Intel® and DTCP*

Protecting premium content and its use in the digital home

The technology vision for the DTCP standard

Intel and four other companies developed the Digital Transmission Content Protection (DTCP) standards specification to provide protected digital entertainment in the home. Imagine never being able to record cable television on a digital video recorder (DVR) for later viewing. Or not being able to sign up for video on demand. Without DTCP, Hollywood studios and other content owners would have been reluctant to ever allow video on demand or pay-per-view digital movies, much less permit a DVR to receive digital television content. Their fear: piracy.

"The Congress shall have the Power to ... promote the Progress Of Science and useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries."
– United States Constitution, Article I, Section 8, ratified 1788 ... and just one example of many national laws around the world protecting artistic works.

DTCP defines a cryptographic protocol for protecting audio/video entertainment content from illegal copying, intercepting and tampering as it traverses digital interfaces such as IEEE 1394, Universal Serial Bus (USB*) and IP-based home networks. Transparent to consumers, DTCP allows people to enjoy high-quality digital pictures and sound without any noticeable performance or quality impact.

DTCP was jointly produced by five member companies — Hitachi, Intel, Matsushita (MEI, also known in the U.S. as Panasonic), Sony and Toshiba — as an outgrowth of the Copy Protection Technical Working Group (CPTWG). These companies are informally known as "the five companies" or the "5C."

As part of this group, Intel had three goals in creating a protected digital environment for the home network:

1. Enable consumer choice, content portability and flexibility in the digital media experience.
2. Protect the rights of content providers and content owners, recognizing their right to be compensated for their intellectual property.
3. Make content protection simple and inexpensive to deploy for PC and consumer electronics (CE) manufacturers.

Today, these goals face new challenges as content protection moves from wired to wireless devices. The advent of the digital home is increasing the number and diversity of devices that can record and share digital content.

"No person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof, that is primarily designed or produced for the purpose of circumventing a technological measure that controls access to a (copyrighted) work."
– U.S. Digital Millennium Copyright Act, Section 1201, signed into law October 1998

What's more, people continue to demand the ability to download content and play it back on the device of their choice — whether it's a personal DVD player, a desktop PC, a television, or all three of these devices. Through VCRs and audio tape players, people have come to expect this kind of freedom.

To enable such freedom while preserving content copyrights, Intel continues to collaborate with other members of the 5C to promote the newest DTCP specification — Digital Transmission Content Protection over Internet Protocol. DTCP-IP is designed to protect premium content as it moves across the wireless local home network. Intel sees this technology as crucial to its vision of the digital home.

Intel's early recognition of the need for DTCP

In the mid-1990s, Intel worked with the CE industry and content owners on modifying the Content Scramble System (CSS) for DVD video to enable DVDs to play on Intel® platforms. From this experience came a key

learning. To protect digital works (for example, premium content available on digital media), copy protection had to start from the source. The solution wasn't going to come from a downstream, after-the-fact technology, but from a solution that involved the content owner as well. CSS was an obvious example. CSS protection is applied to the original content before it is stamped on the DVD.

Around this same time, Intel and other companies realized the need for a digital interface between devices that would enable transfer and playback of digital media without conversion back to analog format. Analog conversion undermined a key digital advantage — the ability to preserve the quality of the content on an end-to-end basis. What was needed was a digital interface so digital devices could transfer and output digital media as digital media. A digital video camera, for instance, needed a way to exchange digital content directly with a computer or monitor.

"People get more satisfaction from their computers when they can show beautiful motion pictures than when they can't. The people that make the most beautiful motion pictures are in Hollywood and other world-renowned film centers. So you have to be able to show those pictures on a PC."
– Michael Moradzadeh, former Intel Director of External Legal Relations and former Chairman of the 5C

One of the first solutions for this interface was IEEE 1394, also known as FireWire*, and Sony i.Link*. USB and USB2 solutions soon followed. These digital interfaces were great for preserving the quality of content as it was transferred from one device to another. But these interfaces also created a need for a new content protection solution that could safeguard the data streams transmitted over them. Content owners were rightfully concerned that the new unprotected digital outputs would enable pirates to hijack a digital data stream and create an unlimited number of perfect copies.

Copy protection wasn't as great an issue during the heyday of VHS. That's because video quality degrades quickly as content is copied from one cassette to another. After several generations, the quality is generally so bad no one is interested in copying it anymore. Digital media, on the other hand, makes a perfect copy every time through countless generations.

