



# Intel<sup>®</sup> Technology Journal

Interoperable Home Infrastructure

**Content Protection  
in the Digital Home**

# Content Protection in the Digital Home

Michael Ripley, Corporate Technology Group, Intel Corporation  
C. Brendan S. Traw, Corporate Technology Group, Intel Corporation  
Steve Balogh, Corporate Technology Group, Intel Corporation  
Michael Reed, Corporate Technology Group, Intel Corporation

Index words: content, protection, transmission, storage, DTCP, CPRM

## ABSTRACT

This paper describes a flexible and extensible framework for distributing digital content in a protected and interoperable manner within the home. Within this framework a “chain” of solutions provide comprehensive, end-to-end protection of digital entertainment content as it is delivered to the home and managed, stored, and consumed on a wide range of devices. These solutions employ a consistent set of technical and licensing mechanisms to ensure that the content is protected in an effective and efficient manner throughout the domain. This leads to a framework in which content protection solutions from a variety of licensors can be selected and combined in a flexible and interoperable manner, based on market forces.

A number of content protection solutions that operate within this framework have been developed and are

incorporated into products on the market today. This paper describes two such solutions:

- Content Protection for Recordable Media (CPRM)
- Digital Transmission Content Protection (DTCP)

## INTRODUCTION

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 personal computers, DVD players and recorders, set-top boxes, and digital televisions, 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

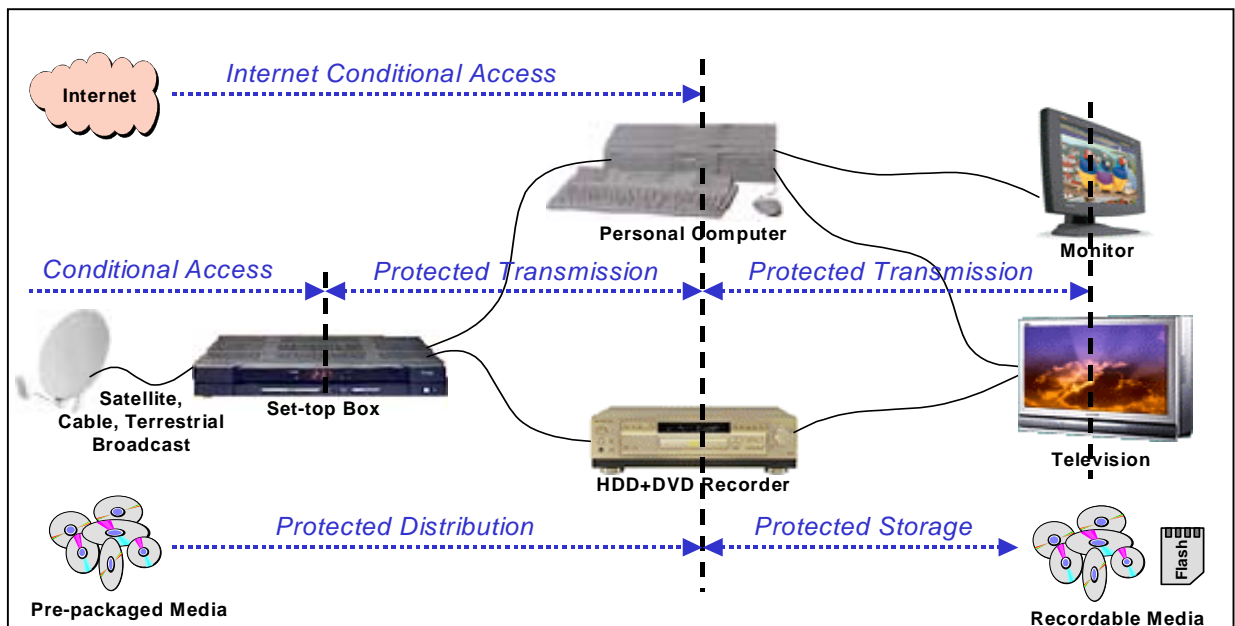


Figure 1: Digital content protection chain

should not be considered definitive.

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, interoperable 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.

