

Advanced Access Content System (AACCS)

Signed CSS 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.

Copyright © 2007-2012 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 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

| | |
|--|----------|
| Notice | iii |
| Intellectual Property..... | iii |
| Contact Information..... | iii |
| CHAPTER 1 INTRODUCTION | 1 |
| 1.1 Purpose and Scope | 1 |
| 1.2 Overview..... | 1 |
| 1.3 Organization of this Document..... | 1 |
| 1.4 References..... | 1 |
| 1.5 Document History | 1 |
| 1.6 Notation | 2 |
| 1.7 Abbreviations and Acronyms | 2 |
| CHAPTER 2 DETAILS FOR CONTENT VALIDATION | 3 |
| 2. INTRODUCTION..... | 3 |
| 2.1 Content Certificate for Signed CSS..... | 3 |
| 2.2 Content Hash Table | 5 |
| 2.3 Hash Unit..... | 6 |
| 2.4 Creating the CSS Content AACS Certificate | 6 |
| 2.5 Verifying the CSS Content AACS Certificate and Screening Obligation | 7 |

This page is intentionally left blank.

List of Figures

Figure 2-1 – Content Signing Process for CSS..... 7

This page is intentionally left blank.

List of Tables

| | |
|---|---|
| Table 2-1 – CSS Content AACS Certificate for DVD-Video Disc | 3 |
| Table 2-2 – Format of Content Hash Table | 5 |

This page is intentionally left blank.

Chapter 1

Introduction

1.1 Purpose and Scope

The Advanced Access Content System (AACCS) specification defines an advanced, robust and renewable method for protecting audiovisual entertainment content, including high-definition 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 *Pre-recorded Video Book* defines common details for using the system to protect audiovisual content distributed on pre-recorded (read-only) storage media. This document, the *Signed CSS* book, defines how to use AACCS to validate the integrity of audiovisual content protected by CSS Technology provided by DVD CCA.

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

DVD-Video content may be protected by CSS Technology. Further, this document provides the data structure and procedure to validate the integrity of the content protected by CSS Technology. Note that encryption and decryption of CSS Technology are used to protect the content, and AACCS Technology is not used for this purpose.

1.3 Organization of this Document

This document is organized as follows:

- Chapter 1 provides an introduction.
- Chapter 2 describes DVD-Video specific procedures related to the content validation.

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.

AACCS LA, *Introduction and Common Cryptographic Elements*

AACCS LA, *Pre-recorded Video Book*

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

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

DVD Forum, *DVD Specifications for Read-Only Disc, Part 3 Video Specifications*

DVD CCA, *CSS Procedural Specifications*

DVD CCA, *CSS Technical Specifications*

1.5 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 superseded version 0.95 dated May 21, 2009. It contained minor editorial clarifications.

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 Abbreviations and Acronyms

| | |
|------|-------------------------|
| CHT | Content Hash Table |
| CSS | Content Scramble System |
| HUN | Hash Unit Number |
| NHV | Number of Hash Values |
| VOB | Video Object |
| VOBS | Video Object Set |
| VOBU | Video Object Unit |

Chapter 2

Details for Content Validation

2. Introduction

Content validation requires the Content Certificate that is specified in Chapter 2 of the *Pre-recorded Video Book* of this specification. This chapter describes additional details of content validation that are specific to DVD-Video format.

As described in the *Pre-recorded Video Book*, every hash units of the AV contents in the DVD-Video format on the disc is hashed, and this hashed value is included in the Content Hash Table. Every part of the Content Hash Table, that corresponds to an AV content file, is then hashed, and this hashed value is included in the unsigned Content Certificate as a Content Hash Table Digest. This unsigned Content Certificate is finally signed by the AACS LA, and this becomes the Content Certificate.

A disc may contain both encrypted contents and unencrypted contents. The Content Certificate, however, shall cover all the AV contents in the DVD-Video format on the disc, whether they are encrypted or not.

2.1 Content Certificate for Signed CSS

Content protected using the CSS technology and distributed on Pre-recorded or CSS protected downloaded DVD Discs can have an AACS signature. If it does, the AACS Licensed Player shall check the signature. If it verifies, it shall treat the content as if it came from a trusted source; otherwise it shall not play the content. The AACS signature is a content certificate called the CSS Content AACS Certificate.

The CSS Content AACS Certificate is stored in the “\AACS” directory of the DVD format in a file named “CSS_CONTENT_CERT.AACS”. The CSS Content AACS Certificate file has the format defined in Table 2-1.

