Content Protection System Architecture

A Comprehensive Framework for Content Protection

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

February 17, 2000
Revision 0.81

Notice

Contents

This page is intentionally left blank.

Executive Summary

The personal computing and consumer electronics industries have developed a number of technologies to protect entertainment content. An overall framework or architecture is needed to ensure that this content is protected in an efficient and effective way as it passes from one technology to another within the content protection system. The Content Protection System Architecture (CPSA) defines a comprehensive and efficient framework that makes it possible to integrate major existing content protection technologies as well as new technologies as they emerge. CPSA is equally effective for PC and consumer electronics implementation. It protects audio and video content in both the analog and digital domains. CPSA also comprehends both physical and electronic content distribution methods.

The CPSA architecture provides a framework of 11 axioms that describe how compliant devices handle copy control information, playback and output, and recording. Adoption of this architecture can strengthen the overall content protection system, ease implementation burdens on developers, and bring consistent guidelines to content protection efforts.

Introduction: The Need for a Comprehensive CP Framework

As more content enters the digital domain, the desire to protect that content grows. With consumers increasingly eager to move content between devices such as PCs, DVD players and recorders, set-top boxes, and digital TVs, a variety of content protection technologies have been developed. These point solutions come together to form an overall "chain" of content protection technologies. Figure 1 depicts an illustrative example of such a chain, where for the sake of clarity analog connections are not shown. This illustration should not be considered definitive.

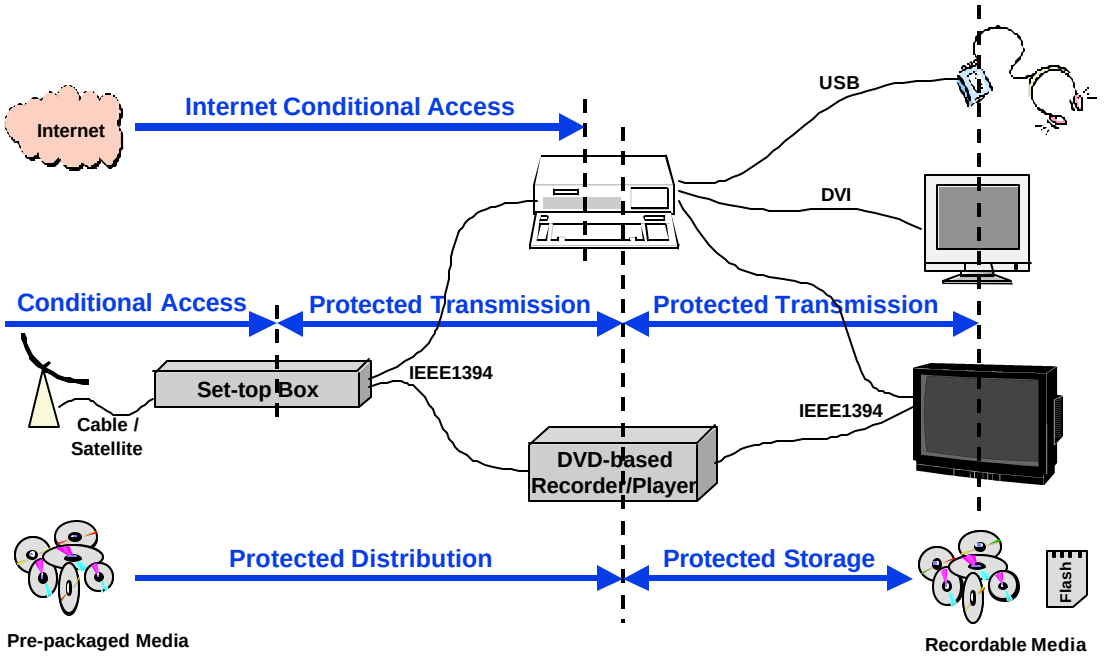


Figure 1. Digital Content Protection Chain

The strength and completeness of the chain depends on more than just the individually developed links. The rising number of content protection technologies makes clear that an overall system architecture is needed to ensure that the individual pieces form a coherent whole.

Without such a unifying architecture, inconsistencies, gaps and even conflicts can occur between the various technologies, reducing the effectiveness of an overall content protection solution. The lack of a unifying architecture also leads to redundant and costly development efforts.