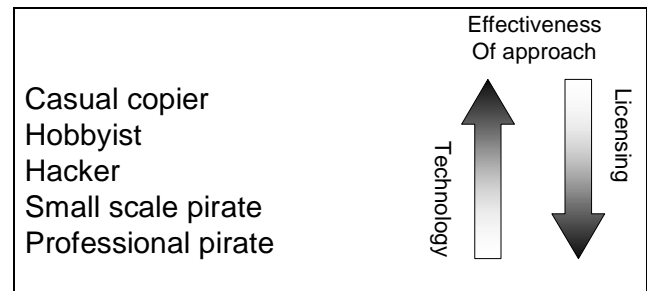
What is needed is an architecture that defines a set of overall principles that content owners and product developers can apply to ensure that content is protected in an efficient and effective way as it passes from one technology to another within the content protection system. Such an architecture can strengthen the overall content protection system, and ease implementation burdens on developers. 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.

## BASIC CONTENT PROTECTION STRUCTURE

Content protection solutions use a combination of technical and legal mechanisms to protect content against use that is inconsistent with the terms under which it was obtained from the content owner. The technical mechanisms take the form of a cryptographic protocol through which content is distributed or stored in an encrypted form. Access to the cryptographic keys and other intellectual property necessary to decrypt the protected content is subject to a license. This license is a legal tool to enforce the conditions under which such access is provided, including rules governing robust implementation and continued protection of content that is received subject to the license and subsequently stored or output.

The combination of technology and licensing provides a potent solution for preventing circumvention of content protection systems, while accommodating consumer expectations. Content protection technologies are effective at preventing unsophisticated attempts to circumvent a particular content protection solution. At the opposite extreme, well-financed professional pirates have routinely demonstrated an ability to defeat content protection technologies that have been incorporated within the economic constraints of consumer products. Conversely, licensing and other legal mechanisms are

much more effective against business entities with assets, employees, and distribution channels.



**Figure 2: Effectiveness of technology and licensing**

Thus, cryptographic technology implementations provide the basis for content protection, and an effective licensing structure provides for enforcement. The following subsections describe technical and licensing elements in further detail.

## TECHNICAL ELEMENTS

Cryptography represents the technical foundation for content protection. This foundation can be broken down into four key elements:

- **Authentication.** To ensure that only licensed products have access to the protected content, technical means are needed to verify that a product is authorized. This is accomplished by the licensor of a content protection technology providing secret values that are only available to licensed products, which can be explicitly or implicitly verified as part of the process to gain access to the content. An example of implicit verification is two products independently calculating and using a secret value that can only be calculated by compliant licensed products. Note that a licensed product can be not only a stand-alone physical device such as a television or set-top box, but also a software application running on a personal computer.
- **Encryption.** Encryption is used to prevent unauthorized access to protected content. Decryption should only be possible by products whose compliance with the licensing conditions is verified via authentication.
- **Usage States.** State is typically associated with content that governs how the content may be used. This information is stored and communicated in a manner that ensures its integrity is maintained. The information can be carried along with the content, with its integrity cryptographically protected.

Additionally, it can be embedded within the content using a watermarking technology or via online mechanisms that obtain a “license.” (“License” in this context means a file that is downloaded from a trusted source that conveys how the content may be used.) Products that license a content protection solution can be compelled through that license to respond to such watermark Usage State information as a means of extending the application of Usage States into the unprotected (e.g., analog) domain.

- **Renewability.** Renewability is used to extend the viability of a content protection solution. This is accomplished through a variety of mechanisms including updating a Digital Rights Management (DRM) system via online mechanisms and/or utilizing revocation. Either technique ensures a system’s integrity is preserved in the event that a licensed product’s authentication and/or encryption-related secrets are compromised and distributed. When such a compromise is detected and verified, the licensor of the content protection solution (through a process described below) may request an update or revocation of the compromised information. Revocable information should be assigned as finely as possible, ideally with each licensed product receiving unique information, thereby localizing the effect of the revocation as narrowly as possible.