Table 2-1 – CSS Content AACS Certificate for DVD-Video Disc

| Byte | Bit | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |
|------|-----|------------------------------------|---|---|---|---|---|---|---|
| 0 | | Certificate Type: 80 ₁₆ | | | | | | | |
| 1 | | Reserved | | | | | | | |
| 2 | | Total_Number_of_HashUnits | | | | | | | |
| ... | | | | | | | | | |
| 5 | | | | | | | | | |
| 6 | | Total_Number_of_Layers | | | | | | | |
| 7 | | Layer_Number | | | | | | | |
| 8 | | Number_of_HashUnits | | | | | | | |
| ... | | | | | | | | | |
| 11 | | | | | | | | | |
| 12 | | Number_of_Digests | | | | | | | |
| 13 | | | | | | | | | |
| 14 | | Applicant ID | | | | | | | |
| 15 | | | | | | | | | |

| | |
|-----------------|--------------------------------|
| 16 ... 19 | Content Sequence Number |
| 20 21 | Reserved |
| 22 23 | Reserved |
| 24 25 | Length_Format_Specific_Section |
| 26 27 | Reserved |
| 28 : 35 | Content Hash Table Digest |
| 36 : 75 | Signature Data |

- A 1-byte Certificate Type value, where 80₁₆ shall be used to indicate a first-generation CSS Content AACCS Certificate
- A 4-byte Total_Number_of_HashUnits field indicates the total number of Hash Units on the optical media.
- A 1-byte Total_Number_of_Layers field indicates the total number of layers on the optical media. This field shall be 01₁₆ for the CSS Content AACCS Certificate regardless of the actual total number of layers.
- A 1-byte Layer_Number field shall be 00₁₆ for the CSS Content AACCS Certificate, regardless of the actual layer number.
- A 4-byte Number_of_HashUnits field indicates the number of Hash Units on the layer for which this CSS Content AACCS Certificate is created.
- A 2-byte Number_of_Digests field indicates the number of Content Hash Table Digests contained within the CSS Content AACCS Certificate. For the CSS Content AACCS Certificate, this value is 1.
- A 2-byte Applicant ID, assigned by the AACCS LA. Each adopter that will be submitting requests to AACCS LA to create CSS Content AACCS Certificates will be assigned a unique Applicant ID. Each CSS Content AACCS Certificate will also be unique.
- A 4-byte Content Sequence Number assigned by the AACCS LA to uniquely identify the Certified Content amongst that applicant's content. The combination of the Applicant ID and the Content Sequence Number is referred to as the CSS *Content_AACCS Certificate_ID*. In other words, the CSS Content AACCS Certificate ID is a 6-byte number.
- A 2-byte Length_Format_Specific_Section that specifies the length of the subsequent Format_Specific_Section. This field shall be set to 0.
- 8-byte Content Hash Table Digests, containing the digests of the Content Hash Tables. The digest consists of the least significant 64 bits of the resulting digest from SHA-1 as described in the AACCS *Pre-recorded Video Book* of this specification.
- A 40 byte Signature Data, calculated using the Entity Private Key, over the entire data up to and including Content Hash Table Digest.

2.2 Content Hash Table

A CSS Disc created by an AACS Licensed Content Producer shall store a Content Hash Tables (CHT), which shall reside in the “AACS” directory under the file name “CSS_CONTENT_HASH_TABLE.AACS”. The CHT contains the eight-byte hash values of all the Hash Units on the DVD disc. The CHT has the format shown in Table 2-2.

Table 2-2 – Format of Content Hash Table

| Byte | Bit | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |
|-------------------------|-----|------------------------------|---|---|---|---|---|---|---|
| 0 : 3 | | Number of Hash Values (NHV) | | | | | | | |
| 4 : 7 | | Reserved | | | | | | | |
| 8 : 15 | | Hash Value of Hash Unit #1 | | | | | | | |
| 16 : 23 | | Hash Value of Hash Unit #2 | | | | | | | |
| ... | | ... | | | | | | | |
| 8*NHV : 7 + 8*NHV | | Hash Value of Hash Unit #NHV | | | | | | | |

CHT consists of the following fields:

- Number of Hash Values (NHV) of 4 bytes which indicates the total number of Hash Values in the CHT. The NHV shall not exceed 500000.
- A series of 8-byte Hash Values, each of which stores the hash value calculated from the corresponding Hash Unit. The hash value is the lsb 64 bits of the SHA-1 hash value. The SHA-1 hash value shall be calculated regardless of whether the Hash Unit are encrypted or not, which means that a player device need not decrypt the Hash Units before checking the hash value.

