DIGITAL CONTENT PROTECTION

HDCP deciphered

White Paper

April 2008

Executive Summary

Audiovisual content, including movies and TV, is increasingly disseminated in digital form on the Web, as well as on physical media. As a result, content providers are using various content-protection technologies to prevent unauthorized uses. High-bandwidth Digital Content Protection (HDCP) protects the last stage in the distribution process, encrypting content transmitted over digital interfaces from set-top boxes, DVD players, personal computers and game consoles, to display devices such as high definition TVs. The consumer electronics industry has rapidly adopted HDCP for the High-Definition Mutlimedia Interface (HDMI). Manufacturers wishing to sell or distribute HDCP products must obtain HDCP licenses from Digital Content Protection (DCP), LLC., and are responsible for implementing products that meet the requirements of the HDCP License Agreement, Specification, Compliance Rules and Robustness Rules (Exhibit 1). DCP recommends implementers utilize HDCP authorized test centers to assist in meeting these requirements. This white paper describes the role of HDCP, how it protects content, and its use in different consumer devices. It also discusses HDCP licensing and product interoperability testing, and briefly outlines future developments.

Introduction

Audiovisual content, is increasingly being distributed to consumers in digital form—over the Internet, cable and satellite networks, and on media such as DVDs.

This widespread availability of digital content has made content providers increasingly concerned about unauthorized copying and use. As a result, content providers, media manufacturers and electronics manufacturers have implemented a variety of content-protection technologies that protect access to high-value content distributed via different media.

High-bandwidth Digital Content Protection (HDCP) is part of this chain of protection. It protects the last stage in the distribution process – the transmission of content from devices such as set-top boxes, DVD players, computers and game consoles over digital interfaces to display devices such as high-definition digital televisions (HDTVs). To protect this content, HDCP uses authentication and encryption techniques.

The consumer electronics ecosystem has rapidly adopted HDCP for the digital High-Definition Multimedia Interface (HDMI). Major manufacturers are incorporating HDCP into their products; roughly one billion HDCP device keys have been shipped to date.

Manufacturers require a license to implement the HDCP specification. The HDCP specification was originally developed by Intel Corporation and is licensed, under authorization from Intel, as a digital output protection technology for audio and audiovisual content. Digital Content Protection, LLC, an Intel subsidiary, is authorized to license the technology to manufacturers. HDCP Adopters or licensees must implement HDCP products that comply with the specification and license agreement and construct them so that they interoperate with other products over standard interfaces. Although not mandatory, DCP recommends manufacturers perform thorough testing of their HDCP products to properly meet these requirements.

This paper describes the role of HDCP, how it protects content, and its use in different consumer devices. It discusses HDCP licensing and product interoperability testing, and briefly outlines future developments.

HDCP's role in digital content distribution

Content protection technologies

Figure1 shows how HDCP fits into the overall content protection picture. A variety of technologies and standards have been developed to protect specific types of media, such as downloaded music and movies on Blu-ray discs. Each of these technologies hands off to HDCP for the last step: the transmission of the content via a digital interface to the display device.

For example, cable and satellite providers use conditional access technology to prevent unauthorized access to content as it is transmitted from the provider to a set-top box. HDCP then protects that content as it is transmitted from the set-top box to a TV. The role of HDCP is to prevent interception and copying or other unauthorized use of this bit stream.