What's needed is an architecture that defines a set of overall principles or axioms that content owners and product developers can apply to ensure that content is protected in an efficient and effective way as it passes from one technology to another within the content protection system. Such an architecture can strengthen the overall content protection system, ease implementation burdens on developers, and apply a consistent set of guidelines to all content protection efforts. By promoting the development of a comprehensive, compatible content protection system, this architecture stands to benefit content owners, content providers, device manufacturers, and above all consumers.

This paper describes such an overall architecture, called the **Content Protection System Architecture** or CPSA.

CPSA Goals and Scope

The goal of CPSA is to establish an overall system architecture for protecting content. CPSA defines a comprehensive and effective framework that makes it possible to efficiently integrate major existing content protection technologies as well as new technologies as they emerge.

The CPSA architecture has been defined to be broadly comprehensive, spanning analog and digital, audio and video, consumer electronics and PC systems, and physical and electronic distribution techniques. Using watermarking and encryption, CPSA specifies a framework for protecting both analog and digital content. Likewise, CPSA's architectural concepts are applicable to both audio and video, so that while specific technologies may be oriented to one domain or the other, the overall architecture is equally effective for audio and video content. Individual technologies have been carefully selected to be equally effective for consumer electronics and personal computer implementations, as well as to encompass the varying requirements of physical and electronic distribution methodologies.

CPSA has also been designed to avoid duplication of effort. As a result of close collaboration with the Secure Digital Music Initiative (SDMI) and the Content Protection Technology Working Group (CPTWG), CPSA is consistent with and encapsulates the current thinking of these groups. Its adds value to the work of these groups by addressing critical "interface" issues needed to ensure a comprehensive content protection framework.

CPSA Overview

A comprehensive content protection system depends on both technologies and policies. CPSA specifies the use of two key technologies, watermarking and encryption, which together provide a means to enforce content protection policies.

Watermarking is a technology that allows information to be embedded in content in a way that is intended to be transparent to the end-user of that content and robust against the information's being removed or altered. The information stays with the content regardless of the content's analog or digital representation.

Watermarking in and of itself does not protect the content. When used as part of a content protection system, watermarking is typically used to carry content management information (CMI)[1]. Sometimes referred to as "usage rules", CMI is information carried with content that

[1] Watermarking can have other uses within a content protection system as well, such as the fragile watermark defined in SDMI.

indicates conditions and requirements constraining use of the content. CMI may include copy control information (CCI), which indicates constraints specific to copying. CMI may also include other information not directly related to copying, such as APS trigger bits (indicating what type of analog protection must be applied to outputs), or information related to playback control (for example, bits indicating whether and in what manner broadcast pause may be applied to Copy Never content). The protection comes from compliant devices responding appropriately to manage the content according to the CMI. Such protection is realized only if there is some means, or "hook", to compel devices to be compliant.

Encryption is that hook. Encryption is a way of scrambling digital content so that it is unusable (not recognizable) unless it is first descrambled (decrypted). To get the necessary intellectual property to be able to decrypt the content, a license is required. That license contract specifies requirements to manage the content according to its CMI.

Content can take on both analog and digital forms as it passes through an overall content protection system. Through the combined use of watermarking and encryption, CPSA addresses protection of content in both the analog and digital domains.

CPSA Axioms

CPSA provides a framework of 11 axioms that describe how CPSA-compliant devices handle the three major areas that are critical to ensuring a comprehensive, consistent content protection scheme: content management information, access, and recording.

Content Management Information Axioms

Content Management Information (CMI) is information carried with content that indicates limitations on its allowed usage, such as constraints on making copies.

1. Content Owner Selects CMI

Axiom: The content owner selects the content management information (CMI) from the supported options.

The content owner selects the appropriate content management information for his or her content from the supported options. The available options vary for different types of content according to agreements made between content owners and device manufacturers. Video CMI follows the encoding rules for video content, which are derived from the Digital Millennium Copyright Act of 1996 and are currently under discussion. Audio CMI follows the DVD-Audio Framework.[2]

2. Ensure Digital CMI Integrity

Axiom: While the content remains in the encrypted digital form, the CMI integrity is ensured during transmission and storage using the encryption and key management protocols.