## LICENSE ELEMENTS

Each content protection solution within the aforementioned framework comprises an adopter’s license, which is a technology license between the purveyor of the given content protection technology and manufacturers who want to include support for the technology within their products. Requiring adopters to enter a license as a condition of implementing the technology is important to maintaining the overall integrity and effectiveness of the content protection solution. Note that the adopter’s license is complemented by additional licenses between the technology licensor and content providers and others, such as a “content participant agreement.”

Apart from language covering confidentiality, intellectual property mutual non-assertions, payment of fees, disclaimers, liability, termination, remedies, etc., an adopter’s license contains special provisions in the following areas:

- *License grant.* A license to patents, trade secrets, and copyrights associated with the technology is granted to adopters only for the purpose of implementing the technology in a manner consistent with the specification and the other terms of the license, which

includes the robustness and compliance rules. Designing and manufacturing a circumvention device under the license is strictly prohibited.

- *Specification changes.* The licensor may make certain changes to the specifications and license documents at the request of adopters, content providers, or on its own initiative. Before doing so, consideration of factors such as the integrity, security, and commercial viability of the content protection solution, and whether such changes would impose additional substantial obligations on adopters, is undertaken. Notice and comment opportunities are provided for content companies participating in the particular technology to allow any concerns about possible adverse effects on content protection to be known and, if the concern remains at the time a change is actually to be made, to allow a neutral arbitrator to determine whether a particular change would actually have a negative effect on content protection.
- *Third-party enforcement.* Content industry companies that have entered into a license agreement with the licensor have a strong vested interest in ensuring the integrity and viability of the content protection solution. These companies are typically given the ability to seek injunctive relief from adopters who are in violation of provisions of the license that directly relate to the effectiveness of the technology.
- *Revocation.* Renewability of the content protection technology is important to maintain its effectiveness. To ensure that devices are only revoked under the specified circumstances described above, a process is provided for consulting with the manufacturer whose device is proposed for revocation. If there is any disagreement about whether the conditions for revocation have been met, arbitration is used to establish the facts and resolve the dispute according to the established process.
- *Compliance rules.* Compliance rules are technical documents embedded within the license that specify when and how subsequent protection technologies are to be applied to protected content that is output or stored. Compliance rules may also include requirements such as the encoding and carriage of Usage States, response to watermarks at unprotected inputs to the device, and limitations on the number or quality of permitted copies of protected content.
- *Robustness rules.* Like the Compliance rules, the Robustness rules are a technical description of how products must be designed and manufactured to make reverse engineering or other modification difficult.

Typically there are separate rules for software and hardware implementation styles. For instance, software requires integrity verification mechanisms, such as signed code. Mechanisms to hide or obscure the operation of code and any secrets contained within may also be required. Hardware rules may require that implementations hide secret values and algorithms, by, for example, embedding them in silicon. Furthermore, products should be designed such that attempts to modify or otherwise tamper with them will likely result in the device being rendered unable to access protected content. Regardless of the implementation style, there are clear prohibitions against incorporating “defeating functions” that would enable a consumer to trivially disable any of the protection for the content. As well there are requirements to keep confidential information secret and to prevent access to the protected content when it traverses busses within the device. For all of these requirements, the levels of threat that must be resisted are described in terms of the types of tools and the skill level of the hacker.

**CONTENT PROTECTION CHAIN**

The license structure described above enables the formation of a “chain” of solutions for protecting content on an end-to-end basis as it is transferred, stored, managed, and consumed on entertainment devices within the home. Various technologies may be available for any particular part of the “chain” and may be selected according to device capability and application. Figure 3 shows an example, using representative content protection solutions, two of which are described in this paper.

Here, content is delivered to the home in an encrypted form via a conditional access technology. Products such

as a set-top box that are designed and equipped to access this content must be licensed in order to receive the keying material necessary to decrypt the protected content. One of the terms of the conditional access license is that subsequent output of content that is subject to that license must be protected by an approved technology. In this example, the set-top box uses Digital Transmission Content Protection (DTCP) on IEEE 1394 interconnects.

