Intel Corporation*

*International Business Machines Corporation*

*Microsoft Corporation*

*Panasonic Corporation*

*Sony Corporation*

*Toshiba Corporation*

*The Walt Disney Company*

*Warner Bros.*

*Final 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 © 2005-2009 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](mailto:licensing@aacsla.com).
- Feedback on this specification should be addressed to [comment@aacsla.com](mailto:comment@aacsla.com).

The URL for the AACSLA LLC web site is <http://www.aacsla.com>.

This page is intentionally left blank.

# Table of Contents

Notice .....	iii
Intellectual Property.....	iii
Contact Information.....	iii
<b>CHAPTER 1 INTRODUCTION .....</b>	<b>1</b>
<b>1. INTRODUCTION.....</b>	<b>1</b>
1.1 Purpose and Scope.....	1
1.2 Overview.....	1
1.3 Organization of this Document.....	2
1.4 References .....	3
1.5 Document History.....	3
1.6 Notation .....	3
1.7 Terminology .....	3
1.8 Abbreviations and Acronyms .....	3
<b>CHAPTER 2 COMPONENTS OF AACRS RECORDABLE MEDIA.....</b>	<b>5</b>
<b>2. INTRODUCTION.....</b>	<b>5</b>
2.1 Binding Nonce .....	5
2.2 Media Identifier (Media ID) .....	6
2.3 Media Key Block (MKB).....	6
2.4 Encrypted Title Keys.....	7
2.5 Usage Rules .....	8
2.6 Encrypted Content .....	8

<b>CHAPTER 3 ENCRYPTION AND DECRYPTION OF VIDEO CONTENT .....</b>	<b>9</b>
<b>3. INTRODUCTION.....</b>	<b>9</b>
<b>3.1 Content Encryption (General).....</b>	<b>9</b>
<b>3.2 Calculating the Protected Area Key.....</b>	<b>10</b>
<b>3.3 AACCS Encryption on Recordable Media.....</b>	<b>10</b>
<b>3.4 AACCS Decryption on Recordable Media.....</b>	<b>11</b>
<b>3.5 Uses of the Binding Nonce.....</b>	<b>11</b>
3.5.1 Secure Move of AACCS Content.....	11

# List of Figures

Figure 1-1 – System Overview (Informative).....	2
Figure 2-1 -- Location of Components on Recordable Media .....	5
Figure 3-1 – AACS Encryption and Decryption.....	9

This page is intentionally left blank.

## List of Tables

Table 2-1 – Binding Nonce.....	6
Table 2-2 -- Media Identifier .....	6

This page is intentionally left blank.

# Chapter 1

## Introduction

### 1. Introduction

#### 1.1 Purpose and Scope

The Advanced Access Content System (AACCS) specification defines an advanced, robust and renewable method for protecting entertainment content, including high-definition audiovisual content. The specification is organized into several “books”. The *Introduction and Common Cryptographic Elements* book defines cryptographic procedures that are common among the various defined uses of the protection system. This document (the *Recordable Video Book*) specifies additional details for using the system to protect audiovisual content transferred to portable/removable recordable storage media such as optical discs.

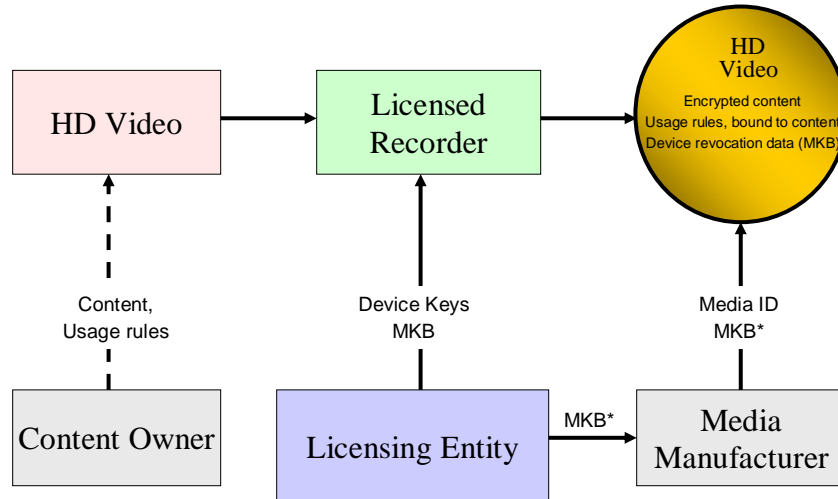
The use of this specification and access to the intellectual property and cryptographic materials required to implement it will be the subject of a license. A license authority referred to as AACCS LA LLC (hereafter referred to as AACCS LA) is responsible for establishing and administering the content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