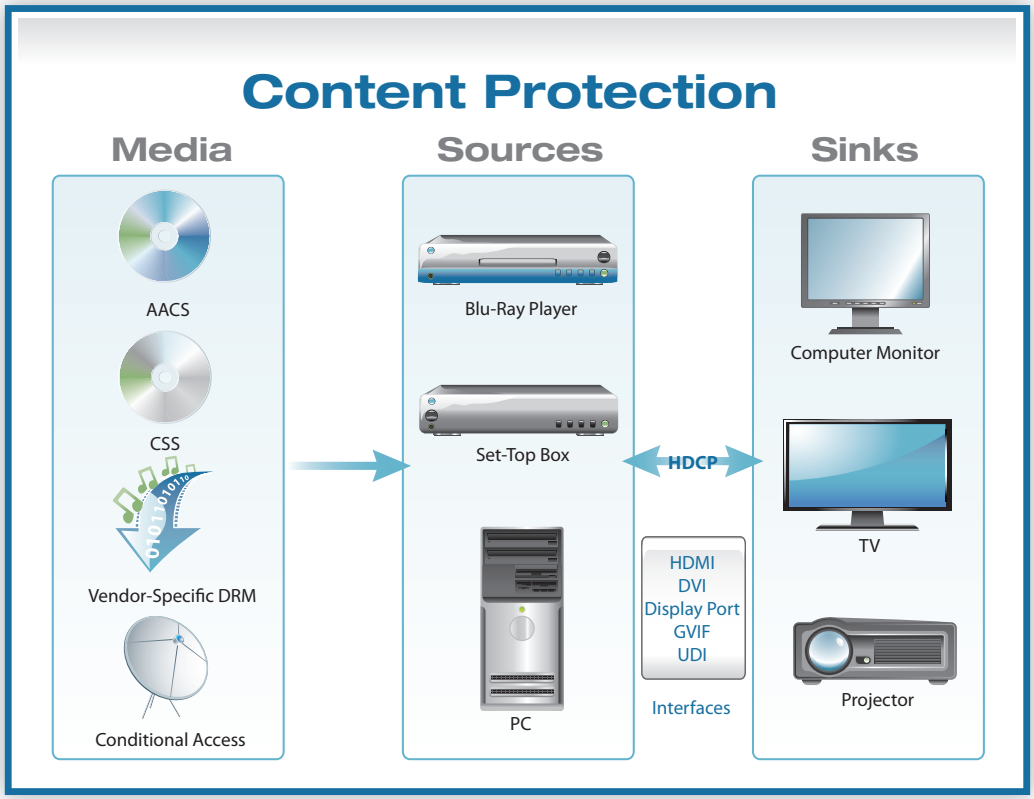


Figure 1.
The Content Protection chain.

Interfaces

HDCP operates entirely over certain digital interfaces, known as HDCP-protected interfaces, as shown in figure 1. Some upstream content-protection technologies, such as the Advanced Access Content System (AACS) used for Blu-ray discs, require all content transmitted over digital interfaces to be protected using HDCP.

HDCP does not protect content that is sent to TVs via traditional analog outputs; however, using analog outputs may mean losing desirable features, such as higher resolution, that are made available only via digital interfaces.

In this paper, we will focus on the use of HDCP over the High-Definition Multimedia Interface (HDMI). This digital interface has been very widely adopted by makers of HDTVs and other

consumer electronics devices. HDMI delivers high-definition video and multi-channel audio over a single cable using standard connectors.

HDCP may also be employed over several other digital interfaces, which currently are Digital Visual Interface (DVI), DisplayPort, GVIF (Gigabit Video Interface), DLI (Digital Light Interface), and UDI (Unified Display Interface).

What HDCP is not:

Content protection vs DRM

It's important to note a key difference between HDCP and other content-protection or rights management technologies. Content providers typically use a Digital Rights Management system (DRM) to protect their content. DRMs are designed to prevent unauthorized uses of the content and to permit other uses or impose other restrictions on such content. For example, a consumer may download a file containing music or video to a digital player. This content is protected by a DRM that controls what a user can do with that content. The DRM may control whether the user can make copies of the file or play the content on other types of devices, for example. HDCP is not a DRM. It performs a very specific role: to encrypt and protect content as it is transmitted as a stream of digital data for display.

HDCP in detail

Types of HDCP devices

HDCP-protected systems may include three types of devices: sources, sinks and repeaters. HDCP protects data as it is transmitted between each of these devices when they are connected via HDMI or other HDCP-protected digital interfaces.