The origins of DTCP

Recognizing the piracy threat presented by digital interfaces, Intel and other members of the Copy Protection Technical Working Group (CPTWG) began to look for a copy protection solution for these interfaces. They formed the Digital Transmission Discussion Group (DTDG). This group quickly discovered each of the industries — CE, PC, and content owners — had their own perspective. A co-chair governance was set up with one chair held by a CE/content owner (Sony) and the other by a representative of the PC industry (Intel®). The group issued a call for proposals and 11 suitable proposals came in.

Two types of solutions were proposed. The first were hardware-based solutions like the Smart Card* technology used by satellite and cable systems. Smart cards though were seen by many as an expensive and unwieldy solution. Wherever the content went, the Smart Card would have to go as well. There would have to be a Smart Card in your set-top box, in your PC, in your personal video recorder, and in your DVD recordable player.

Other proposals focused on other ways to use encryption or cryptography to control usage as content moved from one device to another. Intel, Toshiba and other companies each offered solutions. A period of vigorous debate followed with the 11 proposals going forward independently, including Intel's. Toshiba, believing the only way to forge a successful solution was to bring CE and PC interests together, approached Intel about a combined proposal.

"In those initial meetings, it became very apparent the large gulf between the PC industry and what the PC was capable of and what consumer electronics devices were capable of ... you end up in a situation where you have to design to the lowest common denominator. That is, you need to design your solutions to basically work with every product, even the least capable ones."
– Brendan Traw, Intel Fellow, Director, Content Protection Architecture

Intel had decided copy protection shouldn't be implemented in hardware — an approach that would require platform changes. Instead Intel proposed a software solution that would be clad with "tamper-resistant" software to provide protection for the implementation.

In a way, it's surprising a company known for its silicon would suggest a software solution. But Intel knew a major objective for CE companies was for the solution to be extremely lightweight and inexpensive. CE devices can range hugely in price, from an inexpensive digital recorder for kids to a $5,000 home theatre system. Consequently, any copy protection solution had to work for the cheapest device and add practically nothing to its price.

Beside Intel's and Toshiba's alliance, other groups began to form between DTDG members. Hitachi, Sony and MEI created a merged proposal and presented a formidable coalition as well. In addition, six other miscellaneous proposals were floating around, each trying to build a coalition of companies behind them. Following a series of discussions with Intel, both Hitachi and MEI switched allegiances to help Intel and Toshiba develop a technology based on their proposal. Sony joined soon after, creating critical mass.

The CPTWG decided not to endorse specific solutions, but only provide a forum for discussion. This was a wise move. It avoided fallout within the CPTWG based on any specific endorsement of a technology and left the success of a given solution to the marketplace. The 5C went to work on theirs.

Building a content protection solution from scratch is no easy task

It was one thing to finally reach agreement on a specific solution among the 5C, quite another thing to draft a DTCP specification, develop a licensing process, and build the public key cryptography infrastructure necessary to implement it.

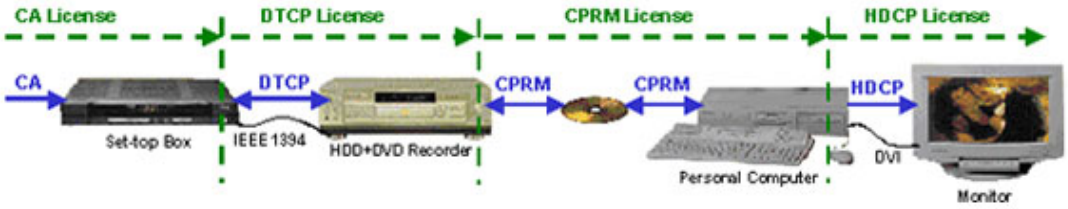
An immediate concern was that content owners might want to prevent all copying and mark everything "copy never." This would defeat most of what the PC and CE industry were trying to do and, most importantly, frustrate the consumer. Consumers expected DVD and digital recording technologies to perform just like VCRs and tape recorders. They expected to be able to make reasonable use of content, including making copies of content. Consequently, part of the initial work was figuring out what kinds of content should be marked "copy never," "copy one generation," and "copy freely." The 5C began work to strike policy and legal agreements that would define and enforce the use of DTCP. An organization for handling all these policy and licensing issues was created. This organization, the Digital Transmission Licensing Administrator, is a limited liability corporation charged with licensing and administering the DTCP technology.