#### 1.2 Overview

In addition to the general objectives described in the *Introduction and Common Cryptographic Elements* book of this specification, the use of AACCS for protecting recordable video content was designed to meet the following specific criteria:

- Provide robust protection for the recording of high definition video content.
- Provide for extended and extensible usage (e.g. jukebox storage, pay for copy).
- Independent of physical storage format to the degree possible.
- Maintain and update the usage rules associated with content transferred to recordable media.

Figure 1-1 presents an informative overview of the system, as used for protecting high-definition video content on recordable media. Actual details and requirements of system operation are described in subsequent chapters.



**Figure 1-1 – System Overview (Informative)**

The AACSLA provides revocation data to the licensed storage media manufacturer and to the licensed manufacturers of recording devices/applications in the form of a Media Key Block (MKB). As described in the *Introduction and Common Cryptographic Elements* book of this specification, the MKB will enable all compliant players and recorders, each using its set of device keys, to calculate that secret key. The AACSLA provides the secret device keys to licensed manufacturers for inclusion in compliant Recorder devices/applications. Separate Device key sets are not required in a device which implements both playback and record capability and separate Device key sets are not required in a device which implements more than one Format. If a set of device keys is compromised in a way that threatens the integrity of the system, an updated MKB can be provided by the AACSLA that will cause a product with the compromised set of device keys to calculate a different key than is computed by the remaining compliant products. In this way, the compromised device keys are “revoked” by the new MKB.

When an AACSLA recordable storage medium is placed in a compliant Recorder, the Recorder uses its device keys to process the MKB and calculate a secret key. The Recorder reads the Media ID and Binding Nonce from the media and derives a unique encryption key using the Usage Rules, Binding Nonce and secret key. The Recorder computes a Message Authentication Code (MAC) using the Title Key and the Media ID. The Recorder encrypts the content with a Title Key. The Title Key is then encrypted with the unique encryption key, effectively binding the content to the media. The encrypted content, Usage Rules, Message Authentication Code, and encrypted Title Key are recorded onto the storage medium. The Recorder may also update the MKB contained on the recordable storage medium based on a set of rules specified in a later chapter in this book.

### 1.3 Organization of this Document

This document is organized as follows:

- Chapter 1 provides an introduction and overview.
- Chapter 2 describes the components required to record and playback AACSLA recordable content.
- Chapter 3 describes procedures for the production (encryption) and off-line playback (decryption) of a protected recorded video Title.

## 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, *Introduction and Common Cryptographic Elements, Revision X*

AACS LA, *Pre-recorded Video Book, Revision X*

[Insert Format Specific Specs, if applicable]

## 1.5 Document History

This document version 0.95 supersedes version 0.91 dated February 17, 2006. It contains no material changes, but its version has been changed to provide continuity with the other 0.95 level documents.

Version 0.91 superseded version 0.90 dated April 13, 2005. It contained editorial improvements since the 0.90 version, plus the following changes:

- Additional clarification on how to treat media such as write-once media.
- Additional clarification on how to verify the version numbers of Read/Write MKBs and Read-Only MKBs
- Binding method for usage rules has been changed from a MAC based binding to an XOR with the Title Key based binding.
- Additional clarification on relationship between Device Key Sets and devices that support playback and/or recording and devices that support more than one format.

## 1.6 Notation

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

## 1.7 Terminology

Except where specifically noted otherwise, this document uses the terminology as described in the *Introduction and Common Cryptographic Elements* book of this specification. Additionally, the following terms are defined here:

Secure Move

Describes a process by which AACS Content can be securely moved between two Licensed Products, if authorized by the Usage and Compliance Rules.