In like manner, a recorder receiving content via the IEEE 1394 interconnect must be licensed if it is to decrypt DTCP protected content. One of the terms of the DTCP license is that exchangeable copies of copy-one-generation content that is subject to that license must be protected by an approved technology. In this example, the recorder uses Content Protection for Recordable Media (CPRM) to protect such copies on writeable DVD formats. Note that the DTCP license also includes provisions for making copies of content subject to that license that are uniquely associated with the licensed product (e.g., time-shifting on a local hard disk drive). Such localized copies must be protected to prevent further copying or playback on another device, using a method that meets the robustness rules of the DTCP license. One suitable method for such local protection may involve encrypting the content using an unpredictable key that is unique to the device.

For a product to play back the exchangeable DVD copy previously mentioned, the product must be licensed in order to decrypt the CPRM-protected content. In this example, that licensed product is a software application running on a personal computer equipped with a DVD drive. Thus, the chaining process is iterated until the content is ultimately consumed at the final device in the chain.

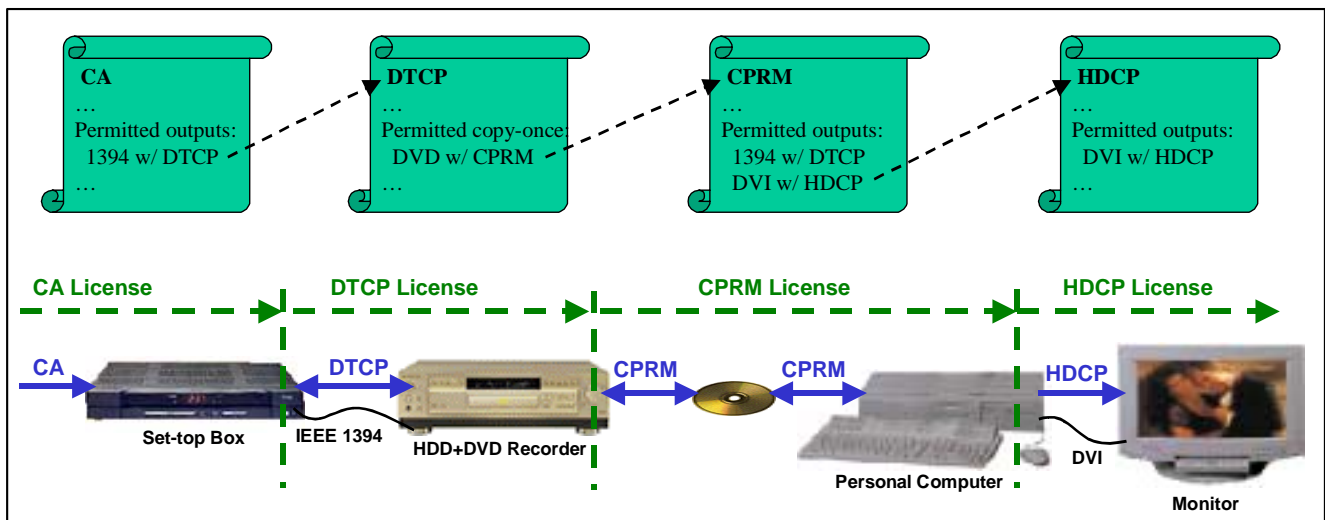


Figure 3: Content protection chain example

## EXISTING SOLUTIONS

This section describes two existing solutions that operate within the framework described above:

- Content Protection for Recordable Media (CPRM)
- Digital Transmission Content Protection (DTCP)

### CPRM

CPRM was developed by IBM, Intel, Matsushita and Toshiba (collectively, the “4C”). It provides a robust and renewable method for protected exchange of content via storage on portable/removable recording media. To date, CPRM has been defined and licensed for use in protecting content in a number of formats stored on a number of physical media types. These include DVD formats, SD Memory Cards, and Secure CompactFlash.

There are two primary technical components of CPRM: the C2 cipher and the Media Key Block.

