Advanced Access Content System (AACS)

Prepared Video Book

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

Revision 0.953
Final
October 26, 2012

This page is intentionally left blank.

Preface

Notice

THIS DOCUMENT IS PROVIDED "AS IS" WITH NO WARRANTIES WHATSOEVER, INCLUDING ANY WARRANTY OF MERCHANTABILITY, NONINFRINGEMENT, FITNESS FOR ANY PARTICULAR PURPOSE, OR ANY WARRANTY OTHERWISE ARISING OUT OF ANY PROPOSAL, SPECIFICATION OR SAMPLE. IBM, Intel, Microsoft Corporation, Panasonic Corporation, Sony Corporation, Toshiba Corporation, The Walt Disney Company and Warner Bros. disclaim all liability, including liability for infringement of any proprietary rights, relating to use of information in this specification. No license, express or implied, by estoppel or otherwise, to any intellectual property rights are granted herein.

This document is subject to change under applicable license provisions.

Intellectual Property

Implementation of this specification requires a license from AACS LA LLC.

Contact Information

Please address inquiries, feedback, and licensing requests to AACS LA LLC:

- Licensing inquiries and requests should be addressed to licensing@aacsla.com.
- Feedback on this specification should be addressed to comment@aacsla.com.
- The URL for the AACS LA LLC web site is http://www.aacsla.com.

This page is intentionally left blank.

Table of Contents

This page is intentionally left blank

List of Figures

This page is intentionally left blank.

List of Tables

This page is intentionally left blank.

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 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. The AACS *Pre-recorded Video Book* specifies additional details for using the system to protect audiovisual content distributed on Pre-recorded (read-only) storage media. This document (the *Prepared Video Book*) specifies additional details for using the system to protect audiovisual content on recordable storage media in a manner functionally equivalent to the AACS Pre-recorded (read-only) format. Specifications covering other storage types, transmission media and formats are expected to be available in the future (see Section 1.7 below).

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 LLC (hereafter referred to as AACS LA) is responsible for establishing and administering the content protection system based, in part, on this specification.

1.2 Overview

The term *Prepared Video* (PV) refers to AACS Content that is semantically equivalent and nearly identical syntactically to AACS Content on AACS Prerecorded Media, but in a format appropriate to recordable media. It may be used for Electronic Sell Through (EST, i.e., downloaded), Manufacturing on Demand (such as via kiosks) or Managed Copy to optical media.

In addition to the general objectives described in the *Introduction and Common Cryptographic Elements* book of this specification, the use of AACS for protecting Prepared Video Content was designed to meet the following specific criteria:

- Provide robust protection for delivery and playback of content in an Electronic Sell Through, Manufacturing on Demand, or Managed Copy model.
- Enable content owners to directly control and manage electronic sell through delivery channels.
- Be independent of physical storage format to the degree possible.
- Provide a means for compliant players to validate that the Prepared Video disc was produced with the approval of the content owner.

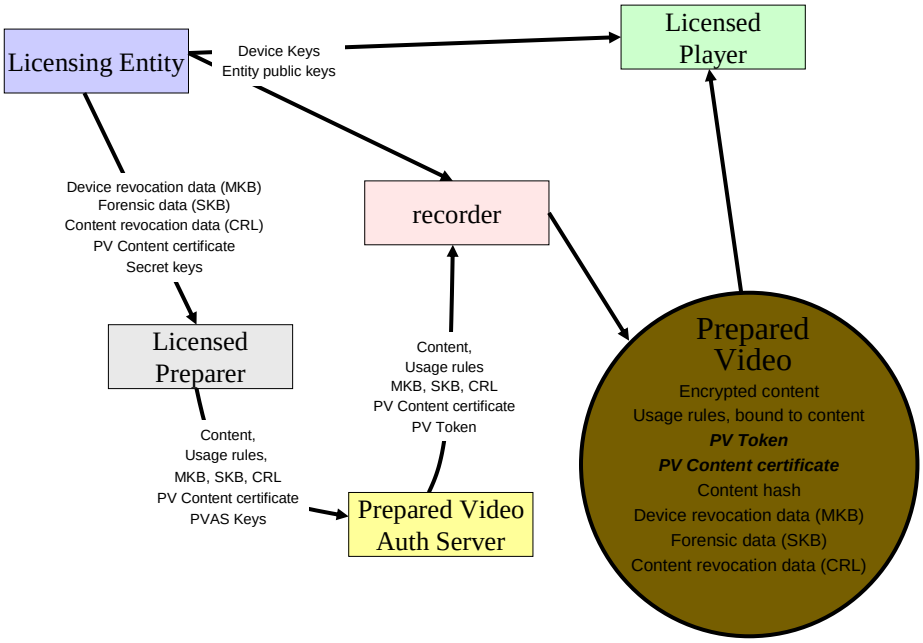

Figure 1-1 - System Overview (informational)

Figure 1-1 presents an informative overview of the system, as used for protecting video content using the Prepared Video format for EST, as defined in this specification. Actual details and requirements of system operation are described in subsequent chapters.

For clarity, it should be noted that when referring to material from the AACS *Pre-recorded Video Book*, the term "Replicator" is functionally equivalent to the use of "Preparer" in this book.

AACS anticipates that multiple scenarios may emerge to leverage the features provided by the Prepared Video format, but in particular two scenarios are contemplated at this time:

1. Direct download from a server to a recorder which in turn "burns" the downloaded image to a recordable physical media using the PV format as defined in this specification book.
2. Managed Copy from Pre-recorded AACS Content (as defined in the AACS *Pre-recorded Video Book*) to a recordable physical media using the PV format as defined in this specification book.
   - NOTE: Managed Copy from a PV formatted disc to another PV formatted disc is also a valid scenario covered by this specification. It is not called out as a separate scenario because the "flow" is the same as for Managed Copy of AACS Content on Pre-recorded media.

Prepared Video is composed of:

1. Certifiable AACS Content, as defined in the AACS *Pre-recorded Video Book*.
2. A Prepared Video Content Certificate, which resembles the Pre-recorded Content Certificate and additionally includes the list of public keys of Prepared Video Authorization Servers.
3. A Prepared Video Token, cryptographically signed by a Prepared Video Authorization Server.

1.3 Prepared Video Workflow

The term *Prepared Video Content* (PVC) refers to AACS Content that is similar to Pre-recorded AACS Content, but prepared for transfer to recordable media. It includes a Prepared Video Token as well as a new Content Certificate. The filenames and details are defined by the individual format groups, and by the format-specific books in this specification.

There are two general circumstances when the Prepared Video format can be used:

- Electronic Sell Through or Manufacturing On Demand
- Managed Copy

1.3.1 Prepared Video for Electronic Sell Through or Manufacturing On Demand

Electronic Sell Through (EST) is the process of downloading content and recording it to optical media. Manufacturing On Demand (MOD) is the process for purchasing a recorded optical disc prepared at the consumer's request. When written in the AACS Prepared Video format, both are functionally equivalent to the Pre-recorded version of the content. Both share the same workflow.

The typical workflow governing the use of Prepared Video for EST or MOD is illustrated and described below.

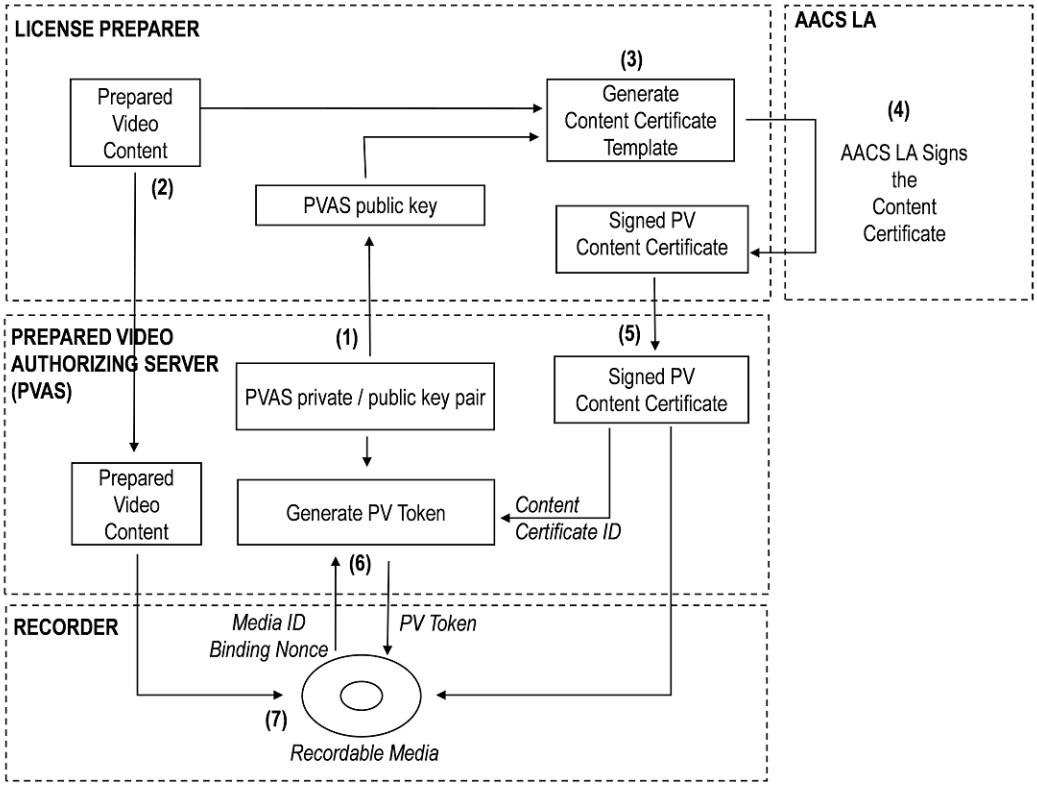

Figure 1-2 - Typical Workflow for Prepared Video, EST/MOD

The main steps of Figure 1-2 are:

1. The Licensed Preparer starts with a PVAS public key. The Licensed Preparer gets this public key in one of two ways:

   a. The PVAS can generate its own public/private key pair and send its public key to the Licensed Preparer.

   b. The Licensed Preparer can generate a public/private key pair itself and then securely provide both keys to the PVAS.