## 1.8 Abbreviations and Acronyms

Except where specifically noted otherwise, this document uses the abbreviations and acronyms as described in the *Introduction and Common Cryptographic Elements* book of this specification.

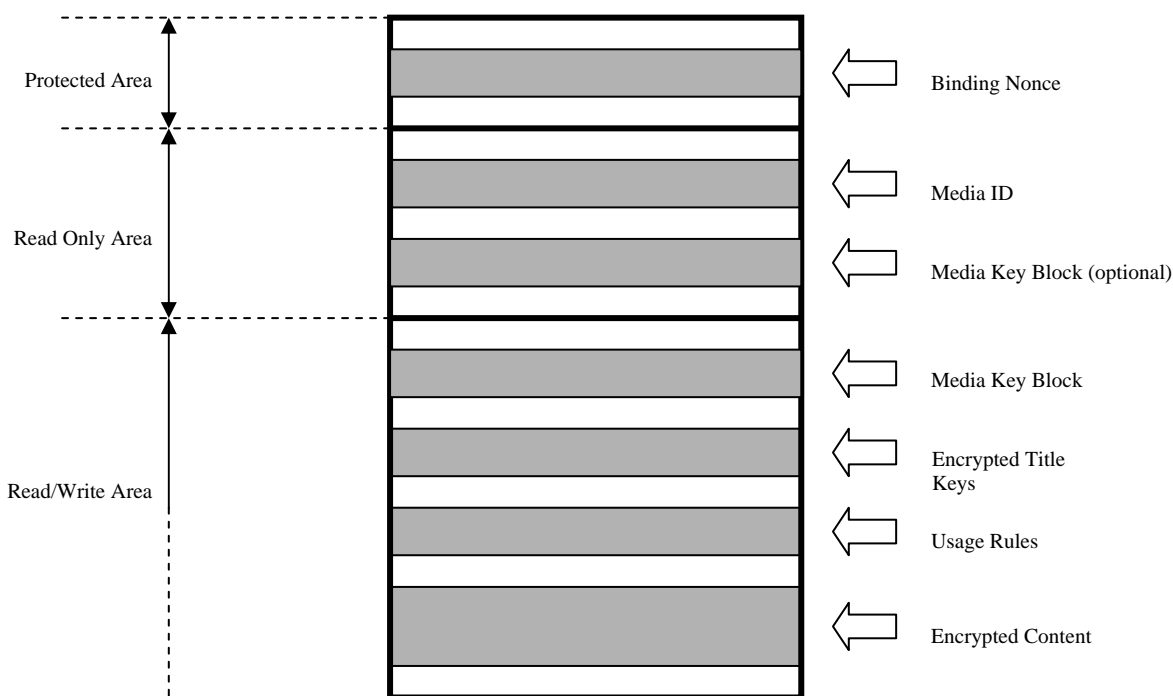
This page is intentionally left blank.

# Chapter 2

## Components of AACS Recordable Media

### 2. Introduction

This chapter specifies the components and the general location constraints required for storage on AACS Recordable Media. The actual format and location of the components is described for each supported storage format elsewhere in this specification. Figure 2-1 provides a high-level view of the position of the necessary components as defined in the *Introduction and Common Cryptographic Elements* book. The storage medium is logically partitioned into read-only, read-write and protected portions. Data in the read-only part is persistent. It has the additional feature that this data can not be duplicated by consumer devices. The Protected Area in the storage media is both read and write accessible, but only by the drive. That is, it is not directly accessible to the end user. The read/write portion has both read and write capabilities and its access is not restricted.



**Figure 2-1 -- Location of Components on Recordable Media**

### 2.1 Binding Nonce

A recorder shall be capable of generating a statistically unique (e.g., random) 128 bit nonce to be associated with each file that will contain Encrypted Title Keys. This Binding Nonce shall be updated each time the associated Title Key File is being modified. Each time a Binding Nonce is updated, every Title Key contained in the associated Title Key File shall be re-encrypted. For media (such as write-once media) where an existing Binding Nonce can not be destroyed or overwritten, the Binding Nonce (and the corresponding Title Key File) shall be written exactly once. The Binding Nonce shall be stored in the Protected Area of the optical media to maintain cryptographic control over when and how it is updated. Table 2-1 shows the logical arrangement of the Binding Nonce. The Licensed Recorder reads and writes the Binding Nonce as described elsewhere in this specification depending on the format of the underlying media. In a system using a drive-host configuration (e.g., a PC), the Binding Nonce is accessed using a drive authentication protocol as described in the *Introduction and Common Cryptographic Elements* book of this specification.