The DTCP specification relies on strong cryptographic technologies to provide flexible and robust copy protection across digital buses. These cryptographic techniques have evolved over the past 20 years to serve critical military, governmental and commercial applications. They have been thoroughly evaluated by hackers and by cryptographic experts, and have proven their ability to withstand attack.

Concurrently, the 5C also set up a public key infrastructure. Under DTCP, every device would require its own unique key sets. The generation, storage and assignment of these keys required a central, highly secure repository. Having a third-party vendor handle the repository would have added too much cost to the end solution. Consequently, Intel stepped in. Intel wrote the software, created the policies for the key generation, procured the equipment, and built a key generation and signing facility from scratch at an Intel site. The result was that Intel and the 5C managed to develop a world-class cryptography specification, create a licensing entity, and build a key generation facility that is the flagship for all devices implementing DTCP. Today, this is one of the world's highest volume key generation facilities.

"For the people who had to implement it, we had to create a set of robustness and compliance rules. You can create a very secure lock, but if people do sloppy implementations, or don't follow the rules of how content should be treated, you've got the lock, but it's mounted on a paper door."
– Stephen Balogh, Business Development Manager, Intel® Corporation; President, Digital Content Protection LLC

Intel's next task was developing an actual implementation of the DTCP specification. Such implementations are vital for finding the ambiguities, contradictions and bugs in a specification. Intel's DTCP implementation validated the specification, enabled key improvements, and provided a reference platform for interoperability testing. Intel's implementation became the gold standard — the one everyone used to test their implementations.



Getting content owners on-board

"Having Warner Brothers and Sony Pictures agree and endorse DTCP technology was a really critical milestone that gave implementers the full confidence that this is a solution that ultimately would be acceptable to Hollywood."
– Brendan Traw

It was one thing to create the DTCP technology, quite another to get content owners — such as Hollywood studios — to use it. In late 1998, the technology was available, licensable, and the first products with it were beginning to appear, albeit just a few. The studios, having the most to lose from piracy, were wary of allowing any copying at all. Intel and the 5C began an intense negotiation process over several years that culminated in Warner Brothers and Sony Pictures signing a content participant agreement in 2001. This was a critical milestone, demonstrating that DTCP could and would appeal to content owners. Having two studios as vocal advocates of the technology was sufficient to move it forward. In part because of this studio support, DTCP is one of the few solutions of its kind that today is actually shipping products. Studio support of DTCP also helped the 5C gain interest and support from organizations such as Cable Television Laboratories, Inc. (CableLabs) — a nonprofit research and development consortium dedicated to helping cable operators integrate new cable telecommunications technologies.

Protecting digital broadcast

The coming of digital terrestrial broadcast helped further launch DTCP into prominence. Digital terrestrial broadcast is transmitted "in the clear" (unencrypted) and thus can't be protected at the source. Consequently, unless the receiving unit for a digital broadcast signal encodes the content with an appropriate protection scheme, digital broadcasts can be freely copied or traded via an Internet file-sharing service.

Without protection, major content owners and producers balked at broadcasting programs digitally. Yet Intel and the rest of the industry viewed digital broadcast as the wave of the future. It offered consumers a higher quality picture, plus required less broadcast spectrum, ultimately freeing spectrum for new uses. Consequently, digital broadcasting was in the best interest of consumers, the CE industry, and the Federal Communications Commission (FCC). In reaction (and to protect their property), broadcasters and content producers pushed the FCC to mandate a system that would place an identifying packet inside a broadcast signal — a broadcast flag — to alert properly enabled devices to restrict the unauthorized retransmission of a program over the Internet.

DTCP works in conjunction with other content protection schemes like CSS. Before allowing data to move through a digital output to a receiving device, DTCP requires the devices to first perform a joint authentication procedure. This authentication consists of a sequence of data swaps and key calculations that validate the licenses of both devices. This prevents pirates from inserting a circumvention device that would record a copy protection data exchange or strip out the protection.