   Informative Note: For option b, it is easier for the Licensed Preparer to create a separate public/private key for each movie. Choosing option b also means that the Licensed Preparer shall define a means for securely sharing those keys with the PVAS.

2. Licensed Preparer prepares the content using AACS technology, as described in subsequent chapters of this book.
3. Licensed Preparer creates the PV Content Certificate associated with the Prepared Video, which includes the public key(s) of its Prepared Video Authorization Server(s) (PVAS) and sends such certificate to AACS LA for signature.
4. AACS LA signs the PV Content Certificate, and returns it to the Licensed Preparer.
5. The Licensed Preparer sends the signed AACS PV Content Certificate to each PVAS to which it has elected to distribute the Prepared Video. At this point, the AACS Content can now be made available for distribution.
6. Upon a request for Prepared Video Content, the PVAS:
    a. Obtains the Media Identifier of the AACS Recordable Media to which the AACS Content will be bound.
    b. Obtains the Binding Nonce that will be associated with the Prepared Video Token.
    c. Retrieves the PV Content Certificate associated with the Prepared Video Content requested.
    d. Constructs the Prepared Video Token (PVT) based on the Content Certificate ID, Binding Nonce and Media ID.
    e. Sends to the recorder:
        i) the Prepared Video Content

            Note: The Download Server would actually be responsible for sending the Prepared Video Content to the recorder in the case where the Download Server is a separate system from the PVAS.

        ii) the associated PV Content Certificate, and
        iii) the associated Prepared Video Token.
7. The recorder burns the Prepared Video Content, along with the associated PV Content Certificate and the Prepared Video Token, on the AACS Recordable Media.

A Licensed Player is required to validate the PV Content Certificate and the Prepared Video Token when playing back Prepared Video Content (see Sections 2.6 and 3.5, respectively).

1.3.2 Prepared Video for Managed Copy

The typical workflow governing the use of Prepared Video for Managed Copy is illustrated and described below.

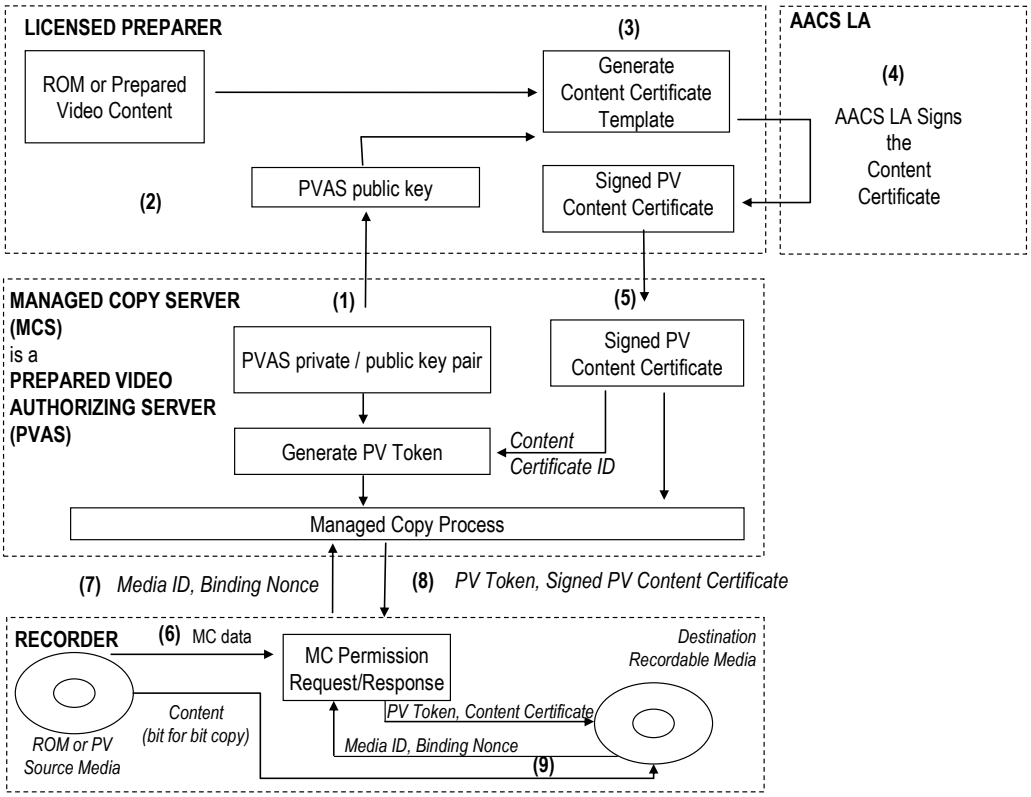

Figure 1-3 - Typical Workflow for Prepared Video, Managed Copy

The main steps of Figure 1-3 are:

0. Licensed Replicator (not shown) prepares the content using AACS technology, as described in the AACS *Pre-recorded Video* book, and creates the Content Certificate associated with the Prerecorded Video and sends such Certificate to AACS LA for signature.

1. The Licensed Preparer starts with a PVAS public key which corresponds to a MCS. The Licensed Preparer gets this public key in one of two ways:

   a. The PVAS can generate its own public/private key pair and send its public key to the Licensed Preparer. The public key of the AACS default Managed Copy Server PVAS shall be provided to the Licensed Preparer.

   b. The Licensed Preparer can generate a public/private key pair itself and then securely provide both keys to the PVAS.

   Informative Note: For option b, it is easier for the Licensed Preparer to create a separate public/private key for each movie. Choosing option b also means that the Licensed Preparer shall define a means for securely sharing those keys with the PVAS.

2. Licensed Preparer prepares the content using AACS technology, as described in subsequent chapters of this book.

3. Licensed Preparer creates the PV Content Certificate associated with the Prepared Video and sends such certificate to AACS LA for signature. The PV Content Certificate includes the public key(s) of the MCS Prepared Video Authorization Server(s) (PVAS).

4. AACS LA signs the PV Content Certificate, and returns it to the Licensed Preparer.

Informative note: When the source disc for a Managed Copy is a Prerecorded Video disc, the content hash for Prepared Video Content will be identical.

5. The Licensed Preparer sends the signed AACS PV Content Certificate, Media Key Deltas (see Section 2.8), and optionally one or more MKBs to all MCS PVAS which will authorize Managed Copies.
6. User initiates a Managed Copy transaction, and the Managed Copy Machine (MCM) collects from the Prerecorded or Prepared Video disc all data relevant to the making of the Managed Copy.
7. As part of the successful execution of the "Request Permission" portion of the Managed Copy transaction, the MCM obtains from the destination disc and sends to the MCS all of the information necessary for the construction of the Prepared Video Token, namely the Media ID and the Binding Nonce.
8. The MCM retrieves the permission response and extracts the PV Token and PV Content Certificate. The communication steps between the MCM and the MCS are described in detail in Chapter 5 of this book.
9. The MCM then records to the destination disc:
   a. the AACS Content
   b. the PV Content Certificate
   c. the PV Token

1.4 Organization of this Document

This document has the same organization as the AACS *Pre-recorded Video Book*. Where the specification is identical, a reference is given to the appropriate section of the AACS *Pre-recorded Video Book*. Only where the use and format of Prepared Video departs from that of Pre-recorded Video, does the specification go into details.

- Chapter 1 provides an introduction and overview.
- Chapter 2 describes procedures related to the authentication and revocation of Prepared Video.
- Chapter 3 describes procedures for the production (encryption) and off-line playback (decryption) of Prepared Video Content.
- Chapter 4 describes the Sequence Key Block.
- Chapter 5 describes the role of AACS Prepared Video in Managed Copy.