**Table 2-1 – Binding Nonce**

Byte	Bit	7	6	5	4	3	2	1	0
0									
:									
15									

## 2.2 Media Identifier (Media ID)

The licensed manufacturer of recordable media shall assign a unique 128 bit identifier to each piece of media. This identifier, referred to as the Media Identifier, is used as a safeguard against “bit-by-bit copying” of protected content, and is therefore stored on the recordable medium in a manner that cannot be altered, or duplicated by consumer recorders, as specified for each supported storage format elsewhere in this specification. Table 2-2 shows the logical arrangement of the Media ID. The Licensed Recorder reads the Media ID as described elsewhere in this specification depending on the format of the underlying media. In a system using a drive-host configuration (e.g., a PC), the Media Identifier is accessed using a drive authentication protocol as described in the *Introduction and Common Cryptographic Elements* book of this specification.

**Table 2-2 -- Media Identifier**

Byte	Bit	7	6	5	4	3	2	1	0
0									
:									
15									

## 2.3 Media Key Block (MKB)

Recordable media have Read/Write Media Key Blocks. Some physical media formats also in addition contain a Read-Only MKB created at manufacturing time. The relevant AACS book specifies whether a given physical media type is required to have a Read-Only MKB. The books also give the file names of the Read/Write MKBs. In general, each individual Application has a different file for its Read/Write MKB and each Application shall store and use exactly one MKB on each Recordable media. All MKB’s on Recordable media shall be Type 3 MKB’s. Additional specifications pertaining to the layout of the MKB are provided in the *Introduction and Common Cryptographic Elements* book of this specification.

The Read-Only MKB is used only as a means for distributing updated MKB’s. The Read/Write MKB is used to control access to the content stored on that media. For physical media formats that require a Read-Only MKB, all devices shall verify that the version number of the Read/Write MKB is greater than or equal to the version number of the Read-Only MKB during playback. Additionally, recorders shall verify the signature of the Read-Only MKB during the version comparison when performing a record step. If the version number of the Read/Write MKB is less than the version number of the Read-Only MKB, then the Read/Write MKB is invalid and the current activity (playback or recording) shall be aborted.

A recording device shall have at least 128K bytes storage for an internal MKB, and shall update the Read/Write MKB it finds on a recordable piece of media if it is out of date compared to the one in its storage. This update shall be performed each time a newer MKB is available as defined below. For media (such as write-once media) where an existing MKB can not be destroyed or overwritten, the Read/Write MKB shall be written exactly once. It is not required, however, to update the Read/Write MKB during playback or for applications

the recording device does not support. In other words, it is only required to update an out-of-date MKB during the normal process of recording application data. If the device supports a physical format which does not have a Read-Only MKB, the device's internal MKB storage shall be read/write non-volatile storage. Otherwise, the internal storage may be read-only.

The recorder shall ensure that the MKB in the Read/Write area is the most up-to-date MKB amongst the following sources:

1. The current Read/Write MKB if it exists.
2. The recorder's internal stored MKB.
3. The Read-Only MKB on the media if it required by the physical format.
4. The MKB on the source media if performing an authorized copy
5. The MKB received from a Remote Server if participating in a network based transaction

In the case where the MKB version number is the same for all available MKB's, the MKB to be used is chosen in the priority order listed above.

A recording device with non-volatile storage shall update the MKB in its storage if it receives a MKB from any of the previously listed sources 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. Since all supported AACS physical formats, both recordable and pre-recorded, use the same key scheme for Media Key Blocks, the recording device with non-volatile storage shall update it regardless of the source of the MKB.

A device updating MKBs shall use the Version Number in the MKB to determine if it is more recent. To verify the integrity of the Version Number, it shall check the signature on both the new MKB and the existing MKB. If the signature is omitted or does not verify on the new MKB, the device shall not continue with the update. If the signature is omitted or does not verify on the existing Read/Write MKB on the media, it is the device's choice whether to write a new MKB. However, it shall not update any existing content on the media protected by the current (tampered) MKB, nor record any new content using that MKB. If a Read-Only MKB is corrupt, the media shall not be used for AACS recording.