Each device contains one or more HDCP transmitters or receivers, or it may contain both receivers and transmitters. Sometimes HDCP and HDMI functionality are combined into a single transmitter or receiver chip.

Source. The source sends the content to be displayed. Examples include set-top boxes, DVD and Blu-Ray players, and computer video cards. A source has only an HDCP/HDMI transmitter.

Sink. This sink renders the content for display so it can be viewed. Examples include TVs and digital projectors. A sink has one or more HDCP/HDMI receivers.

Repeater. A repeater accepts content, decrypts it, then re-encrypts and retransmits the data. It may perform some signal processing, such as up converting video into a higher-resolution format, or splitting out the audio portion of the signal. Repeaters have both HDMI inputs and outputs. Examples include home theater audio-visual receivers that separate and amplify the audio signal, while re-transmitting the video for display on a TV. A repeater could also simply send the input data stream to multiple outputs for simultaneous display on several screens.

For completeness, it is worth noting that home theater systems may also contain HDMI switches that select from multiple source inputs and forward the selected data stream via a single HDMI output. Most switches do not decrypt or encrypt content—they simply provide a way to link sources and sinks together; therefore they are not true HDCP repeaters. However, these switching functions may also be incorporated into true repeaters or into sinks.

HDCP usage scenarios

HDCP sources, repeaters and sinks may connect together in a tree-shaped topology with up to seven levels and 127 devices. This enables many different combinations of devices. Encrypted HDCP content flows through this topology over HDCP-protected interfaces.

Each encrypted HDCP communication takes place between a single transmitter and receiver. Several communication sessions may take place simultaneously within a tree; a source could be sending content to a repeater while the repeater is retransmitting the content to a display, for example. At any given moment, only one device within the topology is acting as a content source; however, multiple HDMI transmitters may be operating because repeaters are capable of sending this content to several different sinks.