CMI is stored and/or transmitted along with the content. While the content remains in the encrypted digital form, the CMI can be carried digitally. For example, the CMI may be encrypted along with the content. The content may also be accompanied by unencrypted CMI, which is protected against tampering by using its value as part of the decryption key for the content. CMI that is associated with encrypted content in a digital manner (either encrypted or unencrypted) is referred to as *digital CMI*.

[2] For the DVD-Audio Framework, see http://www.4Centity.com.

3. Optional Watermarking

Axiom: At the content owner's option, the original content may be watermarked for the purpose of transmitting the CMI with the content, independent of its specific analog, digital or encrypted digital representation.

The CMI may also be embedded into the original content using a watermark. This is known as *watermark CMI*. Watermark CMI enables the CMI to be stored with and transmitted with the content independent of its analog, digital, or encrypted digital representation. Use of watermarking is at the discretion of the content owner. Some content owners may not want to include a watermark in portions of content where they are concerned about transparency, for example. To gain the benefits of watermarking in CPSA, however, it is important to note that watermark CMI must be included in the original content.

Access Control Axioms

In CPSA, encryption can be used to prevent non-compliant devices from accessing protected content. Alternatively, where encryption is not present, compliant devices control access by detecting watermark CMI and responding appropriately.

4. Encrypt Prerecorded Content

Axiom: All CPSA content on prerecorded media is encrypted.

Content encryption is a key facet of CPSA. It ensures that the content cannot be accessed until it is decrypted. In conjunction with licensing structures, it is the "hook" that compels users to honor the provisions of the content protection system. Thus, all digital content that has usage restrictions on prerecorded media (e.g. DVD-ROM) is encrypted.

5. Encrypt Authorized Copies

Axiom: All authorized copies of CPSA content are encrypted, except where specifically agreed otherwise

Just as all content with usage restrictions on prerecorded media is encrypted, so are all authorized digital copies of such content (meaning content that arrives encrypted and/or containing watermark CMI). For example, when a CPSA-compliant device receives analog content with watermark CMI, a digital copy of the analog input will be encrypted. This allows the encryption "hook" mentioned previously to remain in place even for authorized copies. An exception to this is the DVD-audio framework, which allows an unencrypted copy on legacy media (CD-R, CD-RW, Mini-Disc or DAT) of any audio content with a sound quality equivalent to CD-Audio or less.

6. Playback Control

Axiom: Compliant playback modules detect the watermark CMI when present in unencrypted content and respond appropriately to prevent playback of unauthorized copies.

Before playing back unencrypted digital content, compliant playback modules check for watermark CMI. If present in unencrypted digital content, compliant modules will not allow playback, since all digital copies of content with watermark CMI should be encrypted.

7. Output Protection

Axiom: For encrypted content, compliant playback and source modules apply an approved protection scheme to all outputs, according to the digital CMI settings, except where specifically agreed otherwise.

Protection of encrypted CPSA content must continue during transmission, either by encryption (e.g., DTCP) or by an approved analog protection scheme such as Macrovision™. Playback and source modules examine the digital CMI of encrypted content, and apply protection to outputs accordingly. An exception to this is in the DVD-Audio famework, which allows unprotected real-time transmission of any audio content on analog and CD-Audio quality digital (e.g. IEC-958, USB) outputs.

8. Manage Protected Output of Unencrypted Content

Axiom: Compliant source modules check the watermark CMI of unencrypted content prior to protected digital output, and if present, set the digital CMI for the output accordingly.

A compliant source module may optionally forward content that arrives unencrypted to a protected digital output. If it does so, the module must first check for watermark CMI, and if it is present, set the digital CMI of the protected output accordingly. This ensures that the digital CMI corresponds to the watermark CMI, which is necessary since compliant recording modules downstream will check only the digital CMI of encrypted content to determine if a copy is authorized. If watermark CMI is not present in the unencrypted content, a content protection system may still support protected digital output, in which case the digital CMI of the output is set as defined by that system.

Recording Control Axioms

Recording devices maintain content protection by examining digital or watermark CMI and making copies only if authorized to do so. Copies of content are encrypted (except as noted previously), and the digital and watermark CMI are updated to continue the protection of the copied material.

9. Examine CCI Before Copying and Respond Accordingly

Axiom: Compliant recording modules detect and respond appropriately to the CCI, if it is present, before creating a copy, if authorized to do so.