A player-only device is not required to update Read/Write MKBs, nor to have a stored MKB for such a purpose.

## 2.4 Encrypted Title Keys

The keys used to encrypt individual Titles on the media are stored in Title Key Files located in the Read/Write area. Each Title Key File is associated with exactly one Binding Nonce located in the Protected Area. No Title Key File will contain Encrypted Title Keys from more than one application. If Title Keys for an application are stored in more than one Title Key File, then the application shall precisely define how all the Title Key files are to be found on the recordable media and the application shall precisely define whether or not each Title Key File is associated with a separate Binding Nonce or if all the Title Key Files for that application are associated with only one Binding Nonce. Each Title Key is encrypted and decrypted in Electronic Code Book (ECB) mode as described in the *Introduction and Common Cryptographic Elements* book of this specification. The complete format of each Title Key File is described elsewhere in this specification. Header information in each Title Key File shall be of a length that is a multiple of 128 bits. Each individual Title Key entry shall also be of a length that is a multiple of 128 bits.

Each Title Key contained in the Title Key File(s) for a particular application, shall be re-encrypted each time the associated Binding Nonce is updated and each time the MKB associated with that application is updated on the recordable media.

For media (such as write-once media) where an existing Title Key File can not be destroyed or overwritten, a recording device may insert additional Title Keys into the Title Key File when it first creates the Title Key File. The Title Keys may be used for encrypting/decrypting content subsequently written on the media. If the media does support destroying or overwriting the Title Key File, then a recording device shall use newly generated Title Key(s) when making new recordings and shall not use any previously generated Title Key existing on the media. The secure method to distinguish between write-once media and rewritable media is defined in the applicable adaptation book.

### 2.4.1 Updating Encrypted Title Keys

Although the process of updating all the Title Keys for an application usually takes a very small amount of time (much less than a second), it is a critical time. If the device were to fail during the re-encryption process, the user's content might be lost. To greatly reduce the risk of user loss, recording devices shall begin the re-encryption process by renaming the old MKB to a temporary name before writing the new MKB. The temporary name for each MKB is defined in the particular AACCS book that describes the application. When the device completes the re-encryption process, it shall delete the temporary MKB. If any recorder discovers a temporary MKB on a piece of media, it is an indication that the encrypted Title Keys might be corrupted. The device shall perform one of the following protocols to recover the corrupted encrypted Title Keys. Which protocol is chosen depends on where the encrypted Title Keys are stored in the particular application.

A device re-encrypting Title Keys as a normal result of updating a recordable MKB shall also use these same protocols. Once the temporary MKB has been made and the new MKB has been written, the encrypted Title Keys are temporarily in an out-of-sync state. These protocols shall be used to get them back in the correct state.

#### 2.4.1.1 Recovery Protocol When the Encrypted Title Keys are in a Separate File

In this case, the original recording device shall rename the old encrypted Title Keys to a defined temporary name before beginning to write the new encrypted Title Key File. The recovery steps are:

1. Check to see if both a temporary MKB and a temporary encrypted Title Key File exists. **If** they both exist **then** go to step 2 **else** erase the remaining temporary file and exit.
2. **If** (the current MKB does not exist or is corrupt) **then** rename the temporary MKB and temporary encrypted Title Key File to the current files and exit.
3. Decrypt the Title Keys in the temporary Title Key File using the temporary MKB, and re-encrypt the Title Keys using the current MKB, writing the current Title Key File.
4. Delete the temporary MKB and the temporary Title Key File, modifying any nonce associated with the temporary encrypted Title Key File.

In some applications, encrypted Title Keys may be found in more than one file. In this case, the device shall run the protocol separately for each file, not deleting the temporary MKB until all Title Key Files have been processed.