The total number of the Hash Units on the CSS DVD Disc shall not exceed 500,000. If the player encounters a Hash Unit whose Hash Unit Number (HUN) exceeds the NHV, the player shall immediately go to the Stop State. HUN is assigned to each Hash Unit in ascending order within each VOBS. Among VOBS, HUN is assigned in the following order:

VMGM -> VTSM#1 -> VTSTT#1 -> VTSM#2 -> VTSTT#2 -> ... -> VTSM#n -> VTSTT#n.

Note that the value of HUN starts from one. Therefore, if VMGM exists, HUN of the first Hash Unit in VMGM is one, and HUN of the last Hash Unit in VTSTT#n has the largest value in the disc.

2.3 Hash Unit

Each Video Object Set (VOBS) is a collection of Video Objects (VOBs), and each VOB is divided into one or more Cells, which consists of Video Object Units (VOBUs). The entirety of one Video Object Unit is utilized as one Hash Unit in case of CSS Content Hash Table. For more detail of Video Object Unit, refer section 5.1 of *DVD Forum, DVD Specifications for Read-Only Disc, Part 3 Video Specifications*. Note that the number of Video Object Units on a CSS DVD Disc shall not exceed 500,000.

2.4 Creating the CSS Content AACS Certificate

A Licensed Replicator shall create the CSS Content AACS Certificate by the following procedure.

1. The digests of the individual units of content are computed as follows:

$$C_d = [\text{SHA-1}(\text{Hash_Unit})]_{\text{lsb}_{64}}$$

Where Hash_Unit is defined in 2.3 and SHA-1 is the SHA hashing function as defined in *Introduction and Common Cryptographic Elements* book.

All Hash_Units on the media shall be included in this computation. In the case where some of the Hash_Units on the media are encrypted and others are not encrypted, the digest of the unencrypted Hash_Units shall also be included in the CHT. For Hash_Units that are encrypted, C_d shall be calculated after encryption of those Hash_Units.

2. Each instance of C_d is stored in the Content Hash Tables (CHT). Note that the C_d s shall be listed in the CHT in the following order:

$$\text{VMGM} \rightarrow \text{VTSM\#1} \rightarrow \text{VTSTT\#1} \rightarrow \text{VTSM\#2} \rightarrow \text{VTSTT\#2} \rightarrow \dots \rightarrow \text{VTSM\#n} \rightarrow \text{VTSTT\#n}$$

In case VMGM and/or VTSM(s) is(are) missing on the disc, the corresponding C_d (s) is(are) not listed in the CHT. For details of these VOBS files above, refer to *DVD Forum, DVD Specifications for Read-Only Disc, Part 3 Video Specifications*.

3. The digest of the Content Hash Table is computed as follows:

$$\text{CHT}_d = [\text{SHA-1}(\text{CHT})]_{\text{lsb}_{64}}$$

4. The CHT_d is stored in a CSS Content AACS Certificate (CC) and the CSS Content AACS Certificate is cryptographically signed as follows:

$$\text{CC}_{\text{sig}} = \text{AACS_Sign}(\text{AACS_CC}_{\text{priv}}, \text{CC})$$

With AACS_Sign as defined in *Introduction and Common Cryptographic Elements* book and the format and layout of the CSS Content AACS Certificate as defined in Section 2.1. The private key, denoted $\text{AACS_CC}_{\text{priv}}$, is an additional private key of the AACS LA that is used only for the purpose of signing the CSS Content AACS Certificate.

This step will be performed at a secure facility operated by the AACS LA where $\text{AACS_CC}_{\text{priv}}$ is securely stored. The previous steps are all performed by the Licensed Replicator. This process is demonstrated in Figure 2-1.