1.5 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 *Introduction and Common Cryptographic Elements* book.
- AACS *Pre-recorded Video Book*
- AACS *Recordable Video Book*.

1.6 Document History

This document version 0.953 supersedes version 0.952 dated July 14, 2011 and contains NO SPECIFICATION CHANGES. Version 0.952 superseded version 0.951 dated September 28, 2009 and contained NO SPECIFICATION CHANGES. Version 0.951 corrected minor typographical errors found in the first published version (0.95) of this document.

1.7 Future Directions

With its advanced, robust cryptography, key management and renewal mechanisms, it is expected that this technology will develop and expand, through additions to this specification, to address content protection for additional storage types, application formats and usage models, as authorized by AACS LA.

1.8 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.

1.9 Terminology

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

Download Client

> The component that receives the Prepared Video Content, Prepared Video Content Certificate, and the Prepared Video Token (PVT) and places each on recordable media. This client needs to connect to both the Download Server and the Prepared Video Authorization Server.

Download Server

> A server from which Prepared Video Content is downloaded. It may be co-resident with a Prepared Video Authorization Server (PVAS).

Electronic Sell Through (EST)
> Download and burn onto an optical disc in AACS Prepared Video format. Prepared Video (PV) is a format which can be used for EST. See Manufacturing On Demand (MOD).

Licensed Preparer
> An entity licensed to prepare AACS Content for online distribution in AACS Prepared Video format.

Licensed Replicator
> An entity licensed to produce AACS Pre-recorded Video on optical discs.

Media Key Delta
> The Media Key Delta provides a mechanism for assuring that players are able to unlock data items (e.g., Title Key Files) using the MKB recorded onto the PV disc when the data items were encrypted by a Media Key of a different MKB.

Manufacturing On Demand (MOD)
> Creation of AACS Prepared Video Content on an optical disc upon request of the consumer. Prepared Video is a format which can be used for MOD. It uses the same technical process as Electronic Sell Through (EST), but provides a different consumer experience.

Prepared Video (PV)
> Prepared Video is a specific packaging of AACS Content on AACS Recordable Media. It can be thought of as an AACS Pre-recorded Video adapted to a recordable format - including Content Certificates chained back to AACS LA, Content Hash Tables and full interactivity. It is used for Electronic Sell Through, Manufacturing On Demand, or Managed Copy to AACS recordable discs.

Prepared Video Authorization Server (PVAS)
> A server authorized by a content owner to create Prepared Video Tokens for their AACS Content.

Prepared Video Content (PVC)
> Content which has been provided in Prepared Video format. Examples include: Electronic Sell Through, Manufacturing On Demand and Managed Copy to AACS Prepared Video format.

Prepared Video Content Certificate (PV Content Certificate)

The AACS LA signed Content Certificate which is used for Prepared Video. It is similar to the Pre-recorded Video Content Certificate and includes the public key(s) of Prepared Video Authorization Server(s) selected by the content owner.

Prepared Video Serial Number (PVSN)

The treatment of the PVSN is identical to that of the PMSN described for Pre-recorded Video with the exception that the PVSN shall be an "unguessable" Serial Number which cannot be easily forged. If the PVSN is intended for use by the default Managed Copy Server, it contains 1 bit which denotes whether the disc is the result of a Managed Copy operation, or an EST/MOD transaction, followed by 95 check bits, followed by a 32 bit counter. A value of 1_2 in the leading bit shall indicate that the disc is the result of a Managed Copy operation and a value of 0_2 shall indicate that it is the result of an EST/MOD transaction. For additional information, refer to the Serial Number definition in Chapter 5 of the AACS *Pre-recorded Video Book*.

Prepared Video Token (PVT)

A file prepared by the Prepared Video Authorization Server which binds the AACS Content to a specific disc.

1.10 Abbreviations and Acronyms

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

AACS/PV	AACS Prepared Video
AACS/ROM	An AACS Pre-recorded Video disc
EST	Electronic Sell Through
MOD	Manufacturing On Demand
PV	Prepared Video
PVAS	Prepared Video Authorization Server
PVC	Prepared Video Content
PVCC	Prepared Video Content Certificate
PVSN	Prepared Video Serial Number
PVT	Prepared Video Token

Chapter 2
Content Revocation

2 Introduction

The content revocation mechanism for Prepared Video Content is very similar to that for Pre-recorded Content. As such, in this chapter, we will refer to the AACS *Pre-recorded Video Book*, and only elaborate on the key differences between the Pre-recorded Video and the Prepared Video formats.

2.1 Scope

Refer to Section 2.1 of the AACS *Pre-recorded Video Book*.

Summarizing the key differences:

- As with Pre-recorded Video, PV Content Certificate signature verification is required prior to playback; however, with Prepared Video, verifying the signature of the Prepared Video Token is also required.
- As with Pre-recorded Video, the Volume ID and a Serial Number are used in several key functions; however, with Prepared Video, the Volume ID and Serial Number are retrieved from the Prepared Video Token. In Prepared Video, the Serial Number is called the Prepared Video Serial Number (PVSN).

2.2 Content Signing Infrastructure

Refer to Section 2.2 of the AACS *Pre-recorded Video Book*.

2.3 Content hash table

Refer to Section 2.3 of the AACS *Pre-recorded Video Book*.

2.4 Prepared Video Content Certificate

The Prepared Video Content Certificate is similar in many respects to the Pre-recorded Content Certificate. Unless specified otherwise, the processes to compute the values in the certificate are the same as in the Pre-recorded format. As depicted in Table 2-1, the PV Content Certificate contains two additional fields: the number of PVAS entries and a series of PVAS public keys.

Table 2-1 - Data Format for the Prepared Video Content Certificate

Byte \ Bit	7	6	5	4	3	2	1	0
0	Certificate Type: 07_{16}							
1	Reserved							
2 … 5	Total_Number_of_HashUnits							
6	Total_Number_of_Layers							
7	Layer_Number							

Byte \ Bit	7	6	5	4	3	2	1	0
8 … 11	Number_of_HashUnits							
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							
24 25	Length_Format_Specific_Section #L							
26 … 26+L-1	Format_Specific_Section Reserved for definition and possible extension in format adaptation books							
26+L : 33+L	Content Hash Table Digest #1							
…	…							
26+L+(N-1)*8 … 33+L+(N-1)*8	Content Hash Table Digest #N							
34+L+(N-1)*8 : 73+L+(N-1)*8	Public Key of Authorizing Server #1							
…	…							
34+L+(N-1)*8+(M-1)*40 … 73+L+(N-1)*8+(M-1)*40	Public Key of Authorizing Server #M							

Byte \ Bit	7	6	5	4	3	2	1	0
74+L+(N-1)*8+(M-1)*40 : 113+L+(N-1)*8+(M-1)*40	Signature Data							

Note: L is the length determined by Length_Format_Specific_Section, N is the number of Content Hash Table Digests, and M is the number of Authorizing Servers. For an explanation of Length_Format_Specific_Section and Content Hash Table Digests, see Section 2.4 of the AACS *Pre-recorded Video Book.*

Refer to the AACS *Pre-recorded Video Book* for the description of each field in the PV Content Certificate, except for the following fields, which are particular to the Prepared Video format:

- A 2-byte "Number of Prepared Video Authorizing Servers Entries" field, which indicates the total number of PVAS public keys encountered in the certificate.
- A series of 40 byte "Public Key of Authorizing Server" fields, containing the public key value of each server authorized by the content owner.

Any limitations on the size of the PV Content Certificate will be defined in the format adaptation books of this specification.

As in the Pre-recorded case, the creation of the PV Content Certificate is performed by the Licensed Preparer, and the signing of the certificate is performed by a secure facility operated by AACS LA. The Licensed Preparer shall submit the certificate to the secure facility and receive the signed certificate back from that facility. The PV Content Certificate– signed by AACS LA, will be stored on the recordable media along with the AACS Content and the PV Token.

The AACS LA provides its Entity Public Keys (which correspond to the Entity Private Keys) to each licensed manufacturer for inclusion in each licensed device or application produced. Licensed Products shall treat the Entity Public Keys as Integrity Required, as defined in the license agreement. Prior to providing access to Certified Content, Licensed Products shall verify the signature of the PV Content Certificate. If at any point in the process the verification fails, such access shall be aborted. Unless the Licensed Product has a robust means of detecting change of the storage medium, it shall, whenever a PV Content Certificate is re-read from the medium, either re-verify the signature of the certificate or robustly verify that the certificate is the same as one whose signature it already verified, before using the Content Hash Table Digest contained therein for comparisons with the CHT.

Prior to providing access to Certified Content, Licensed Products shall also read and process a Content Revocation List having a List Version value equal to or greater than the Minimum CRL Version value, as described in Section 2.6 of the AACS *Pre-recorded Video Book*.

2.5 Creation of the Prepared Video Content Certificate

Refer to Section 2.5 of the AACS *Pre-recorded Video Book*.