In August 2004, the FCC approved 13 technologies as appropriate for use in digital TV (DTV) reception equipment to give effect to the broadcast flag. DTCP was one of the approved technologies, and the only publicly offered output protection technology that permits copying over several interfaces. DTCP has also been tasked with safeguarding the IEEE 1394 interface of digital receivers (including cable and satellite set-top boxes) to prevent illicit duplication of copyrighted programming.

The "public" nature of DTCP is something that should be noted. The 5C felt that although content protection provided a springboard for content owners to release more high-value digital content and develop new

business models, content protection was not a product feature that could be marketed to consumers. The 5C believed it was more valuable to consumers and to the relevant industries to enable new markets for digital services and products than to charge market-rate royalties for their intellectual property in DTCP.

"While content protection ultimately can benefit consumers because it stimulates content providers to make their content available in digital form, content protection also imposes restrictions on what consumers can do. Consequently, consumers will never see content protection as a benefit that they would be willing to pay for."
— Seth Greenstein, partner at law firm McDermott Will & Emery (represents Hitachi for 5C)

The 5C also felt that if they didn't charge market rate royalties for their intellectual property, it was only fair that licensees also agreed not to assert their own patent portfolios against other licensees as a condition for licensing the technology. This is called a "non-assert" clause. This meant that any company that licensed DTCP had to agree, consistent with the 5C philosophy, to neither make a business out of their patent portfolios nor create a profit-producing license pool. Intel and the 5C dedicated substantial efforts, against a few but fervent competitors, to convince the FCC to preserve use of DTCP as a broadcast flag technology under the 5C "non-assert" structure. The 5C took the position that if companies wanted to create and license a competing proprietary solution for profit they could. DTCP has continued to prevail.

DTCP-IP ... the big bang?

One of the most important extensions of DTCP technology was support of IP-based networks. In 2001, Intel recognized that home networks were moving toward IP and began working with the 5C to map DTCP to IP-based networks. This is an exciting new direction. As IP networks spring up in the home and people move to new broadband content sources, companies like Movielink and CinemaNow that offer digital content over the Internet are growing quickly in popularity. These developments, combined with all the existing sources of content (cable, satellite, terrestrial broadcast, and physical media such as DVDs) are propelling the use of DTCP. What's more, in the digital home, DTCP-IP makes the perfect common denominator for protecting content as it is exchanged from one device to another, such as from a desktop PC to a DVR connected to a TV. Whether the connection is wireless, USB, IEEE 1394, or Bluetooth* technology, DTCP can maintain the source's content usage policies. Consequently, DTCP is favored to appear in an ever-growing number of devices.

"DTCP's natural evolution has been to become the common denominator to the numerous and disparate digital rights management (DRM) and content protection solutions that bring content into the home. DTCP was designed to work between the most competent and complex devices and the simplest devices on the home network, making it a lingua franca of content protection solutions."
– Stephen Balogh

To serve as this common denominator in the home, Intel had to work out an interesting localization problem: How do you determine whether or not a DTCP device is communicating with a device within the same home rather than a neighbor's device or something across the country? Intel, with the 5C, developed a number of solutions. One was a limitation on how many routers an IP packet can travel before being eliminated. Another was a "round-trip timer" that measures the latency between the source and receiving devices. If the latency period is too long, then the exchange isn't permitted because the receiving device is probably outside the home.

Key learnings

The development of DTCP brought Intel deeper into the worlds of CE and the content industry than it had ever gone. Through this process came a lot of key learnings about the different interests of the respective industries and their common ground. Some of these learnings are summarized here.

1. **Successful negotiations require appreciation of the mindset of all parties.** It was obvious from the start that the PC and CE industries worked differently. While the PC industry is competitive and driven by cost, the CE industry is cost-sensitive to a degree even the PC industry has trouble understanding. CE companies count every byte of memory, whereas the PC industry starts with megabytes. Objectives, timing and risks also all vary from one industry to another. Consequently, it's vitally important to understand where the other side is coming from and offer alternative solutions acceptable to all parties.