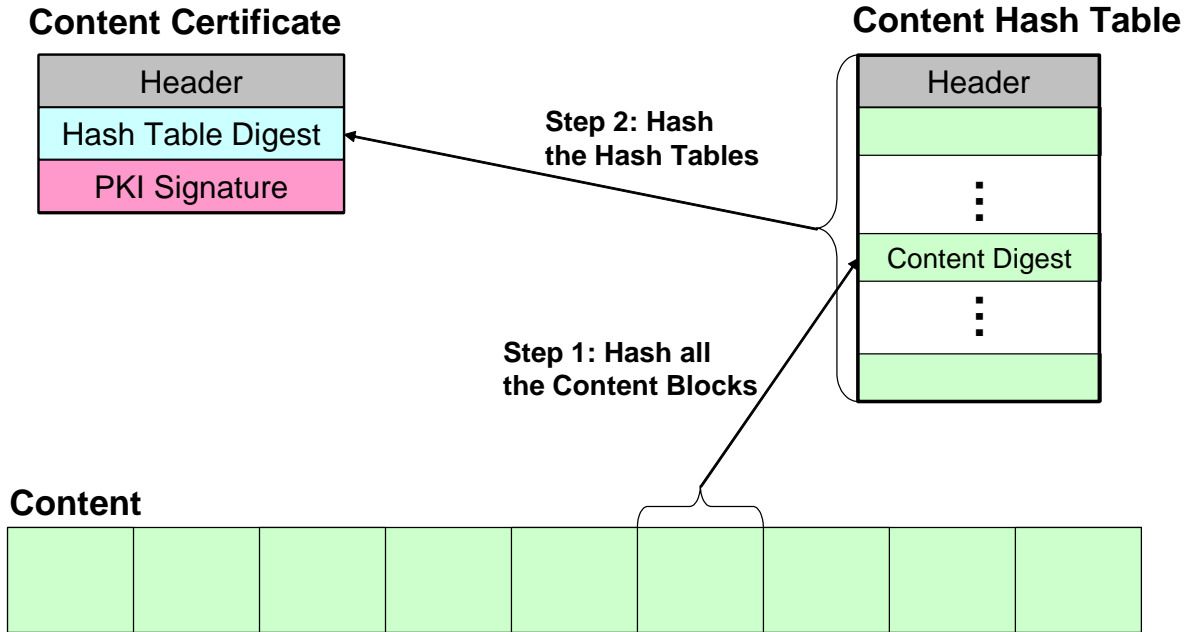


Figure 2-1 – Content Signing Process for CSS

2.5 Verifying the CSS Content AACS Certificate and Screening Obligation

As a condition of bypassing screening of the Trusted Source Mark from content stored on CSS protected media, a Licensed Product shall for each starting use, verify the integrity of that content by the procedure enumerated below. If a CSS Content AACS Certificate is present and does not validate, then playback is halted.

If the initial CSS Content AACS Certificate validation step above is *skipped*, then the Licensed Product will screen for the Trusted Source Mark, and if it is detected, the Licensed Product will check for a valid CSS Content AACS Certificate by the procedure enumerated below. If the CSS Content AACS Certificate validates, then enforcement will be suppressed, and Trusted Source Mark screening will stop.

1. If the CSS Content AACS Certificate ID is on the AACS Content Revocation List (CRL) stored in the player, the player shall not play the content. If the player has not yet acquired a CRL from AACS protected content, then it shall skip this step.
2. Selects a subset of hash units randomly from all content hash units, from which the content hash value is calculated. The Licensed Product shall select the subset of hash units using one of the following two procedures:
 - a) Selects 7 hash units randomly from all content hash units
 - b) Selects the first hash unit and additionally selects at least 1% of the remaining content hash units from the position where playback begins until the end of the Title, where the hash units are randomly selected and evenly distributed throughout all content hash units. As an example, the Licensed Product could use a pseudo randomly generated value modulo 100 to determine which one of the next 100 hash units to verify.

All digests in the CHT shall be included in this selection process.

3. Calculates hash value for each of the selected content hash units.

$$C_d = [\text{SHA-1}(\text{Hash_Unit})]_{\text{lsb}_{64}}$$

Where Hash_Unit is as defined above and SHA-1 is the SHA hashing function as defined in *Introduction and Common Cryptographic Elements* book.

4. Reads Content Hash Table (or tables), which includes the content hash values corresponding to the selected content hash units and calculates the Content Hash Table digest.
$$\text{CHT}_d = [\text{SHA-1}(\text{CHT})]_{\text{lsb}_{64}}$$
5. Reads CSS Content AACS Certificate, which includes the Content Hash Table digest that should match the digest calculated in step 3. If they do not match, the Licensed Product shall not proceed with content playback.
6. Verifies the Signature of the CSS Content AACS Certificate, where the Content Hash Table digest (or digests) has been replaced with the digests calculated in step 3.
$$\text{AACS_Verify}(\text{AACS_CC}_{\text{pub}}, \text{CC}_{\text{sig}}, \text{CC})$$

With AACS_Verify as defined in *Introduction and Common Cryptographic Elements* book. The public key, denoted AACS_CC_{pub}, is an additional public key of the AACS LA that is used only for the purpose of verifying the CSS Content AACS Certificate. All Licensed Players are required to store this AACS LA's additional public key in a way that resists malicious modification.
7. The Licensed Product will not proceed with content playback if the signature fails to correctly verify.
8. For each selected hash unit, verifies that the calculated C_d from step 3 is equal to the corresponding C_d that was contained in the selected Content Hash Tables. The Licensed Product will not proceed with content playback if the digest of any of the selected hash units fails to match the expected digest value.