2.6 Verifying the Prepared Video Content Certificate

The Licensed Product shall verify that the PV Content Certificate corresponds to the AACS Content on the disc: as a condition of playing, copying or other use of AACS Content stored on the recordable media as defined in the relevant format adaptation books of this specification, a Licensed Player shall verify the integrity of such AACS Content, using the procedure described in section 2.6 of the AACS *Pre-recorded*

Video Book, and repeat such procedure at each starting use of the AACS Content. If the verification of the PV Content Certificate fails, the Licensed Player shall stop usage of the AACS Content.

Refer to Section 2.6 of the AACS *Pre-recorded Video Book* for details on the verification process.

2.7 Content Revocation List (CRL)

AACS Prepared Video Content can be revoked by either the presence of an applicable Revocation Record for Content Certificate ID in the CRL, or the presence of an applicable Recordable Media Revocation Record (RMRR) in the CRL. Both of these records are described in Section 2.7 of the AACS *Pre-recorded Video Book*.

2.7.1 Revocation Record for Content Certificate ID and Prepared Video

This record has the same meaning and functionality as described in the AACS *Pre-recorded Video Book*, with the proviso that where the term Content Certificate ID is used, that the corresponding PV Content Certificate ID used.

2.7.2 Recordable Media Revocation Record (RMRR)

The structure of this CRL record is described in Section 2.7 of the AACS *Pre-recorded Video Book*. The purpose of this record is to allow a means for selectively revoking PV Content bound to specific AACS Recordable Media IDs. Further, this record can be used to revoke a specific Media ID of a specific AACS Recordable Media type.

A Licensed Player shall check for the applicability of an RMRR to a specific piece of AACS Content and/or media by the following steps:

1) Does the AACS Recordable Media Type stored in the RMRR match the AACS Recordable Media Type in question? If not, this record *is not* applicable.
2) Does the Media ID stored in the RMRR match the Media ID of the AACS Recordable Media in question? If not, this record *is not* applicable.
3) Is the value of the ICCID flag stored in the RMRR equal to 1? If it is then this RMRR *is* applicable.
4) Does the Content Certificate ID stored in the RMRR match the PV Content Certificate ID, if so this RMRR i*s* applicable, if not then this RMRR *is not* applicable.

If an applicable RMRR is found, a Licensed Player capable of supporting the AACS Prepared Video format shall not playback the AACS Content. Further, if the RMRR was found to apply at step 3 above then the AACS Recordable Media is considered revoked for use with Prepared Video and a Licensed Recorder shall not record AACS Prepared Video Content to this AACS Recordable Media.

2.8 Prepared Video Token

Prepared Video Authorization Servers (PVAS) provide to a recorder a Prepared Video Token (PVT). This token contains the public key of the authorizing server. The integrity of this public key is assured by its inclusion in the PV Content Certificate. Table 2-2 shows the format of the Prepared Video Token.

Table 2-2 - Data Format for Prepared Video Token

Byte \ Bit	7	6	5	4	3	2	1	0
0 .. 39	PVAS Public Key							

Byte \ Bit	7	6	5	4	3	2	1	0
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 Token includes:

- A 40 byte PVAS Public Key, the public key of the PVAS which signed the PVT.
- A 16 byte Prepared Video Volume ID.
- A 1 bit Prepared Video Serial Number Status Flag, where 0_2 indicates the PVSN is undefined and 1_2 means that the PVSN has been defined.
- A 1 bit Move Allowed Flag, where 0_2 means that a recorder is not allowed to perform a Move (as defined in Section 3.6) and 1_2 means that Move is allowed. Note: When the PV Content is a result of a Managed Copy to non-write once media, the Move Allowed Flag shall be set to 1_2.
- A 1 bit Bus Encryption Enabled (BEE) Flag, where 0_2 means that bus encryption is not enabled for the AACS Content covered by this PV Token, and 1_2 means that bus encryption is enabled for that AACS Content.
- A 16 byte Media Key Delta. A Player, after processing the Media Key Block, shall XOR the resulting Media Key with the value in this field before doing further processing with the Media Key, such as processing the Sequence Key Blocks, or decrypting various Title Keys.

  The Media Key Delta provides a mechanism for assuring that players are able to unlock the Title Key File using the MKB recorded onto the PV disc when the Title Key File was encrypted by a Media Key corresponding to a different MKB. Informatively, the Media Key Delta values are useful for several purposes:
  - When Prepared Video format is being used as a destination of a Managed Copy, the PVAS can set the Media Key Delta value so that the Media Key from the Media Key Block in the Managed Copy can be adjusted so that the result is the same as the Media Key in a Media Key Block associated with the original AACS Content.
  - The content owners can optionally design a given item of Pre-recorded Content and Prepared Video Content to be bit-for-bit identical, including any Sequence Key variations, even though they use different types of Media Key Blocks.

- The PVAS may optionally update Media Key Blocks, which potentially contain new revocation information, associated with previously released Prepared Video Content without re-encrypting the original AACS Content.

- A 16 byte Prepared Video Serial Number. The treatment of the PVSN is equivalent to that of the PMSN on AACS Pre-recorded Media.
- A 40 byte Prepared Video Token Signature Data, calculated using the PVAS Private Key. The PVT Signature Data is created as follows:

  PVT_{sig} = AACS_Sign($PVAS_{priv}$, Media ID || Binding Nonce || PV Content Certificate ID || PVT_{data})

  Where:

  - AACS_Sign is as defined in the AACS *Introduction and Common Cryptographic Elements* book.
  - $PVAS_{priv}$, is the private key associated with the PVAS public key found in the PVT.
  - Media ID is the AACS Recordable Media identifier as defined in the AACS *Recordable Video Book*.
  - Binding Nonce is the AACS Binding Nonce value defined in the AACS *Recordable Video Book* and associated with the Prepared Video Token file.
  - PV Content Certificate ID is a 6 byte PV Content Certificate identifier, the concatenation of the 2-byte Applicant ID and the 4-byte Content Sequence Number, as defined in Section 2.4.
  - PVT_{data} includes bytes over the entire data up to but not including the Prepared Video Token Signature Data.

2.8.1 Obtaining the Data for the PVT

The PVAS needs both the Binding Nonce and the Media ID from the destination media to correctly sign the PVT. That data is not secret, and how it is communicated from the client to the PVAS is a design decision of the PVAS. Note that recordable Licensed Drives associated with the Download Client are required to implement the Host/Drive Authentication Protocol (see options 2 and 3 below), as defined in Chapter 4 of the AACS *Introduction and Common Cryptographic Elements* book, and therefore obtaining this data requires a Host Certificate and its associated private key.

The EST/MOD system designer has three choices:

1. The client is designed so that it is not required to implement Host/Drive Authentication.
2. The system may be designed with an AACS Host Certificate and private key in the Download Client, as long as the client meets the robustness requirements in the AACS license.
3. The PVAS itself may have the AACS Host Certificate and private key and use a remote drive authentication protocol to obtain this information.

   A "remote drive authentication protocol" means a protocol similar or identical to the protocol defined for remote reading of the PMSN in Section 5.5.1 of the AACS *Prerecorded Video Book*. Such a PVAS shall follow the restrictions defined in Section 5.7 of the same book. As long as these restrictions are met, the PVAS may design its own protocol for this remote authentication, or it may use the "performReadDrive" Web service message defined for that purpose in that book, or it may use the host private key in the Download Client, at its option.

2.8.2 Storing the PVT on the media

The Download Client stores the PVT in a file on the destination media. Additional details about file names and locations are specified in the format specific books of this specification. The Binding Nonce shall be committed to the destination media before performing the Managed Copy or EST/MOD transaction to ensure that the Binding Nonce is not lost or corrupted if a power failure or other memory corruption occurs during the transaction.

2.9 Server Interaction for EST / MOD

The EST / MOD model for recording Prepared Video Content differs from the Managed Copy scenario described in Chapter 5 of this document. With Managed Copy, the source AACS Content is already known and takes the form of a Prerecorded Video disc or another Prepared Video disc which the recorder uses to make the copy. This is not the case for EST / MOD, This model is characterized by AACS Content which may be available from a download server or other source, which will generally have many different eligible pieces of AACS Content.

Although this section refers to a "download server" and "download client", these are notional concepts, not necessarily standalone components. For example, an MOD kiosk might contain elements of both a server and a client.

The download delivery and purchase of Prepared Video has four distinct phases:

1. The discovery phase. The user browses amongst the various pieces of AACS Content available on the server to select the AACS Content and the particular offer associated with the AACS Content.
2. The authorization phase. The user is authorized to receive the AACS Content most likely via, but not limited to, a financial transaction.
3. The content delivery phase. The actual AACS Content is delivered to the client and burned on recordable media.
4. The Prepared Video Token delivery. A PVT is delivered to the client and is also recorded on the media. A valid PVT is necessary before the AACS Content can be played.

Note that phases 2 and 3 can occur in either order. Because the AACS Content is not playable until the PVT is delivered, the actual AACS Content can be delivered, burned, and verified on the media before the user has been authorized to receive it.