C2 is a 10-round Feistel network block cipher with a 64-bit block size and a 56-bit key. The 4C companies designed and adopted C2, despite general cryptographic design principles which encourage use of well-known and well-evaluated ciphers, since no “well-known” alternatives had been identified that provided the necessary balance between suitability of hardware and software implementation, minimal licensing fees, and the ability to exclusively license C2 for use in 4C content protection solutions. This last attribute is particularly important, as circumvention of the 4C technologies will likely require use of the C2 cipher algorithm, which must

be licensed from 4C. The C2 cipher is used to both encrypt and decrypt content and also as the basis of one-way and hash functions. Also, a license is now available for certain “stand-alone” uses of the C2 cipher (see the C2 License at <http://www.4Centity.com> for details).

Media Key Blocks (MKBs) are tables of cryptographic values that implement a form of broadcast key distribution, and they provide for renewability in 4C content protection solutions. MKBs are generated by the 4C Entity, LLC, and enable compliant licensed products to calculate a common “media key.” Each licensed product is given a set of “device keys” when manufactured (also provided by the 4C Entity, LLC), which are used to process the MKB to calculate the media key. Device key sets may either be unique per device, or used commonly by multiple devices (4C licenses describe the details and requirements associated with these two alternatives). If a set of device keys is compromised in a way that threatens the integrity of the system, updated MKBs can be released that cause the compromised set of keys to calculate a different media key than is computed by the remaining compliant devices. In this way, the compromised device keys are “revoked” by new MKBs. In existing 4C solutions, MKBs are carried on compliant portable storage media, and devices use the corresponding medium’s key as the basis for encrypting and decrypting protected content stored on that medium.

Figure 4 provides an illustrative example of CPRM being used to protect video content stored on writable DVD media. Note that this figure provides a simplified overview; for complete details see the CPRM technical

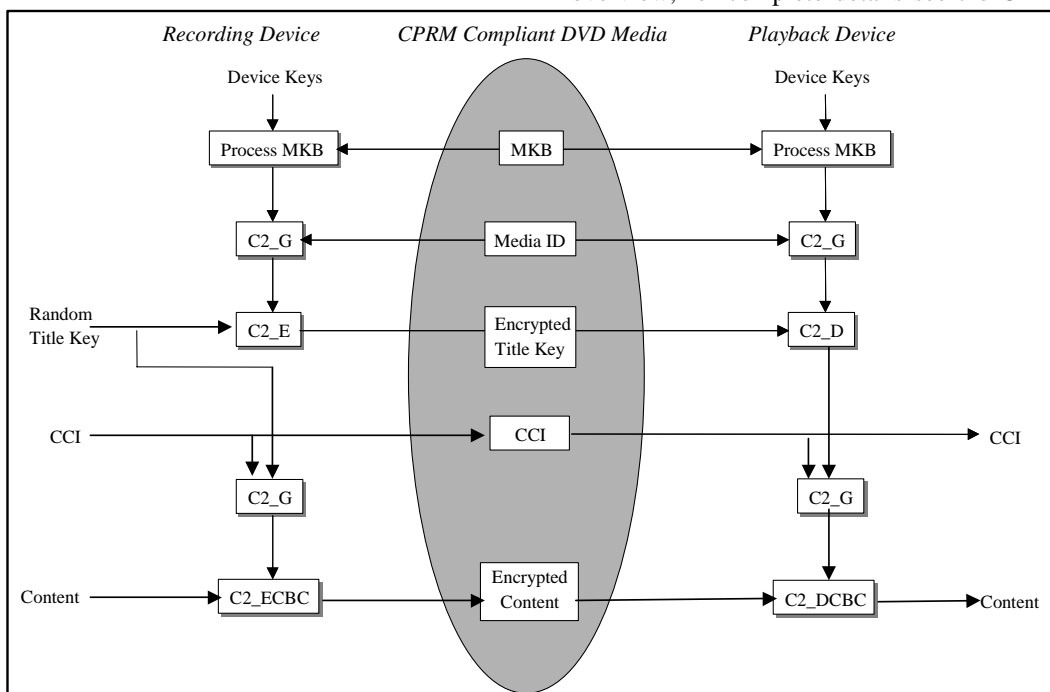


Figure 4: CPRM operation

specifications [www.4centity.com](http://www.4centity.com)