- *Digital CCI is examined for encrypted content*
- *Watermark CCI is examined for unencrypted content*

Before making a copy, a compliant recording module checks the CCI information. If the module is making a copy from an encrypted source, it checks the digital CCI; otherwise, it checks the watermark CCI. The copy is made only if the CCI indicates that it is authorized.

10. Update CCI Before Copying

Axiom: Compliant recording modules appropriately update both the digital CCI and the watermark CCI, when present, before creating a copy.

Prior to creating a copy of CPSA content, compliant recording modules will appropriately update both the digital CCI and the watermark CCI, if present. Since the watermark CCI is always updated when a copy is made, compliant playback modules are not required to have watermark updating capability. Note that for non-CPSA content (unencrypted content without watermark CMI), a protection system[3] may still support making an encrypted copy, in which case the digital CCI of the copy is set as defined by that system.

[3] For example, SDMI allows unencrypted, non-watermarked content to be brought into the protected (e.g. encrypted) SDMI domain.

11. Temporary Images

Axiom: Compliant recording modules do not inspect or update either the digital CCI or the watermark CCI when making an image that is both temporary and localized.

To allow for enhanced (e.g. time-shifted) viewing of copy-never content, compliant recording modules do not inspect or update either the digital CCI or the watermark CCI when making an image that is both temporary and localized. Content controlled in this manner must exist in a playable form for only a limited time, and must be stored in such a way that it can only be played back from the system used to create the image. Since such an image is not useful as an archival copy, it may be made independent of restrictions on copying indicated by the CCI. Note that although CCI is neither checked nor updated in this case, some types of content might contain other types of CMI, such as bits related to time shifting, that would need to be checked and updated appropriately.

CPSA-Consistent Content Protection Technologies

Below is a representative list of CPSA-consistent content protection technologies, at the time of this publication. Technology summaries and contact information are provided in Appendix B.

- CPRM for protecting content stored on recordable media such as DVD or Flash
- CPPM for protecting pre-recorded DVD-Audio content
- CSS for protecting pre-recorded DVD-Video content
- DTCP for protecting content during digital transmission over 1394 and USB
- HDCP for protecting content moving across high-bandwidth interfaces to digital displays
- Conditional Access for protected distribution of premium content via cable or satellite
- 4C / Verance Watermark for embedding and reading watermark CMI in audio content
- A video watermarking scheme, to be selected by the DVD CCA

CPSA Examples

This section illustrates how the CPSA axioms are applied in several hypothetical scenarios. Flow diagrams are provided for four CPSA-compliant modules: a recording module, playback module, source module and display module. These modules could be mapped onto a variety of real devices. For example, a recorder module could be mapped onto a CE recording device, or a combination of PC and drive, or another product combination. Assume all modules are for video devices, so the modules might represent, respectively, a video recorder, video player, television and set-top box. Each diagram shows which specific CP-related checks and transformations are performed at which points in the data path, from input to output.

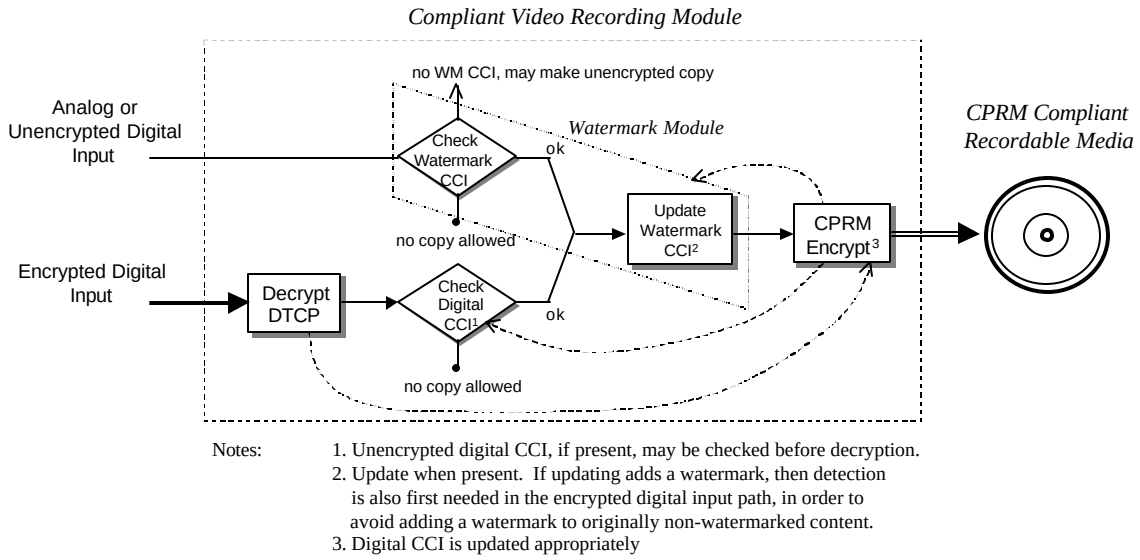
Please note that these diagrams are for illustrative purposes only, and are neither definitive or exhaustive. The technologies shown are <u>not</u> the only ones that can be used for their given function. For example, DTCP is representative of content protection technologies for digital transmission, but other technologies that adhere to the CPSA architecture could also fill that role. In addition, certain application-specific details that are outside the scope of the architecture, such as media type detection and authentication, are omitted.