The next section describes an informative API for discovering content and associated offers available via a download server. The Get PV Content Offers API (Sections 2.9.1 and 2.9.2) supports an efficient and flexible means of discovering PV source content through a mechanism of repetitive calls which allow navigation of hierarchically categorized content offered for Prepared Video recording from the download server. Offers associated with content are also acquired using that API.

AACS also defines an informative API for phase 4. The first three phases are generally defined by the particular online store the user is visiting, and the store will naturally choose mechanisms that are most compatible with its current mode of operation, so these mechanisms are system-specific. The informative phase 4 API is the Request PVT message (see Sections 2.9.4 and 2.9.5). It is used to obtain a PVT associated with a destination media for the Prepared Video operation. If a financial transaction is necessary, it shallbe performed against the particular offer selected prior to use of the Request PVT API.

2.9.1 Get PV Content Offers

This section is informative, describing one possible API for the content discovery phase.

The Get PV Content Offers message is a Web service API which allows the client a flexible mechanism to find PV Content of interest. Several pieces of meta-data can be specified to search, including the content ID, title, as well as a pvMetaData field which can be customized between PV Clients and PV Servers. The details of the Web service API are given by the contentOffers schema in Appendix A.

The Get PV Content Offers Message request contains the following information:

languageCode	This is an ISO 639 compliant language code value which allows the PV Client to communicate its locale language information to the PV Server. The PV Server also uses this information to prepare the appropriate offers for the response
pvSessionID	A session ID used to maintain continuity across multiple invocations of this API. Upon first invocation, it shall be set to "0".
content ID	An optional content ID. If this is provided, then it identifies the exact AACS

	Content desired. If a match is found this will result in a response containing any available offers applicable to that AACS Content.
title	This optional field allows specifying the title of the desired AACS Content. If the title does not match one known to the server, the server may use heuristics to obtain reasonable matches.
pvMetaData	An optional opaque structure which contains meta-data to assist in isolating the desired PV Content in the response. It may also be used to successively narrow down the response through multiple invocations of this API.
contentNodeURL	Download Servers can choose to organize content into categories to facilitate searches. This takes the form of a classification hierarchy. Each node of the hierarchy is represented by a pvContentNode. This optional contentNodeURL parameter allows specifying one or more of the referencing URLs (typically acquired from a prior invocation of this API), each of which identifies to the download server groups for which the client is requesting lower level information. That information will either be another node or nodes in the hierarchy, or the call will result in identifying one or more pieces PV Content together with applicable offers for each (see section 2.9.2 below).

If the combination of search criteria provided result in anything other than the identification of an actual piece of PV Content (i.e., a title), then offers are not returned. Offers are only returned which correspond to an actual title. The request can be re-issued with narrower criteria until the desired title and its associated offers are returned.

2.9.2 Get PV Content Offers Response

This is an informative section.

The Get PV Content Offers message response is returned by the download server when it received the Get PV Content Offers Message request. Refer to Appendix A for the schema which describes this message and its associated data structures.

The Get PV Content Offers Message response contains the following information:

languageCode	This is an ISO 639 compliant language code value which tells the client which language the PV Server has used to present the offers.
pvContentNode	If the criteria provided on the request resulted in any matches for content, then an array of one or more pvContentNodes will be returned. Included with each pvContentNode:

contentNodeURL	URL of this Content node
parentNodeURL	URL of the parent of this Content Node, if one exists.
title	This is a title for the grouping, or represents the actual title if this URL represents a single piece of PV Content.
abstract	This is an abstract describing the grouping, or the abstract for the title if this URL represents a single piece of PV Content.
pvOffer	This is one or more PV offer structures and is only included if the URL represents a single piece of PV Content.

oui	Unique ID associated with this offer
description	Description of the offer

image	Optional Image associated with the offer
financialApplicationURI	Optional URI where a client application for performing the financial transaction can be found.
financialHTMLURL	URL where the financial transaction can be transacted.
price	Cost of the offer.

2.9.3 Purchase Phase

These sub-sections discuss considerations for actually purchasing Prepared Video Content. Behavior and requirements here are analogous to that described for Managed Copy in Chapter 5 of the AACS *Pre-recorded Video Book.*

The fundamental concept is that, during the purchase phase, the end user performs the financial transaction in order to purchase a particular piece of AACS Content to be placed on a particular destination disc. The destination disc is, of course, defined by the Media ID and the Binding Nonce. Once the Media ID and the Binding Nonce has been associated with a particular piece of AACS Content as part of the purchase phase, then a connection failure in the rest of the protocol can be simply retried: the PVT can be sent as many times as necessary until the client has received it successfully. Additional PVT transmissions do not create additional copies, because the PVT is only usable on one piece of media.

This paragraph is informative, however, if a system implements all APIs described in Section 2.9, this behavior is mandatory. AACS never specifies the details of the financial transaction. Instead, each online store is expected to use whatever financial system is most convenient for it. AACS does require, however, that the online store provide secure continuity between the financial transaction and the upload of the destination Media ID and Binding Nonce. In other words, it shall not be possible for a man-in-the-middle to substitute his own binding information during another user's purchase. In the case that the user is sending his credit card information under HTTPS, for example, this requirement can be achieved by having the binding information being sent up in the same HTTPS session.

Note that the Media ID and Binding Nonce are obtained on a PC client only after performing drive authentication. A PC client is not required to have a Host Certificate or any AACS secrets to create a Prepared Video disc. If the server wishes to support such a secretless client, it may implement the Perform Read Drive protocol, as defined in section 5.5.1 of the AACS *Pre-recorded Video Book.* With this protocol, the client acts as a proxy while the server actually performs the drive authentication and executes authenticated commands. In this case, the authenticated commands would be reading the Media ID and the Binding Nonce. The client needs to observe the Media ID and Binding Nonce responses from the Drive and remember them for the purchase phase and the Request PVT message below.

2.9.4 Get Prepared Video Token Message

This section is informative, describing how the PVT is requested by and delivered to the PV Client.

Note that there are no security concerns with delivering the same PVT over and over again, because the PVT is tied to a single piece of physical media. The PV Client can safely retry this message in the case of errors. Likewise, the Prepared Video Authorization Server shall maintain a cache of recently delivered PVTs so that they can be resent, if necessary, without requiring a new financial transaction.

Once the appropriate offer has been selected and the financial transaction has been successfully completed, the PV Client sends a getPreparedVideoToken message to the PVAS. The getPreparedVideoToken Web service message is described by the schema in Appendix A. It is executed synchronously and the response is returned as described in Section 2.9.5 below. Arguments for this message are:

contentID	The Content ID of the particular piece of AACS Content.
oui	Offer Unit. This is an optional parameter. It is a string containing the ID of the particular offer that was selected as a part of the transaction. Its value is system specific. (In the case the system is using the Get PV Content message above, the offer ID is in the response from that message.) Note that the Content ID, Media ID, and Binding Nonce uniquely identify a transaction, so in some systems this parameter may be omitted.
pvBindingData	Information sent to the PVAS which is specific to this binding, in particular, the Media ID and the Binding Nonce. See Table 2-3 for the format of this data

Table 2-3 - Data Format of PV Binding Data

Bit / Byte	7	6	5	4	3	2	1	0
0 : 15	Media ID							
16 … 31	Binding Nonce							

2.9.5 Get Prepared Video Token Message Response Creation

When the Server receives a Get Prepared Video Token Message request, the contents of the message are compared to the information received in the initial Get PV Content Offers message and any subsequent transactions that occurred. If all the information is correct and the conditions (including the financial transaction) have been satisfactorily met, the PV Server shall compose a "Get Prepared Video Token Message Response" to be sent to the PV Client. This response message is a Web service which is described in Appendix A, It contains the following information:

status	Indicates whether or not a PVT has been granted. This status field can be used to facilitate the Application Layer's ability to determine the authorization status. A value of zero indicates success.
statusMessage	This is an optional text field suitable for end users, which may contain a reason for failure when the status code returned is non-zero (failure).
PVTInfo	This field contains the PVT and optionally other files which the PVAS may want to update such as the MKB. Its format is identical to that sent when a Managed Copy is made into Prepared Video format; see section 5.5.9.

Chapter 3
Content Encryption and Decryption

3 Introduction

The content encryption and decryption mechanisms for Prepared Video Content are very similar to those for Pre-recorded Video Content. As such, in this chapter, we will refer to the AACS *Pre-recorded Video Book*, and only elaborate on the key differences between the Pre-recorded and the Prepared Content implementations.

Note that for Prepared Video, they are two generic models for how the AACS Content arrives on the optical disc:

1. Electronic Sell Through/Manufacturing On Demand (EST/MOD)
2. Managed Copy

In EST/MOD, the AACS Content is transmitted from a server (download and burn) before arriving on the recordable optical media. In Managed Copy, the AACS Content is copied directly from either a Pre-recorded optical disc or a Prepared Video disc to the recordable optical media.