#### 2.4.1.2 Recovery Protocol When the Encrypted Title Keys are in the Content File

In the extreme case, each content file contains its own encrypted Title Key. In that case, it is not likely that there is a temporary version of the encrypted Title Keys. Where there is no temporary version defined for the encrypted Title Keys, the protocol is slightly different:

1. If there is no current MKB or it is corrupt, rename the temporary MKB to the current MKB and exit.
2. Loop through all the content files decrypting the Title Keys using the temporary MKB:
  - a. If the Title Key verifies (using a verification string built in to the encrypted Title Key data, or by some other application-specific method), re-encrypt the Title Key using the current MKB.
  - b. Loop to step 2.
3. Delete the temporary MKB.

## 2.5 Usage Rules

The Usage Rules describe the end user's rights to protected content as formulated by the content owner. These Usage Rules are bound to the content by incorporating them in the encryption/decryption process. The Usage Rules are recorded in the Read/Write portion of the storage medium. Both Binding Nonce and Usage Rule are used to calculate encrypted Title Key as described in Section 3.3. For media (such as write-once media) where an existing Usage Rules file can not be destroyed or overwritten, the Usage Rules file shall be written exactly once.

## 2.6 Encrypted Content

Encrypted content (content or data protected by AACCS) is recorded in the Read/Write portion of the storage medium.

# Chapter 3

## Encryption and Decryption of Video Content

### 3. Introduction

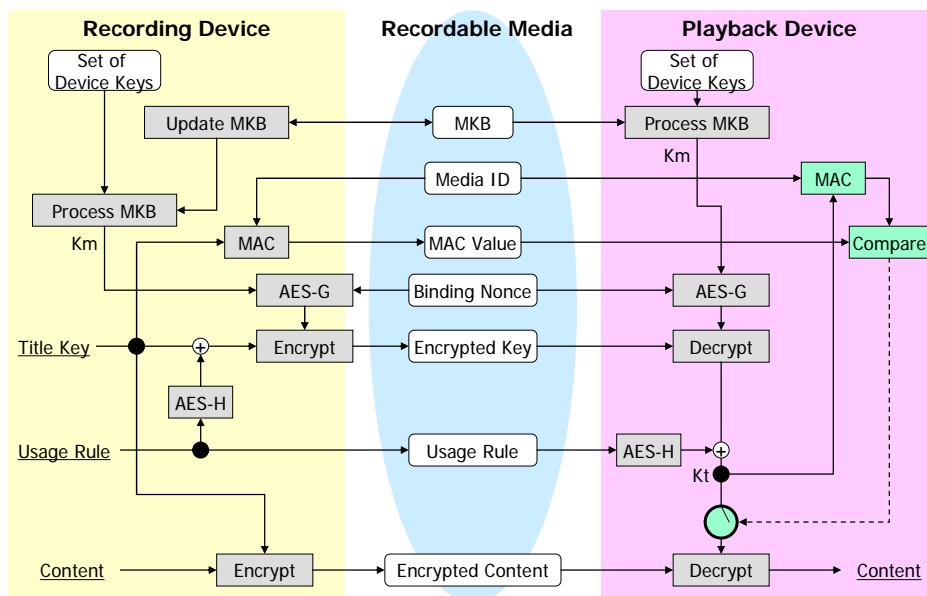
This chapter specifies the procedures for encryption and decryption of video content protected by AACS on recordable storage media where the Usage Rules have been bound to the Title Key. In general, content bound using this method will be content such as over the air “broadcast” content. The remainder of the chapter describes the procedures in detail.

### 3.1 Content Encryption (General)

Each recordable medium that contains encrypted content will contain an MKB in the Read/Write area. This MKB will enable all compliant devices, each using their set of secret Device Keys, to calculate the same Media Key as described in the *Introduction and Common Cryptographic Elements* book of this specification. . If a set of Device Keys is compromised in a way that threatens the integrity of the system, an updated MKB can be released that will cause a device with the compromised set of Device Keys to be unable to calculate the correct Media Key. In this way, the compromised Device Keys are “revoked” by the new MKB. When the first encrypted content is being recorded to a recordable medium, the recorder will place a new MKB in the Read/Write area using the rules defined earlier in this specification. During subsequent recordings, the MKB will be updated if a newer MKB version is available. When the MKB is updated, existing Title Keys shall be re-encrypted using the new Media Key that is computed from the new MKB.