Each writable DVD disc that supports CPRM carries a Media Key Block (MKB) as read-only data stored in the lead-in area and a unique media identifier (Media ID) stored in the burst-cutting area, a region that is uniquely written on each disc in a manner that cannot be recorded or modified with consumer DVD equipment. A DVD recorder (e.g., stand-alone recorder, or software application running on a PC) that is equipped and licensed to use CPRM makes a permitted copy onto such a disc in the following manner. The recorder reads the MKB from the disc, and uses its secret Device Keys to process the MKB and calculate the Media Key. The Media Key is then combined with the Media ID, using the C2 One-way Function (C2\_G), to form a Media Unique Key. The Media Unique Key is used to encrypt a randomly generated Title Key using the C2 cipher encryption function C2\_E, and the encrypted value is stored on the data area of the disc. The Title Key is also combined with the content's Copy Control Information (CCI) using the C2 One-way Function (C2\_G), and the result is used as a key to encrypt the content using the C2 cipher in cipher block chaining mode, a function denoted as C2\_ECBC.

Thus, the content is encrypted in a manner that cryptographically "binds" it to that particular disc, through the use of the unique Media ID. The protected content can be played back from that disc by any compliant player that is equipped and licensed to use CPRM. Such a player uses its Device Keys and the relevant C2 decryption functions to carry out the corresponding playback process, as shown above.

The following subsections describe various physical media and content formats for which CPRM is currently defined and licensed. It is anticipated that CPRM will be applied to additional formats in the future.

## DTCP

DTCP was developed by Hitachi, Intel, Matsushita, Sony, and Toshiba (collectively, the "5C"). DTCP provides system renewability as well as an encrypted exchange of content and CCI between authenticated devices. To date, DTCP has been defined and licensed for use in protecting the transmission of content via the IEEE 1394 serial bus (1394), the Universal Serial Bus (USB), and the Media Oriented Systems Transport (MOST), which is used in the automotive sector.

CCI is carried embedded in the content stream according to the content format (e.g., MPEG). For instance an MPEG-2 transport stream descriptor has been defined to carry this CCI. In addition, the CCI is mapped into an

Encryption Mode Indicator (EMI) that provides protected, yet easily accessible, access to the CCI.

Content is encrypted using the M6 block cipher that is used in converted cipher block chaining mode with 56-bit keys.

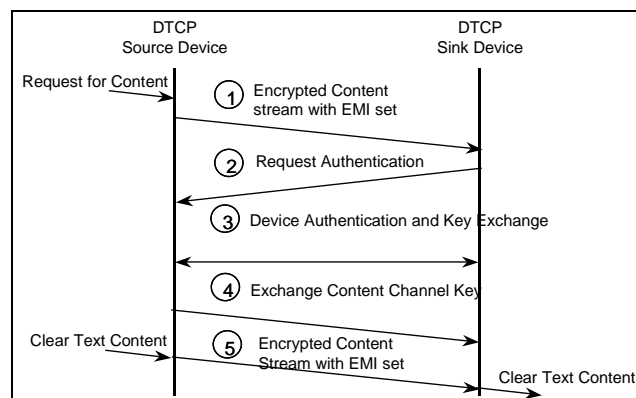
Two authentication and key exchange (AKE) procedures based on challenge/response procedures are defined to enable manufacturers to trade off implementation complexity versus value of content to be handled:

Full Authentication (for all content) is based on Digital Signatures and Diffie-Hellman Key Exchange using a 160-bit elliptic curve public-key cryptosystem compatible with IEEE P1363.

Restricted Authentication (acceptable for "copy\_once" and "copy\_no\_more" content only) is based on shared-secret techniques.

System renewability is provided through device certificate revocation. The license administrator can, under a rigorously specified set of conditions, exclude individual, compromised devices from participating in the protection system with devices supporting Full Authentication. Revocation lists are carried in System Renewability Messages that are distributed with content and between compliant devices.

Figure 5 shows an overview of the operation of the content protection system. The device that is the source of protected content has been instructed to transmit the content via the IEEE 1394 serial bus isochronous transport.