These diagrams observe the following conventions:

- Diamonds indicate checks (e.g., checking digital and/or watermark CMI).
- Rectangles indicate transformations (e.g., encryption, decryption, watermark CMI updating, and the application of APS (analog protection system) at an output). These checks and transformations have specific names in cases where representative CPSA-consistent technologies (e.g. DTCP) apply.

- Single solid lines show the flow of unencrypted data.
- Double solid lines show the flow of encrypted data.
- Curved dotted lines indicate which licenses compel which checks and transformations.

Compliant Video Recording Module



Notes:
1. Unencrypted digital CCI, if present, may be checked before decryption.
2. Update when present. If updating adds a watermark, then detection is also first needed in the encrypted digital input path, in order to avoid adding a watermark to originally non-watermarked content.
3. Digital CCI is updated appropriately

Figure 3. Compliant Video Recording Module

Content Flow, Encrypted Digital Input

The module checks the digital CCI and makes a copy only if authorized to do so. For digital CCI that comes encrypted along with the content, this check must occur after decryption. In some cases the content may also be accompanied by unencrypted digital CCI (protected from tampering via cryptographic key management), which could be checked before the content is decrypted, as indicated by Note 1. In any case, both types of digital CCI are checked as required to determine if a copy is authorized before proceeding to make the copy.

If a copy is permitted, then after performing DTCP decryption the module updates the watermark CCI appropriately to reflect that a copy has been made. Note that for content arriving via an encrypted input, there is no requirement to check the watermark CCI for the purpose of determining if a copy can be made, since the digital CCI is checked for that purpose. However, for watermarking technologies that update CCI by adding a watermark, it is necessary to check for watermark CCI before updating, solely to avoid adding a watermark to originally non-watermarked content (Note 2). In this way the decisions of content owners who elect not to watermark portions of their original content are honored.

Finally, the module performs CPRM encryption on the content and stores it on CPRM-compliant media. As Note 3 indicates, the encrypted copy's digital CCI is set appropriately to reflect the copy.

Content Flow, Analog or Unencrypted Digital Input

The module checks the watermark CCI and makes a copy only if authorized to do so. If a copy is authorized, the module updates the watermark CCI, if present, to reflect the copy and performs CPRM encryption on the content. The encrypted copy's digital CCI is set appropriately to reflect the copy (Note 3). Finally, the encrypted content is stored on CPRM-compliant media.

Depicted License Obligations

The DTCP license requires, as a condition for decryption, that the module:

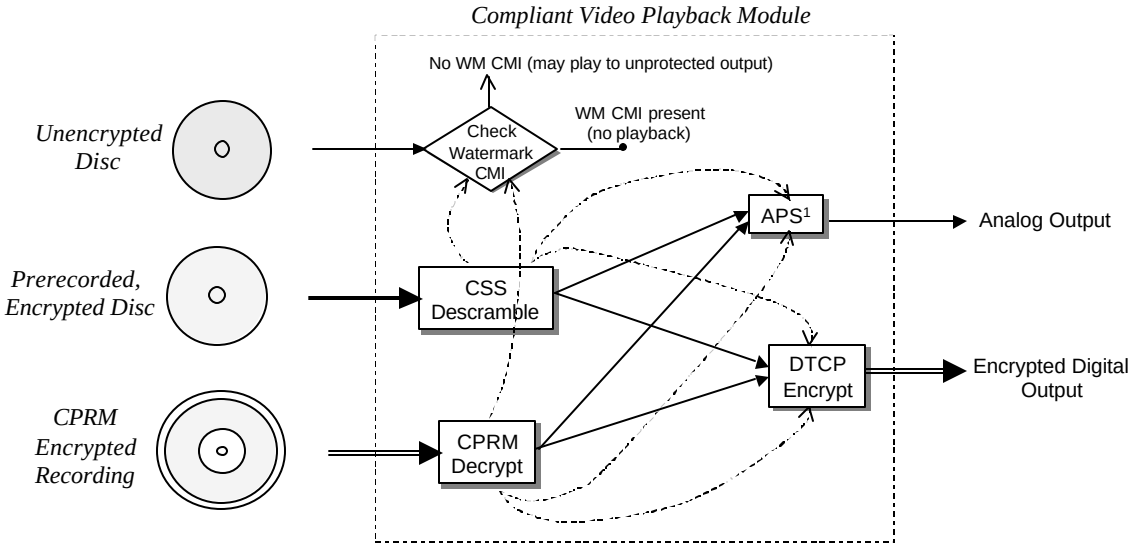
- Use an approved protection technology (such as CPRM) when making an authorized copy.

The CPRM license requires that the module:

- Check the digital CCI of content arriving via an encrypted digital input before making a copy, if one is authorized
- Check the watermark CCI of content arriving via an analog or unencrypted digital input before making a copy, if one is authorized
- Update the watermark CCI, if present, before making an authorized copy.
- Encrypt authorized copies, setting the digital CCI appropriately to reflect the copy.

Note that if a recording device records from an encrypted digital input, the license for decryption of the digital input can require that the subsequent recording be encrypted. In turn, the license for making the encrypted recording can require watermark CMI detection before recording from analog inputs. On a device that makes only unencrypted recordings from analog or unencrypted inputs, there is no license that compels the device to observe the watermark CMI. However, a recording of watermarked content made by such a device will not be playable on compliant players (which require that such recordings be encrypted).

Compliant Video Playback Module



Notes: 1. APS applied as indicated by the digital CMI

Figure 4. Compliant Video Playback Module

Content Flow, CPRM Encrypted Recording

The module performs CPRM decryption on the content. Then the module performs DTCP encryption on the content before digital output, or applies APS to the content before analog output, as indicated by the digital CMI.

Content Flow, Pre-Recorded Encrypted Disc

The module performs CSS decryption (descrambling) on the content. Then the module performs DTCP encryption on the content before digital output, or applies APS to the content before analog output, as indicated by the digital CMI.

Content Flow, Unencrypted Disc

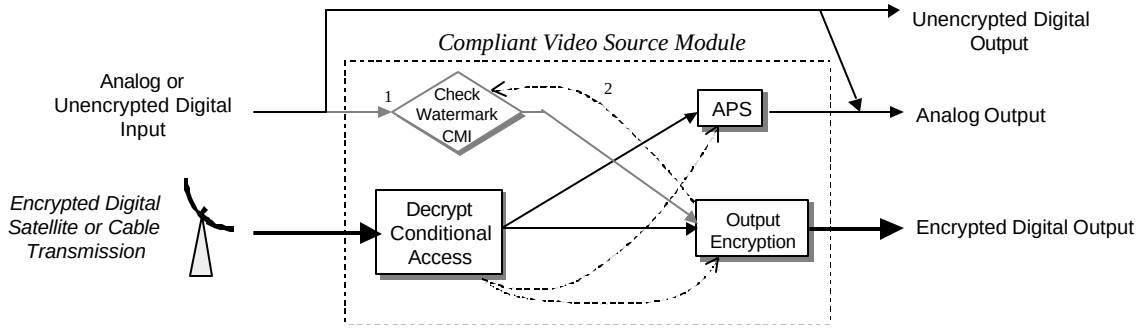
The module checks for watermark CMI. If watermark CMI is present, the module does not perform playback of the content, which is considered to be a non-compliant copy since it is not encrypted. Otherwise, the content may be played to an analog or unencrypted digital output.