In EST/MOD and Managed Copy, the Prepared Video Authorization Server (PVAS) provides a Prepared Video Token, making the Prepared Video format functionally equivalent to the Pre-recorded format.

The following figures provide examples of these two models. Contrast these figures to Figure 3-1 in the AACS *Pre-recorded Video Book*.

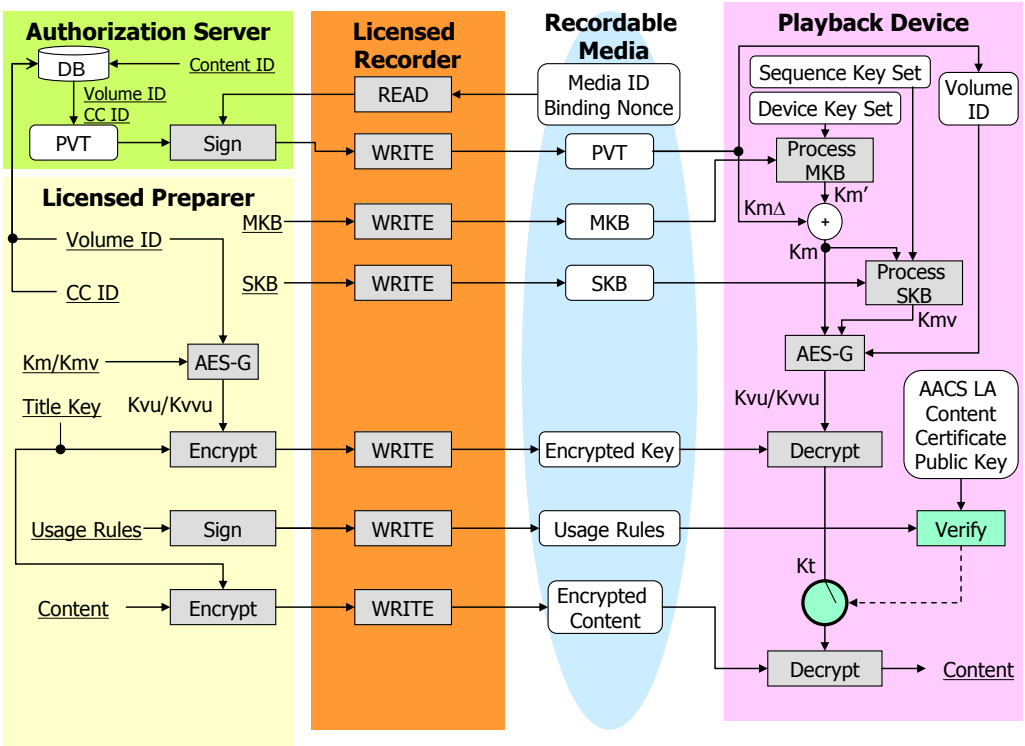

Figure 3-1 - Prepared Video Encryption and Decryption Overview, EST/MOD

The principle differences to be noted between Figure 3-1 in this book and the AACS *Pre-recorded Video Book* are:

- A recorder is between the Licensed Preparer and the recordable media.
- KCD is not included, as this construct is specific to the Pre-recorded Video format. In other words, Type 3 MKBs are always used instead of Type 4 MKBs for recordable media.
- Volume ID and PV Content Certificate ID are provided by the Licensed Preparer to the Authorization Server, where they are packaged in the Prepared Video Token, itself cryptographically signed and bound to the target recordable media.
- The Media Key Delta is needed by the PVAS to ensure all players are able to unlock the Title Key File using the MKB recorded onto the PV disc even if the Title Key File was encrypted using a Media Key from a different MKB. Licensed Preparers decide how to provide this value to the PVAS. Options are:
    - Pre-calculate the Media Key Delta for each MKB which may be burned onto a disc, and provide this to the PVAS.
    - Require that the PVAS have its own set of Device Keys so that it is able to process the two MKBs (i.e., the MKB on the prerecorded disc, and the MKB on the recordable disc) to obtain the associated Media Keys, and then XOR them together to derive the Media Key Delta.
- The playback device extracts the Volume ID from the PVT.

In Figure 3-2 provides an informative example of the same process as it applies to a Managed Copy to the AACS Prepared Video format. Note that the authorization for making a Managed Copy is not shown in this diagram (see Chapter 5 of this document).

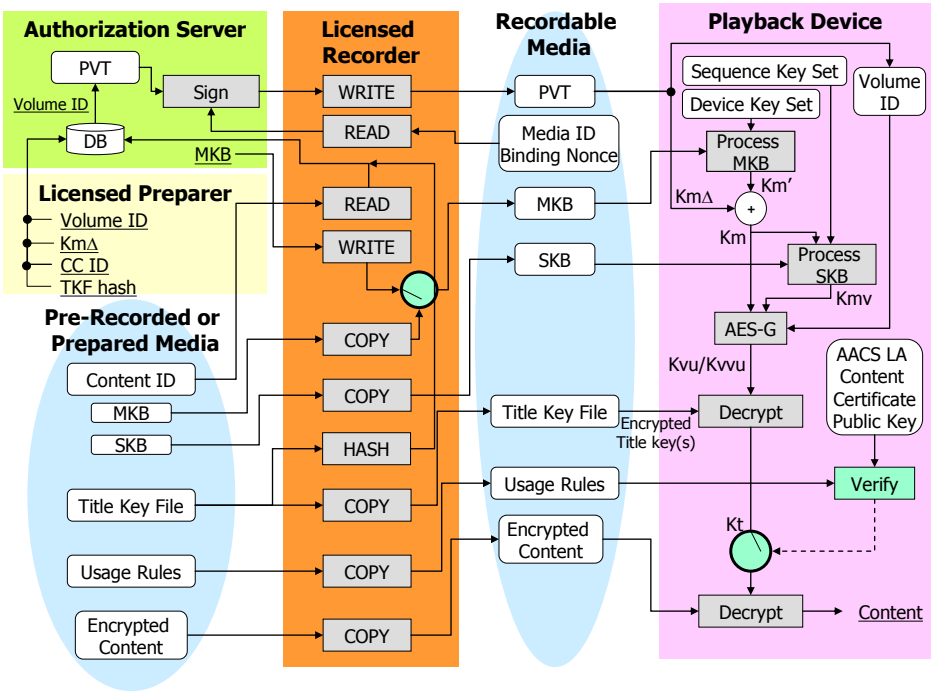

Figure 3-2 – Prepared Video Encryption and Decryption Overview, Managed Copy

Some key things to note about Figure 3-2:

- Managed Copy can take place from either a Pre-recorded disc or a Prepared Video disc.
- The Volume ID always comes from the Authorization Server, even though the source of the Managed Copy is either a Pre-recorded disc, which contains a Volume ID, or a Prepared Video disc, which contains a Prepared Video Token containing a Volume ID.
- Volume ID is a look up in the PVAS keyed off of the Content ID and a SHA-1 Hash of the Title Key File (TKF Hash) stored on the source Pre-recorded or Prepared Video disc. The TKF Hash is used to distinguish the case in Pre-recorded Content where a single Content ID was mastered more than once and has more than one Volume ID associated with it.
- For each unique MKB used in the original AACS Content, at least one Media Key Delta and its associated Type 3 MKB shall be stored in the PVAS.
- Since the Prepared Video format, like the Pre-recorded Video format, includes a Content Hash Table – the transfer to the Prepared Video format on the recordable media shall be a bit-for-bit match to the source as far as the Content Hash Table is concerned. Additional details can be found in Chapter 5.

3.1 Content Encryption (general)

Refer to Section 3.1 of the AACS *Pre-recorded Video Book*.

Note that for Prepared Video, the Volume ID created by the Licensed Preparer shall be provided to the PVAS, where it is maintained in association with the Content ID and the TKF Hash, as defined in Chapter 5 of the AACS *Introduction and Common Cryptographic Elements* book.

3.2 Content Decryption (general)

Refer to Section 3.2 of the AACS *Pre-recorded Video Book*, but note that for Prepared Video there is the additional check for an applicable Recordable Media Revocation Record in the CRL and if one is found, the Licensed Player shall not playback the AACS Content. This check happens after the check for an applicable Revocation Record for Content Certificate ID.

Note: the Volume ID used in decryption of Prepared Video is extracted from the Prepared Video Token. See Section 2.8 of this document.

Note: the Media ID is used to enable playback of AACS Prepared Video Content, it shall be discarded upon removal of the instance of media from which it was retrieved.

3.3 Calculating the Volume Unique Keys

Refer to Section 3.3 of the AACS *Pre-recorded Video Book*.

3.4 AACS Encryption on Prepared Video Content for Recordable Media

Refer to Section 3.4 of the AACS *Pre-recorded Video Book*.

3.5 AACS Decryption on Prepared Video Content for Recordable Media

Refer to Section 3.5 of the AACS *Pre-recorded Video Book*.