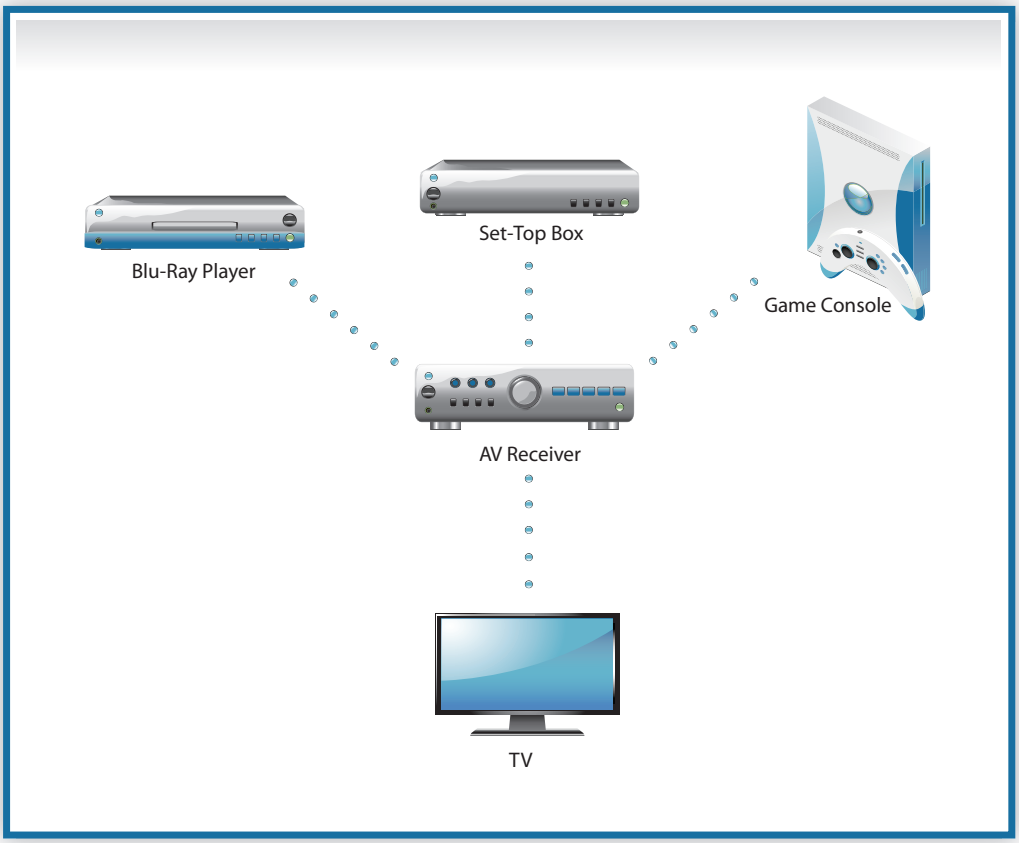


Figure 2.
A common home theater tree-shaped topology. Three sources (a Blu-ray player, set-top box and game console) are connected to a repeater (audiovisual receiver) which is connected to a sink (TV). All communication among the devices in the tree is protected by HDCP.

Some possible arrangements:

1. A TV (sink) connected to one or more sources. An example is an HDTV with four HDMI inputs. A consumer could connect one source, such as a Blu-ray player, satellite set-top box or game console, to each of these inputs. The consumer selects a single source and views the content via the TV,.

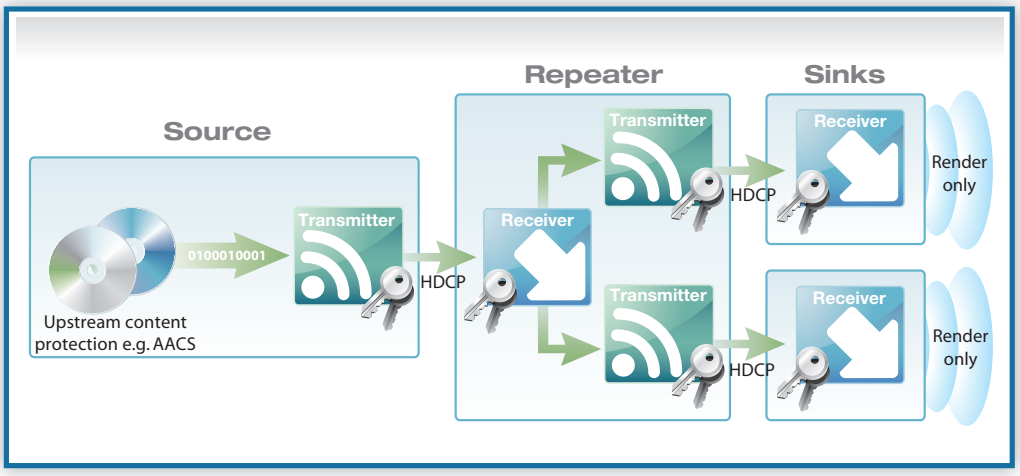
2. Multiple sources are connected to an audiovisual receiver, which acts as a repeater, as shown in figure 2. The receiver's output is connected to the sink (TV). In this case, the consumer uses the AV receiver to select the source. The receiver separates out the audio signal and amplifies it to deliver surround sound, and then transmits the visual content to the TV.

3. A sports bar has a single input, such as a digital broadcast of a football game, and wishes to display the content on multiple TV screens. The bar uses an HDMI repeater to do this. The repeater receives input from a single satellite box source and sends the content to multiple displays (sinks).

How HDCP works

HDCP protects content using authentication and encryption. Before sending HDCP-protected data, the transmitting device initiates an authentication process to confirm that the receiver is authorized to receive the data. Once the receiver has been authenticated, the transmitter encrypts the data stream to prevent eavesdropping and sends it to the receiver.