**Figure 5: DTCP operation**

*Step 1:* The source device is requested to initiate the transmission of a stream of protected content. The embedded CCI of the content is examined to determine the appropriate EMI value (e.g., "copy\_once," "copy\_never," or "copy\_no\_more") to associate with the encrypted content stream. The source device may choose to transmit an empty content stream until at least

one device has completed the appropriate authentication procedure.

*Step 2:* Upon receiving the content stream, the sink device inspects the EMI to determine the copy protection status of the content. If the content is marked “copy\_never,” the sink device requests that the source device initiate Full AKE. If the content is marked “copy\_once” or “copy\_no\_more” the sink device can request Restricted AKE if Full Authentication is not available. If the sink device has previously performed the appropriate authentication, it can immediately proceed to Step 4.

*Step 3:* When the source device receives the authentication request, it proceeds with the type of authentication requested by the sink device, ensuring that Full AKE is performed if the content is marked “copy\_never.”

*Step 4:* Once the devices have completed AKE, the keys required to access the encrypted content stream are exchanged between the devices.

*Step 5:* Encrypted content flows between the devices.

The application of DTCP is not limited to 1394, USB, and MOST. It is suitable for use with any digital interconnect that supports bi-directional communications. With the emergence of wired and wireless IP networking technologies within the home environment, including Ethernet and 802.11 wireless solutions, efforts are currently underway to add DTCP support to that infrastructure. The principal challenges

associated with this mapping are to constrain DTCP protected content to the home and personal network space and prevent anonymous, “hot-spot”-based sharing of content.

## CONCLUSION

Figure 6 shows an example of end-to-end protection within the digital home, using representative existing content protection solutions.

The strength and completeness of the end-to-end protection stems from an overall system architecture that ensures the individual technologies form a protected whole. Intel is promoting the development of a comprehensive, compatible content protection system, because it will benefit content owners, content providers, device manufacturers, and above all, consumers. Consumers are demonstrating a growing desire to move digital content among devices such as personal computers, DVD players, set-top boxes, and digital televisions. A variety of content protection technologies have been developed to protect digital content within each of these devices. Chaining these point solutions together will enable digital content usage throughout the home, maintain the integrity of the content, and minimize implementation burdens on developers.