The PV Content Certificate (PVCC) contains the public keys of all PVAS allowed to authorize Prepared Video for that AACS Content. The PVCC is digitally signed by AACS LA. The PVT contains the public key of the PVAS, which shall correspond to one in the PVCC. The concatenation of the PVCC ID, the target recordable disc Media ID, and the PVT is digitally signed by the PVAS. This is represented in Figure 3-3.

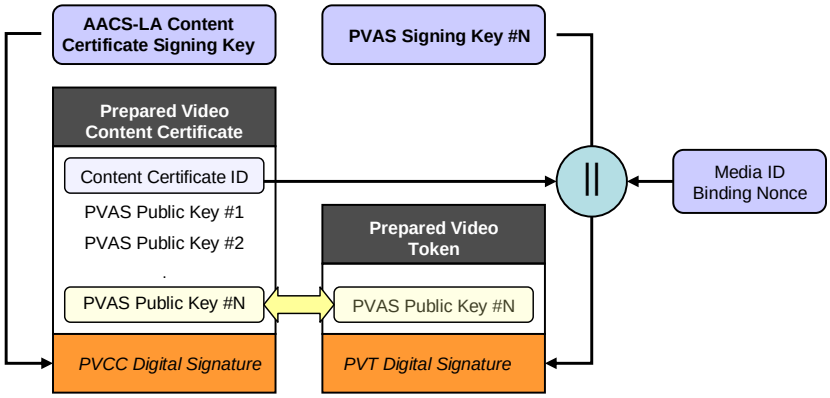

Figure 3-3 - Prepared Video Format Digital Signature Hierarchy

Prior to providing access to Certified Content, Licensed Products shall read and validate the Prepared Video Token following the steps below:

1. Verify that the public key of the Prepared Video Authorizing Server included in the Prepared Video Token is also present in the PV Content Certificate.
2. Verify that the Prepared Video Token is valid, using:

   AACS_Verify($PVAS_{pub}$, PVT_{sig}, Media ID || Binding Nonce || PV Content Certificate ID || PVT_{data})

   Where:

   - AACS_Verify is as defined in the *Introduction and Common Cryptographic Elements* book
   - PVT_{sig}, is the Prepared Video Token Signature Data, as described in Section 2.8
   - $PVAS_{pub}$ is the public key of the Prepared Video Authorizing Server retrieved in step 1 above
   - Media ID is the media identifier present on the AACS Recordable Media
   - Binding Nonce
   - PV Content Certificate ID is the content identifier retrieved from the PV Content Certificate, the concatenation of the 2-byte Applicant ID and the 4-byte Content Sequence Number, as defined in Section 2.4
   - PVT_{data} includes bytes over the entire data up to but not including the Prepared Video Token Signature Data

Licensed Players shall use a $PVAS_{pub}$ value retrieved from the PV Content Certificate.

If the PVT is not present, or if the PVT verification fails, the Licensed Player shall not playback the AACS Content.

As noted in Section 3.2 above a Licensed Player will check for an applicable Recordable Media Revocation Record in the CRL and if found, shall not playback the AACS Content.

3.6 Secure Move of Prepared Video using the Binding Nonce

Because the Binding Nonce is used in the computation of the signature on the PVT, Managed Copy content stored in the Prepared Video format can be securely "moved" to another destination media. The procedures for updating the source medium during a secure move of Prepared Video Content are as follows:

1. Verify that the Prepared Video Token is valid, using:

   AACS_Verify($PVAS_{pub}$, PVT_{sig}, Media ID || Binding Nonce || PV Content Certificate ID || PVT_{data})
2. Verify that the Move Allowed Flag in the PVT is set to a 1_2.

   If the Move Allowed Flag in the PVT is set to a 0_2 (meaning that Move is "not allowed"), then the recorder shall not continue with this move procedure.
3. Generate a new Binding Nonce and a new PVT which contains all 0's and commits the new Binding Nonce and new PVT to the source media.
4. Read the new Binding Nonce. The Licensed Recorder shall read the new Binding Nonce that is now associated with the new PVT to ensure that the Binding Nonce value has been updated on the physical media.
5. Bind the AACS Content to the destination. The recorder binds the AACS Content to the destination using a binding method defined by the destination technology.

The 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.

The procedure defined in this section of the specification is not allowed for media (such as write-once media) where an existing Binding Nonce cannot be destroyed or overwritten.

Informative Note: As an optimization step, AACS Content that has been securely moved from a Prepared Video formatted disc is capable of being "re-enabled" on that same disc by obtaining a new PVT from a PVAS. The process and rules for acquiring the new PVT are not defined in this specification and will instead be defined in the rules of the technology which is the source for this type of a "move back" action.

This page is intentionally left blank.

Chapter 4
Sequence Key Block

4 Introduction

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* for details.

This page is intentionally left blank.

Chapter 5
Managed Copy and Prepared Video Content

5 Introduction

The Managed Copy protocol is defined in Chapter 5 of the AACS *Pre-recorded Video Book.* This chapter contains additional information that defines how the Prepared Video format can be used as a source and as a destination for Managed Copy. Because properly formatted Prepared Video Content requires the PV Token, Managed Copies made in PV format inherently use Server-side Binding, as defined in Chapter 5 of the AACS *Pre-recorded Video Book* .

The two scenarios where Prepared Video is used in the Managed Copy process are when Prepared Video is:

- a destination for Managed Copy from an AACS Pre-recorded Video disc – a Managed Copy Output Technology (MCOT); that is, an AACS/ROM or AACS/PV disc, to an AACS/PV disc, or
- a source for Managed Copy – that is, AACS/PV to an approved MCOT.

5.1 Managed Copy Machine Initiation

Refer to Section 5.1 of the AACS *Pre-recorded Video Book* for background.

Note that Prepared Video Content may be both the source and the destination in a single Managed Copy transaction.

5.2 Connection Protocol

Refer to Section 5.2 of the AACS *Pre-recorded Video Book*.

5.3 Managed Copy Account Transactions

Refer to Section 5.3 of the AACS *Pre-recorded Video Book*.

5.4 MCS Certificate

Refer to Section 5.4 of the AACS *Pre-recorded Video Book*.

5.5 Managed Copy Messages

Refer to Section 5.5 of the AACS *Pre-recorded Video Book*.

5.5.1 Perform Read Drive

Refer to Section 5.5.1 of the AACS *Pre-recorded Video Book*. If the source is an AACS Prerecorded Video disc, then secretless clients use the Perform Read Drive protocol to obtain the PMSN. If the source is an AACS Prepared Video disc, then the client simply reads the PVSN as described in the next section.

5.5.2 Peform Read Drive Response

Refer to Section 5.5.2 of the AACS *Pre-recorded Video Book*.

5.5.3 Request Offer

When the source disc for a Managed Copy is an AACS Prepared Video disc, the Managed Copy Machine shall extract the value of the PVSN in the Prepared Video Token and include this as the PMSN in the

Request Offer message to the Managed Copy Machine (see Section 5.5.3 of the AACS *Pre-recorded Video Book*).

5.5.4 Offer Response Creation

Refer to Section 5.5.4 of the AACS *Pre-recorded Video Book*.

5.5.5 Offer Response Verification and Interpretation

Refer to Section 5.5.5 of the AACS *Pre-recorded Video Book*.

5.5.6 Check Serial Number

Refer to Section 5.5.6 of the AACS *Pre-recorded Video Book*.

5.5.7 Check Serial Number Response

Refer to Section 5.5.7 of the AACS *Pre-recorded Video Book*.

5.5.8 Request Permission

Refer to Section 5.5.8 of the AACS *Pre-recorded Video Book*.

When the destination MCOT is AACS Prepared Video, the MCM_MCOTInfo field of the Request Permission message is required, then the Managed Copy Machine shall use it to send the Media ID and Binding Nonce of the target recordable disc, and a hash of the Title Key File from the source disc, to the Managed Copy Server. The format for the MCM_MCOTInfo field is given in Table 5-1.

Table 5-1 - Data Format of MCOTParams and/or MCM_MCOTInfo for PV MCOT

Bit / Byte	7	6	5	4	3	2	1	0
0 : 15	Media ID							
16 … 31	Binding Nonce							
32 … 51	SHA-1 Hash of the Title Key File							

The name and location of the Title Key File is format-specific, and is described in the relevant application books of this specification.

The MCS is acting as a PVAS in the case that the destination is Prepared Video. The MCM may observe the Media ID and Binding Nonce from the "performReadDrive" remote authentication protocol (described in Section 5.5.1 of the AACS *Pre-recorded Video Book)*, or it may read them itself.

5.5.9 Request Permission Response Creation

In addition to the steps described in Section 5.5.9 of the AACS *Pre-recorded Video Book*, when the destination MCOT is AACS Prepared Video, the Managed Copy Server performs the role of a PVAS.