Figure 3.
HDCP tree showcasing receivers, transmitters and keys



Each HDCP transmitter or receiver includes 40 56-bit secret keys, known as Device Private Keys, as shown in figure 3. These keys, provided by DCP, are unique to the transmitter or receiver, highly confidential and not available to other devices.

All HDCP transmitters or receivers also include a Key Selection Vector (KSV) provided by DCP. This 20-bit binary value uniquely identifies the HDCP transmitter or receiver. Devices exchange KSVs and use them during authentication and encryption.

The transmitters and receivers also implement the HDCP cipher, an algorithm that encrypts and decrypts data. The cipher generates pseudo-random numbers that are passed between the devices and used during authentication and encryption.

Authentication

HDCP authentication has three parts:

1. First Part of Authentication: The transmitter and receiver both calculate a shared secret session key that they use for encrypting and decrypting data. By completing this process, the receiver demonstrates that it holds valid, secret device keys without needing to reveal those keys publicly.

   This happens in several steps. First, the transmitter sends its KSV to the receiver, along with a pseudo-random value generated by its cipher. In return, the receiver sends its KSV to the transmitter, along with a single bit that indicates whether the receiver is a repeater.

   The transmitter and receiver then each use the other device's KSV and their own Device Private Keys to generate a shared secret value. Because all HDCP keys are mathematically related, this calculation results in an identical value within each device.

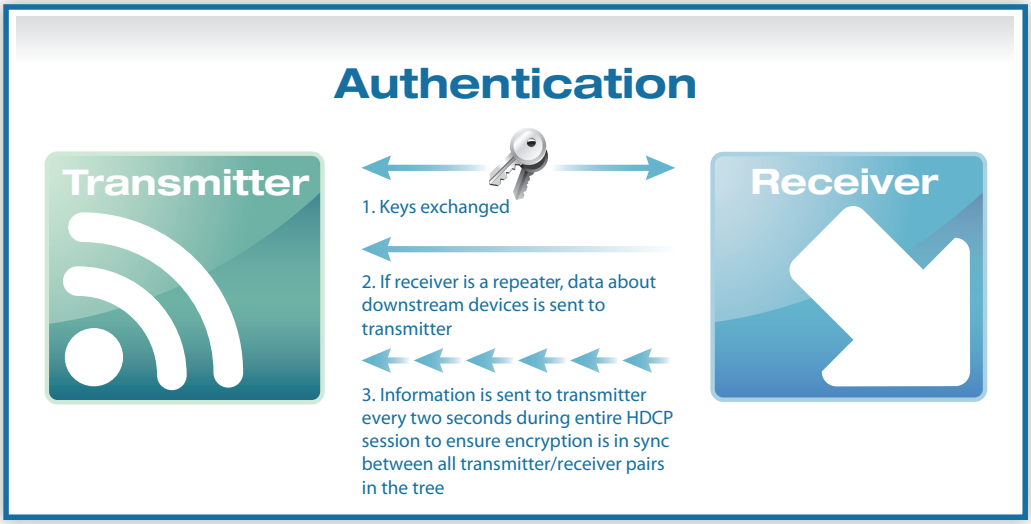
   This value is secret, so the two devices do not transmit the value over the network; however, they each feed the shared secret value and the pseudo-random number into their HDCP cipher engine. The HDCP cipher generates a secret shared session key along with another value, which the receiver sends to the transmitter to indicate it has successfully completed its part of the authentication process. The transmitter compares it with its own calculated value, and if the two are identical, authentication is successful. The transmitter can then start sending a stream of content, encrypted using the session key, which only the receiver can decipher.

2. Second Part of Authentication: This occurs only if the receiving device is a repeater. The receiver sends to the transmitter a list of all downstream receiver KSVs, as well as the number of levels in the tree. This enables the transmitter to determine whether the maximum tree size has been exceeded and whether all devices in the tree are valid.