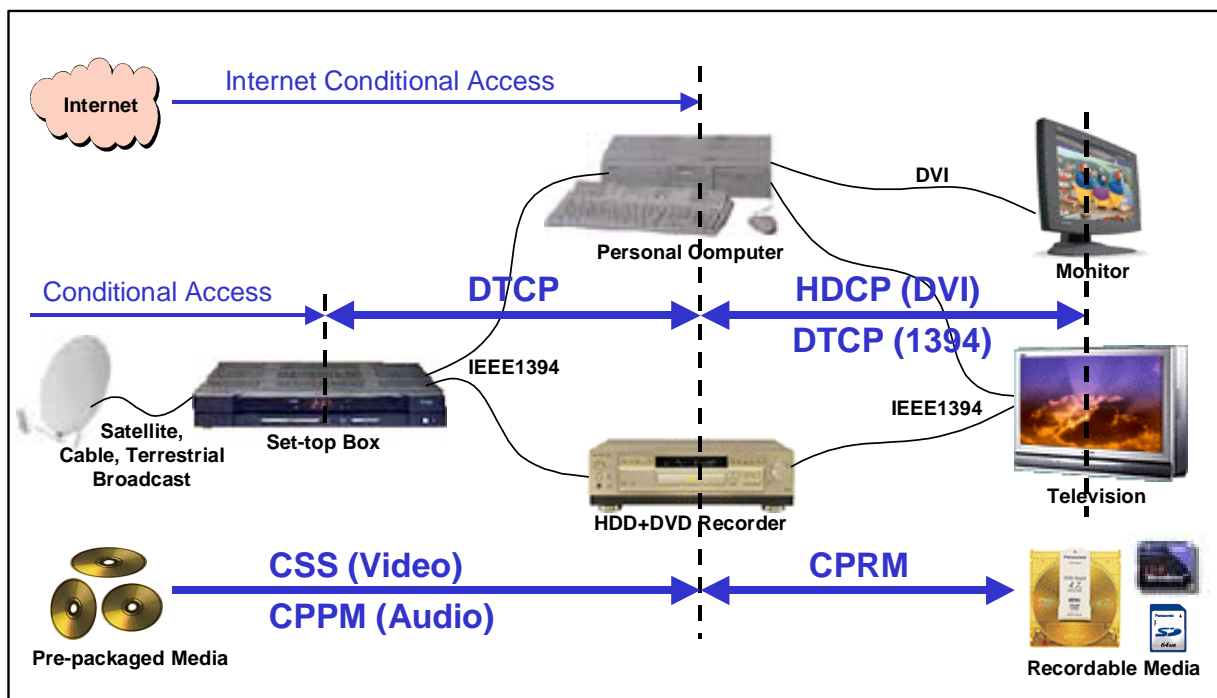


Figure 6: Example of end-to-end content protection

## REFERENCES

- [1] C. Brendan Traw, "Protecting Digital Content within the Home," *IEEE Magazine*, October 2001, pp. 42-47.
- [2] Bloom, Cox, Kalker, Linnartz, Miller, and Traw, "Copy Protection for DVD Video," in *Proceedings of IEEE*, Vol. 87, No. 7, July 1999, pp. 1267-1276.
- [3] Marks and Turnbull, "Technical Protection Measures: The Intersection of Technology, Law, and Commercial Licenses," *Workshop on Implementation Issues of the WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty*, World Intellectual Property Organization, Geneva, Switzerland, 1999.
- [4] Lotspiech, Nusser, and Pestoni, "Broadcast Encryption's Bright Future," *IEEE Computer*, Vol. 35, No. 8, August 2002, pp. 57-63.

## AUTHORS' BIOGRAPHIES

**Michael Ripley** is a Staff Engineer within Intel's Corporate Technology Group. He joined Intel in 1995, and during the past several years has been the technical lead on a number of Intel's content protection efforts, including development of CPPM for DVD-Audio and CPRM for several formats. Mike is the recipient of various awards, including the Intel Achievement Award. His e-mail address is [michael.ripley@intel.com](mailto:michael.ripley@intel.com).

**C. Brendan S. Traw** is a Senior Principal Engineer within Intel's Corporate Technology Group. His current focus is on the management and protection of entertainment content within emerging digital environments. He has lead the development of industry-leading content protection solutions including DTCP for digital networks, HDCP for DVI, CPPM for prerecorded DVD Audio, and CPRM for various recordable media formats. Brendan is the author of over a dozen papers and book chapters and has received eight US patents. He received a Ph.D. degree in Computer Science from the University of Pennsylvania. His e-mail address is [brendan.traw@intel.com](mailto:brendan.traw@intel.com).

**Stephen Balogh** is a Business Development/Marketing Manager within Intel's Corporate Technology Group. He has an extensive background in establishing, growing, and managing content protection technology licensing and key generation infrastructures. Steve has held leading positions in CP technology diffusion efforts including President of the Digital Content Protection LLC, President of the Digital Transmission Licensing Administrator LLC, Manager of the DTCP Key generation facility, and he is presently Intel's Steering

Committee member for the DVD Forum. His e-mail address is [stephen.p.balogh@intel.com](mailto:stephen.p.balogh@intel.com).

**Michael Reed** is a Marketing Director within Intel's Corporate Technology Group. He has 16 years of marketing experience within the technology industry. Michael joined Intel in 2000. Prior to that he was the Vice President of Marketing for Diamond Multimedia's Rio Division, makers of the industry-leading Rio digital audio player. Michael holds a B.S. degree in Computer Science from Bowling Green State University and an MBA degree from the University of Oregon. His e-mail address is [michael.j.reed@intel.com](mailto:michael.j.reed@intel.com).

Copyright © Intel Corporation 2002. This publication was downloaded from <http://developer.intel.com/>.

Legal notices at <http://developer.intel.com/sites/developer/tradmarx.htm>.

For further information visit:

[developer.intel.com/technology/itj/index.htm](http://developer.intel.com/technology/itj/index.htm)