2. **The lifespan for intellectual property is very different in the PC and content industries.** In both the PC and content industries, high value is placed on intellectual property, but in the PC industry the products are more ephemeral. Take software. Within a few years, a new version is released and the prior release is fairly irrelevant. Software is much more about the evolution of a product, and in a way, this perpetual obsolescence helps protect it against piracy. In the case of a motion picture, such as "Casablanca," there is no obsolescence. Made in 1942, "Casablanca" 60-plus years later remains the same and still retains the same value it has always had. In the end, Ingrid Bergman still gets on the plane. The content never changes. And piracy severely threatens its value. Consequently, those in the PC industry have to take particular care to understand the attitude toward intellectual property by content owners.
3. **The product lifespans between the PC and CE are very different.** PC performance improves so much over several years that people are accustomed to regularly buying new computers. That's not true with the CE industry. People get angry when their 8-year-old VCR no longer works. People expect televisions to last 10 to 15 years. When CE products do get replaced, the replaced product often just moves to another place in the home. For anyone creating a content protection solution, this means any aspect of the technology that requires a presence in a CE device must have a long lifespan.
4. **The nature of PC and CE products are very different.** CE products have a fixed function. They're a TV set or a DVD player and that's all they do. Consequently, when the CE industry thought about content protection, they assumed all devices would be fixed function and that if there was a flag in a stream of content telling that product not to copy the transmission, it would not copy it. They weren't thinking about a PC which is programmable and could possibly be modified to ignore that flag. Intel brought this kind of thinking into the picture.
5. **Audio recording devices and VCRs have created certain expectations about listening and viewing content.** People expect to be able to record content, especially broadcast or cable content, for playback later at their convenience. In the end, all industries concerned will be better served if reasonable consumer expectations with respect to playback and recording are accommodated. This means implementing encoding rules that offer various levels of restrictions on content use rather than a blanket "no copy" rule.
6. **Copy protection isn't a product the industry should sell.** Copy protection simply enables cooperation between the various industries (PC, CE, content) in the delivery and consumption of content. Not every company in the CE or PC industry feels this way. Some see copy protection as a source of revenue. But by not making copy protection a profit center, product price points remain low, the industry avoids proprietary solutions not everyone can share, and everyone enjoys the broadest benefits (particularly in respect to interoperability, choice and price).
7. **To influence the direction a key technology takes, a company has to be willing to invest significantly in its outcome.** Obviously, to get something like DTCP off the ground and gain support for it from three industries is a tremendous undertaking. For Intel this meant developing the technology, the applications, and sample implementations. It meant building the key generation facility and undertaking its long-term maintenance. And it meant years of negotiating with and educating the entire ecosystem (CE, PC and content companies) on DTCP and its benefits.
8. **Content protection is 40 percent technology and 60 percent policy.** Intel learned it's very important to look beyond the engineering and consider the bigger societal issues at play. All parties needed to put their interests on the table and discuss solutions that made sense for everyone, particularly the consumer.

What lies ahead

Today, DTCP is the leading solution addressing content protection between devices in the digital home. Nearly a hundred companies have licensed it. Consumers can go into any electronics store today and find many products that support DTCP.

At the same time, there's much more work to be done. The next few years will see much more content come into the home through broadband and wireless technologies. What's more, many more devices will be available that can receive, store, exchange and play this content. It will be important to continue to build support for DTCP and DTCP-IP throughout the CE, PC and content industries. Intel will be working hard to keep the channels of communication open between all three industries and the respective needs of each industry in mind as we try through DTCP to deliver the best and broadest options for the use of digital media throughout the home.

Meanwhile, Intel is also involved in work on other content protection standards. Specifically for the digital home, Intel has:

- Participated heavily in the original CSS (DVD) content protection and playback structure.
- Developed the High-bandwidth Digital Content Protection (HDCP) specification for protecting digital entertainment content over the High-Definition Digital Multimedia Interface (HDMI) and Digital Visual Interface (DVI).
- Contributed to the Content Protection for Pre-Recorded Media (CPPM), a technology for protecting digital content on DVD Audio.
- Contributed to the Content Protection for Recordable Media (CPRM), a technology for protecting digital content on certain portable media formats such as recordable DVDs and SD Memory Cards.
- Helped draft the Content Protection System Architecture (CPSA) which defines an overall framework for integrating many of these technologies as well as new technologies as they emerge.
- Launched the formation of the Advanced Access Content System (AACS) a technology for managing content stored on the next generation of prerecorded and recorded optical media for consumer use with PCs and CE devices.
- Created the Content Management License Administrator (CMLA) in conjunction with Nokia, Panasonic and Samsung, to enable the rapid delivery of high-quality digital content to mobile handsets and other devices that deploy the Open Mobile Alliance (OMA) Digital Rights Management version 2.0 specification.