For each protected Title, the Licensed Recorder calculates a cryptographic hash of the Media Key and the Binding Nonce, and uses the result to encrypt the Title’s Title Key, after first XORing the Title Key with a hash of the Usage Rules. The encrypted content, Encrypted Title Key(s), Usage Rules and MKB are stored on the recordable medium as specified for each supported storage/content format elsewhere in this specification.

Figure 3-1 presents an overview of this process.



**Figure 3-1 – AACS Encryption and Decryption**

### 3.2 Calculating the Protected Area Key

The Protected Area Key ( $K_{pa}$ ) is used to encrypt and decrypt individual Title Keys stored on recordable media. The Protected Area Key is calculated as follows:

1. Calculate the Media Key ( $K_m$ ):

The Licensed Recorder processes the Media Key Block to calculate the Media Key ( $K_m$ ) as described in the *Introduction and Common Cryptographic Elements* book of this specification.

2. Retrieve the Binding Nonce:

The Binding Nonce is stored in the Protected Area of the recordable media as specified in the format specific books of this specification. Note that in a system using a drive-host configuration (e.g., a PC), the Binding Nonce is accessed using a drive authentication protocol, as described elsewhere in this specification.

3. Calculate the Protected Area Key ( $K_{pa}$ ):

$$K_{pa} = \text{AES-G}(K_m, \text{Binding Nonce})$$

where AES-G represents the AES-based one-way function defined in the *Introduction and Common Cryptographic Elements* book.

### 3.3 AACS Encryption on Recordable Media

The following steps detail the minimum procedures for encrypting AACS content on recordable media as illustrated in Figure 3-1 above.

1. Generate the Title Key

The Licensed Recorder generates a statistically unique 128-bit Title Key ( $K_t$ ).

2. Generate a Message Authentication Code of the Media ID using the Title Key

The Licensed Recorder uses the Title Key to generate a MAC of the Media ID to ensure that the correct Media ID is being used to bind the Title to the physical media. The MAC is computed as follows:

$$\text{MAC}_{id} = \text{CMAC}(K_t, \text{ID}_m)$$

where CMAC represents a MAC function as defined in the *Introduction and Common Cryptographic Elements* book and where the MAC length shall be 128 bits.

3. Encrypt the content

The Title Key is used to encrypt the Content (C) as follows:

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

where AES-128CBCE represents encryption by the AES algorithm in CBC mode as defined in the *Introduction and Common Cryptographic Elements* book.

4. Encrypt the Title Key(s)

The Title Key(s) is encrypted ( $K_{te}$ ) as follows:

$$K_{te} = \text{AES-128E}(K_{pa}, K_t \oplus \text{AES-H}(\text{Usage Rules}))$$

where AES-128E represents encryption by the AES algorithm in ECB mode as defined in the *Introduction and Common Cryptographic Elements* book and  $K_{pa}$  as defined in Section 3.2.

5. Transfer the data

The Licensed Recorder transfers the encrypted Title Key(s) ( $K_{te}$ ),  $\text{MAC}_{id}$ , updated Usage Rules and the encrypted AACS content to the recordable media in the location and manner as specified for each supported format elsewhere in this specification.

### 3.4 AACS Decryption on Recordable Media

The following steps detail the minimum procedures for decrypting AACS content on recordable media as illustrated in Figure 3-1 above.

#### 1. Decrypt the Title Key(s)

The Title Key(s) is decrypted ( $K_t$ ) as follows:

$$K_t = \text{AES-128D}(K_{pa}, K_{te}) \oplus \text{AES-H}(\text{Usage Rules})$$

where AES-128D represents decryption by the AES algorithm in ECB mode as defined in the *Introduction and Common Cryptographic Elements* book and  $K_{pa}$  as defined in Section 3.2.

#### 2. Verify a Message Authentication Code of the Media ID ( $MAC_{id}$ ) using the Title Key

The MAC of the Media ID as stored on the media is compared to the current MAC and playback is aborted if there is a mis-match

$$MAC_{id} == \text{CMAC}(K_t, ID_m)$$

where CMAC represents a MAC function as defined in the *Introduction and Common Cryptographic Elements* book,  $MAC_{id}$  represents the MAC of the Media ID using  $K_t$  that was retrieved from the storage media and where the MAC length shall be 128 bits.