In general, because Prerecorded Video Content and Prepared Video Content are so similar, the Managed Copy process into Prepared Video format is usually a bit-for-bit copy. Any exceptions to this rule are called out in the format-specific books of this specification.

In addition, in the case the source of the Managed Copy is Pre-recorded Video Content, the MCM shall copy the recordable MKB, not the pre-recorded MKB, to the destination copy. This is because the pre-recorded MKB might have been designed with Key Conversion Data (KCD), which is not available on AACS Recordable Media. The MCS/PVAS shall set the Media Key Delta field in the PVT to make sure the copy is playable.

The MCS/PVAS generates a PVT file for the destination. In addition, it may send a new MKB file, and it may send other files, such as a PV Content Certificate, as required in different format-specific cases. All these files are given in the MCS_MCOTInfo field of the "Request Permission" message response. Table 5-2 shows the format for each file.

Table 5-2 – MCS_MCOTInfo File Format

Bit / **Byte**	**7**	6	5	4	3	2	1	0
0 .. 3	Length (N)							
4 … M+3	File Path/Name (M characters)							
M+4	File Path/Name Delimiter (00_{16})							
M+5 … N+3	File Data							

The fields are as follows:

- Length. The total length of the entry (excluding this field), including the file path and name, the path/name delimiter, and the file data. Since there may be multiple files in the MCS_MCOTInfo, the end of the list is denoted with a 0 length.
- File Name/Path. This is the ASCII name and logical location of the file. The directory separator is the backslash ('\'). If the file exists it shall be overwritten. Any missing directories shall be created. If the file path or name contains invalid characters, the action is MCM-specific.
- File Path/Name Delimiter. The end of the file path is denoted by a null character.
- File Data. The file data follows. The length of the file is Length minus the length of the file name/path plus the delimiter. If the file does not fit on the destination media, the action is MCM-specific.

The MCM simply needs to copy the file data to the named destination in the destination media. The name and path for this file is format specific.

In general, an MCM shall not begin copying AACS Content from the source to the destination prior to receiving a valid response to the "Request Permission" message. Prepared Video format output is an exception to this rule. The MCM may begin a bit-for-bit copy of the source AACS Content into a buffer (such as a hard disc) prior to receiving permission. This prevents the awkwardness of forcing the user to swap discs multiple times if the MCM only has a single Encryption Drive. Of course, the buffer copy is not playable by a Licensed Player until it has been copied to valid destination media and given a correct PVT by the MCS, which happens only after a valid permission has been received.

5.6 Making a Managed Copy

Refer to Section 5.6 of the AACS *Pre-recorded Video Book*.

5.7 Informative Section: Components of a Managed Copy Architecture

Refer to Section 5.7 of the AACS *Pre-recorded Video Book*.

A Appendix: Prepared Video Schema

The follow schema is informative. It defines the data structures and messages necessary to implement the optional messages described in section 2.9.

```
<?xml version="1.0" encoding="UTF-8"?>
<schema xmlns="http://www.w3.org/2001/XMLSchema"
      targetNamespace="http://www.aacsla.com/2008/01/PreparedVideo"
      xmlns:xs="http://www.w3.org/2001/XMLSchema"
      xmlns:pv="http://www.aacsla.com/2008/01/PreparedVideo"
    elementFormDefault="qualified" >

      <xs:element name="pvtData" >
            <xs:complexType>
                  <xs:sequence>
                        <xs:element ref="pv:status"
                              minOccurs="1" maxOccurs="1" />
                        <xs:element ref="pv:statusMessage"
                              minOccurs="0" maxOccurs="1" />
                        <xs:element ref="pv:pvtInfo" minOccurs="1"
                              maxOccurs="1" />
                  </xs:sequence>
              </xs:complexType>
    </xs:element>

    <xs:element name="pvContentNode" >
      <xs:complexType>
            <xs:sequence>
                  <xs:element ref="pv:contentNodeURL" minOccurs="1"
                        maxOccurs="1" />
                  <xs:element ref="pv:parentNodeURL" minOccurs="0"
                        maxOccurs="1" />
                  <xs:element ref="pv:title" minOccurs="0"
                        maxOccurs="1" />
                  <xs:element ref="pv:abstract" minOccurs="0"
                        maxOccurs="1" />
                  <xs:element ref="pv:pvOffer" minOccurs="0" />
            </xs:sequence>
      </xs:complexType>
    </xs:element>

    <xs:element name="pvOffer">
      <xs:complexType>
            <xs:sequence>
                  <xs:element ref="pv:oui" minOccurs="1" maxOccurs="1"
/>
                  <xs:element ref="pv:description" minOccurs="1"
                        maxOccurs="1" />
                  <xs:element ref="pv:image" minOccurs="0"
                        maxOccurs="1" />
                <xs:element ref="pv:financialApplicationURI"
                      minOccurs="1" maxOccurs="1" />
                <xs:element ref="pv:financialHTMLURL" minOccurs="1"
                    maxOccurs="1" />
```

```
                <xs:element ref="pv:price" minOccurs="0" maxOccurs="1"
/>
            </xs:sequence>
        </xs:complexType>
    </xs:element>

    <xs:element name="title" final="restriction">
      <xs:simpleType>
            <xs:restriction base="xs:string">
                  <xs:maxLength value="1024" />
            </xs:restriction>
        </xs:simpleType>
    </xs:element>

    <xs:element name="description" final="restriction">
      <xs:simpleType>
            <xs:restriction base="xs:string">
               <xs:maxLength value="65536" />
            </xs:restriction>
        </xs:simpleType>
    </xs:element>

    <xs:element name="abstract" final="restriction">
         <xs:simpleType>
         <xs:restriction base="xs:string">
               <xs:maxLength value="4096" />
          </xs:restriction>
       </xs:simpleType>
    </xs:element>

    <xs:element name="image">
        <xs:complexType>
        <xs:sequence>
              <xs:element ref="pv:imageURL" minOccurs="1" maxOccurs="1"
/>
              <xs:element ref="pv:title" minOccurs="1" maxOccurs="1" />
          </xs:sequence>
      </xs:complexType>
    </xs:element>

    <xs:element name="getPreparedVideoTokenMessageType" >
      <xs:complexType>
            <xs:sequence>
                  <xs:element ref="pv:contentID" minOccurs="1"
                        maxOccurs="1" />
                  <xs:element ref="pv:oui" minOccurs="1" maxOccurs="1"
/>
                  <xs:element ref="pv:pvBindingData" minOccurs="1"
                        maxOccurs="1" />
            </xs:sequence>
      </xs:complexType>
    </xs:element>

    <xs:element name="getPreparedVideoTokenMessageResponseType" >
      <xs:complexType>
            <xs:sequence>
```

```
                <xs:element ref="pv:status" minOccurs="1"
                      maxOccurs="1" />
                <xs:element ref="pv:pvtData" minOccurs="1"
                      maxOccurs="1" />
          </xs:sequence>
    </xs:complexType>
  </xs:element>

  <xs:element name="getPVTContentOffersMessageType" >
    <xs:complexType>
          <xs:sequence>
                <xs:element ref="pv:languageCode" minOccurs="1"
                      maxOccurs="1" />
                <xs:element ref="pv:pvSessionID" minOccurs="1"
                      maxOccurs="1" />
                <xs:element ref="pv:contentID" minOccurs="0"
                      maxOccurs="1" />
                <xs:element ref="pv:title" minOccurs="0"
                      maxOccurs="1" />
                <xs:element ref="pv:pvMetaData" minOccurs="0"
                      maxOccurs="1" />
                <xs:element ref="pv:contentNodeURL" minOccurs="0"
                      maxOccurs="1" />
          </xs:sequence>
    </xs:complexType>
  </xs:element>

  <xs:element name="getPVTContentOffersMessageResponseType" >
    <xs:complexType>
          <xs:sequence>
                <xs:element ref="pv:languageCode" minOccurs="1"
                      maxOccurs="1" />
                <xs:element ref="pv:pvContentNode" minOccurs="0" />
          </xs:sequence>
    </xs:complexType>
  </xs:element>

  <xs:element name="status" type="xs:nonNegativeInteger" />
  <xs:element name="statusMessage" type="xs:string" />
  <xs:element name="pvtInfo" type="xs:base64Binary" />
  <xs:element name="languageCode" type="xs:string" />
  <xs:element name="contentNodeURL" type="xs:anyURI" />
  <xs:element name="imageURL" type="xs:anyURI" />
  <xs:element name="oui" type="xs:string" />
  <xs:element name="parentNodeURL" type="xs:anyURI" />
  <xs:element name="price" type="xs:string" />
  <xs:element name="financialApplicationURI" type="xs:anyURI" />
  <xs:element name="financialHTMLURL" type="xs:anyURI" />
  <xs:element name="contentID" type="xs:string" />
  <xs:element name="pvBindingData" type="xs:base64Binary" />
  <xs:element name="pvSessionID" type="xs:string" />
  <xs:element name="pvMetaData" type="xs:base64Binary" />

</schema>
```