Depicted License Obligations

The CPRM and CSS licenses each require:

- Checking watermark CMI before playing unencrypted content
- Applying an approved protection when playing encrypted content to a digital or analog output

Compliant Video Source Module



Notes:
1. Watermark checking capability is needed only in modules that support this optional path.
2. License requirement of an output encryption scheme that supports protection of unencrypted inputs.

Figure 5. Compliant Video Source Module

Content Flow, Encrypted Digital Input

The module decrypts the input content using the technology pertaining to the given conditional access scheme. Then the module performs DTCP encryption on the content before digital output, or applies APS to the content before analog output, as indicated by the digital CMI.

Content Flow, Analog or Unencrypted Digital Input

In this example, the module supports the option of forwarding unencrypted content to an encrypted digital output (note 1). When that path is taken, the module checks the watermark CMI, and then performs output encryption on the content. The encrypted output's digital CCI is set appropriately to correspond to the watermark CMI, if present. If watermark CMI were not present, and the output encryption scheme supported protection of such content, then the digital CCI would be set according to rules defined by the output encryption scheme for that case.

Depicted License Obligations

The license for the conditional access decryption requires that the module:

- Apply an approved protection when forwarding encrypted content to a digital or analog output.

If the output encryption scheme supports protection of unencrypted inputs, then its license requires that the module:

- Check the watermark CMI, and if present set the digital CMI of the encrypted output accordingly (note 2).

Compliant Video Display Module

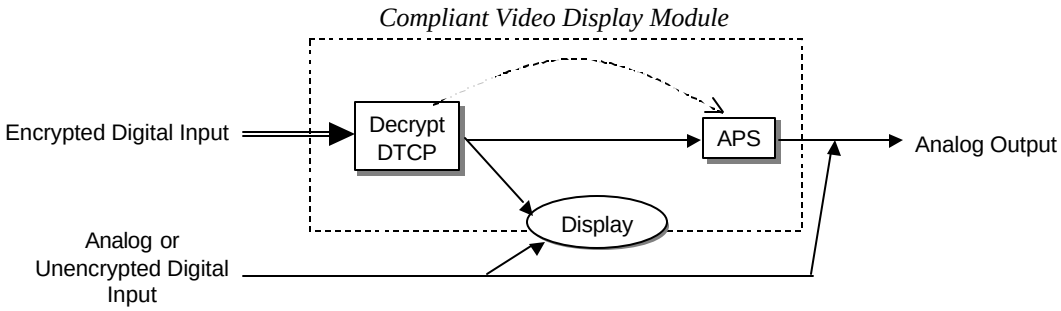


Figure 6. Compliant Video Display Module

Content Flow, Encrypted Digital Input

The module performs DTCP decryption on the content, and then either displays it, or applies APS (as indicated by the digital CMI) before forwarding it to an analog output.

Depicted License Obligations:

The DTCP license requires that the module apply APS (as indicated by the digital CMI) before forwarding the content to the analog output.

4C and Content Protection

The 4C applies the resources of IBM, Intel, Matsushita and Toshiba to the goal of developing technologies and infrastructure for a comprehensive, cohesive content protection solution. The companies' resources and expertise in cryptography, watermarking, and tamper resistance have been brought to bear on solving the complex problems of delivering robust yet cost effective content protection solutions that balance the needs of content owners with those of implementers and consumers.

Summary

The Content Protection System Architecture defines a comprehensive, efficient framework for protecting commercial entertainment content. The architecture is flexible enough to allow for integration of new technologies as they develop. CPSA sets up an overall framework that accommodates the needs of various technologies while still providing guidance for the overall

system. By specifying a framework for handling CMI and identifying the content protection obligations of compliant modules, CPSA simplifies the device development process, reduces redundant development efforts, and promotes compatibility and consistency between the content protection schemes of playback and recording devices. The adoption of CPSA can strengthen the overall content protection system, bring greater consistency to all content protection efforts, ease implementation burdens on developers, and foster the growth of the digital entertainment industry.

Please address questions and comments about this paper to cpsa-comment@4Centity.com.

Appendix A. CPSA Axioms

Content Management Information Axioms

1. The content owner selects the content management information (CMI) from the supported options.

2. While the content remains in the encrypted digital form, the CMI integrity is ensured during transmission and storage using the encryption and key management protocols.