#### 3. Decrypt the Content:

The Title Key ( $K_t$ ) is used to decrypt the encrypted Content ( $C_e$ ):

$$C = \text{AES-128CBCD}(K_t, C_e)$$

where AES-128CBCD represents decryption by the AES algorithm in CBC mode as defined in the *Introduction and Common Cryptographic Elements* book.

Playback of AACS Content shall only be performed using the Title Keys and Media ID which are read from the media as defined in the applicable adaptation book. Except where otherwise provided for in these specifications, the values used to enable playback of AACS content (e.g. Title Keys and Media ID) shall be discarded upon removal of the instance of media from which they were retrieved. Any derived or intermediate cryptographic values shall also be discarded.

## 3.5 Uses of the Binding Nonce

### 3.5.1 Secure Move of AACS Content

AACS protected content can be securely moved between two compliant products, if authorized by the Usage and Compliance Rules. This move is protected against a Replay attack on the source media by use of the Binding Nonce as defined in Section 2.1. The new Binding Nonce shall be committed to the Source medium prior to writing the moved Title Key(s) to the Sink medium. In a system using a drive-host configuration (e.g., a PC), the Binding Nonce is accessed using the Protocols for Reading and Writing the Protected Area Data as defined in Chapter 4 in the *Introduction and Common Cryptographic Elements* book.

The procedures for updating the Source medium during a Secure Move are as follows:

#### 1. Decrypt Title Keys on Source medium

The Licensed Recorder calculates  $K_{pa}$  as defined in Section 3.2 and decrypts each of the Title Keys ( $K_{te}$ ) contained in the Title Key File that contains the Title Key to be moved.

$$K_t = \text{AES-128D}(K_{pa}, K_{te})$$

where AES-128D represents decryption by the AES algorithm in ECB mode as defined in the *Introduction and Common Cryptographic Elements* book.

#### 2. Delete "Moved" Title Keys from the Title Key File in working memory

The Licensed Recorder deletes the Title Key(s) that are being moved from the Title Key File as defined elsewhere in this specification.

#### 3. Generate a new Binding Nonce

The Licensed Recorder generates a new Binding Nonce to be associated with the Title Key File

4. Read the new Binding Nonce

The Licensed Recorder reads the new Binding Nonce to be associated with the Title Key File to ensure that the Binding Nonce value has been updated on the Source medium.

5. Encrypt Remaining Title Keys in working memory

The Licensed Recorder calculates the new (with the new Binding Nonce)  $K_{pa}$  as defined in Section 3.2 and Encrypts each of the remaining Title Keys ( $K_{te}$ ) contained in the Title Key File that contains the Title Key to be moved.

$$K_{te} = \text{AES-128E}(K_{pa}, K_t)$$

where AES-128E represents encryption by the AES algorithm in ECB mode as defined in the *Introduction and Common Cryptographic Elements* book.

6. Update the Title Key File on Source medium

The Licensed Recorder updates the Title Key File in the manner described in either (a) or (b) below.

(a) If the Licensed Recorder writes the updated Title Key File in the same logical address on the source medium, the recorder writes the Title Key File together with the new Binding Nonce. Then, the recorder reads the new Binding Nonce and verifies that it matches the value received in Step 4.

(b) If the Licensed Recorder writes the updated Title Key File in a different logical address on the Source medium, the recorder changes the old Binding Nonce associated with the old Title Key File. Then, the recorder reads the Binding Nonce associated with the old Title Key File and verifies that it is has been changed. Upon completion of the change process for the Binding Nonce associated with the old Title Key File, the recorder writes the Title Key File together with its new Binding Nonce. Then, the recorder reads the new Binding Nonce and verifies that it matches the value received in Step 4.

7. Transfer the Title Keys to the Sink medium

The Title Keys being moved can now be written to the Sink medium.

8. Delete the content

The content shall be deleted from the Source medium unless recovery is to be supported. If desired, the Licensed Recorder is allowed to leave a copy of the moved content on the Source medium to expedite a future “move back” (recovery) process. If a copy of the content is left on the Source medium, it will not be accessible because the associated Title Keys are no longer bound to the source medium. It will only become accessible again if the associated Title Keys have been successfully “moved back” to the Source medium.