3. At the content owner's option, the original content may be watermarked for the purpose of transmitting the CMI with the content, independent of its specific analog, digital or encrypted digital representation.

Access Control Axioms

4. All CPSA content on prerecorded media is encrypted.

5. All authorized copies of CPSA content are encrypted, except where specifically agreed otherwise.

6. Compliant playback modules detect the watermark CMI when present in unencrypted content and respond appropriately to prevent playback of unauthorized copies.

7. For encrypted content, compliant playback and source modules apply an approved protection scheme to all outputs, according to the digital CMI settings, except where specifically agreed otherwise.

8. Compliant source modules check the watermark CMI of unencrypted content prior to protected digital output, and if present, set the digital CMI for the output accordingly.

Recording Control Axioms

9. Compliant recording modules detect and respond appropriately to the CCI, if it is present, before creating a copy, if authorized to do so.

- Digital CCI is examined for encrypted content
- Watermark CCI is examined for unencrypted content

10. Compliant recording modules appropriately update both the digital CCI and the watermark CCI, when present, before creating a copy.

11. Compliant recording modules do not inspect or update either the digital CCI or the watermark CCI when making an image that is both temporary and localized.

Appendix B. Representative CPSA-Consistent Content Protection Technologies

Content Protection for Recordable Media (CPRM)

Summary	Specification enabling protected exchange of audio/visual content recorded on DVD and Flash media; specifies encrypted storage of content, protected storage of content management information, system renewability, and methods to prevent playback of bit-by-bit copies.
Developed by	4C (IBM, Intel, MEI, Toshiba)
Contact:	4C Entity, LLC http://www.4Centity.com

Content Protection for Pre-recorded Media (CPPM)

Summary	Under development at the time of this publication. Specification for robust protection of DVD-Audio content stored on DVD-ROM media. Specifies encrypted storage of content, protected storage of content management information, system renewability, and methods to prevent playback of bit-by-bit copies.
Developed by	4C (IBM, Intel, MEI, Toshiba)
Contact:	4C Entity, LLC http://www.4Centity.com

Content Scrambling System (CSS)

Summary	Method for protecting DVD-Video content via authentication and content scrambling.
Contact:	DVD Copy Control Association (CCA) http://www.dvdcca.org

Digital Transmission Content Protection (DTCP)

Summary	Specifies robust encryption of content passing between digital devices in the home, through the use of copy control information, authentication and key exchange, digital encryption and system renewability.
Developed by	5C (Hitachi, Intel, MEI, Sony, Toshiba)
Contact:	Digital Transmission Licensing Administrator, LLC (DTLA) http://www.dtcp.com Email: dtla@dtcp.com Telephone: 503-264-1562 Fax: 503-264-4151

High-bandwidth Digital Content Protection (HDCP)

Summary	Content protection for high-bandwidth interfaces to digital displays, such as DVI.
Developed by	Intel
Contact	Digital Content Protection LLC http://www.digital-CP.com Email: Info@Digital-cp.com Telephone: 503 264-6576 Fax: 503-264-4151

4C / Verance Watermark

Summary	Technology for creating and reading watermarks in audio content.
Developed by	Verance Corporation
Contact:	Verance Corporation http://www.verance.com

CPSA Glossary

CMI

Content Management Information. Information carried with content that indicates conditions and requirements constraining the use of that content. Sometimes referred to as “usage rules.”

CCI

Copy Control Information. Content Management Information that indicates constraints specific to copying. CCI is a subset of CMI.

CPSA axiom

One of eleven basic CPSA principles that embody CPSA policies and together provide a framework for comprehensive, efficient content protection.

CPSA content

Audio or video content that contains watermark CMI, and/or is encrypted by a CPSA encryption method.

Compliant recording module

A module that writes authorized copies of CPSA content onto supported recordable media.

Compliant playback module

A module that performs authorized output of CPSA content from recordable or prerecorded media.

Digital CMI

Content Management Information that is associated with encrypted content in a digital matter (either encrypted or unencrypted).

Localized

Refers to images whose usable playback is possible only when it occurs from the system used originally to create the image.

Temporary

Refers to images that will exist in a playable form for only a limited period of time as specified.

Watermark CMI

Content Management Information that is embedded into the original content using a CPSA watermark and is carried with the content regardless of whether the content is represented in analog, digital, or encrypted digital form.