3. Third Part of Authentication: This final stage occurs periodically during the transmission of encrypted content. Every 128 video frames or at least once every two seconds, the

receiver sends information to the transmitter, and the transmitter uses this information to verify that the devices are synchronized and that the receiver is receiving and accurately decrypting the content.

Figure 4.
HDCP Authentication Process



Encryption

After authentication, the transmitter uses its HDCP cipher engine and the shared session key to create a stream of encrypted data that can only be decrypted by the receiver. The receiver uses its HDCP cipher engine and its copy of the session key to decrypt the content.

HDCP licensing and use

Manufacturers who choose to use HDCP need to license it from DCP. By doing so, they agree to comply with the HDCP License Agreement and accordingly, make their products compliant with the HDCP specification and compliance rules and relevant interfaces such as HDMI, and to meet interoperability requirements.

Licensed technology Adopters are required to meet content protection requirements. For example, the HDCP License Agreement prohibits high-definition digital video sources from transmitting protected content to non-HDCP enabled receivers, and such devices from making copies decrypted content. Adopters agree to store highly confidential information securely and robustly, and to design products that meet industry standards to effectively frustrate attempts to defeat the content protection, including attempts to obtain highly confidential information such as device keys.

Key provisioning

Typically, consumer electronics manufacturers incorporate HDCP into their products by buying HDCP chips from a DCP-licensed vendor. These chips already contain the keys.

The makers of HDCP chips burn the KSVs and Private Device Keys into each piece of silicon. These keys are highly confidential, and protecting them from being compromised is an essential aspect of the manufacturing process.

Manufacturers are responsible for prohibiting access to the keys, and this involves maintaining tight control over keys, down to the factory floor. One method to simplify the task of protecting keys is to use a third-party solution, such as Certicom KeyInject*, to securely transport and inject keys into silicon during the manufacturing process.

Revocation

Any security system needs to anticipate the possibility that keys could be compromised and then used to make unauthorized copies of content. To protect against this, the HDCP specification and license agreement include a mechanism for revoking products' unique KSVs.

Once a KSV has been revoked, a receiver with that KSV can no longer receive HDCP content. Sources check the receiver's KSV during authentication to determine whether it has been revoked. Lists of revoked KSVs are typically delivered with audiovisual content on media such as DVDs. A source checks the receiver's KSV against this list.

The HDCP License Agreement sets forth the conditions under which keys may be revoked. An Adopter has the ability to dispute revocation and the mechanisms for such a dispute are set forth in the HDCP License Agreement.

Approved Retransmission Technology (ART)

To accommodate emerging high-speed home networking technologies, DCP has begun evaluating and approving Approved Retransmission Technology (ART) that it deems sufficiently meet security requirements for the transmission of protected content.

Examples of ARTs include proprietary wireless technologies that enable consumers to connect parts of a home theater system together without using cables. These ARTs typically consist of two parts, which are considered to comprise a single product and must be used together: a wireless transmitter that plugs into the HDMI port on a transmitting HDCP-compliant device such as a source, and a paired wireless receiver that plugs into the HDMI port on a receiving device such as a display (sink). The ART receives HDCP-encrypted data output via the HDMI port, decrypts it, transmits it wirelessly using a proprietary encryption mechanism, and re-encrypts it using HDCP at the receiving end.

It is important to distinguish ARTs from HDCP approved outputs. Upstream content protection systems, such as other content protection technologies and DRMs, allow content to be transmitted in digital form only on specific HDCP-approved outputs, such as HDMI interfaces. An ART, though considered secure, is not an approved output. However, it is important to note

that ART transmitters typically plug into HDMI connectors or other approved outputs. The transmitting device can therefore transmit HDCP-encrypted content via the HDMI approved output; the ART receives the content from the approved output, decrypts it and retransmits using its proprietary encryption scheme.

Testing and Interoperability

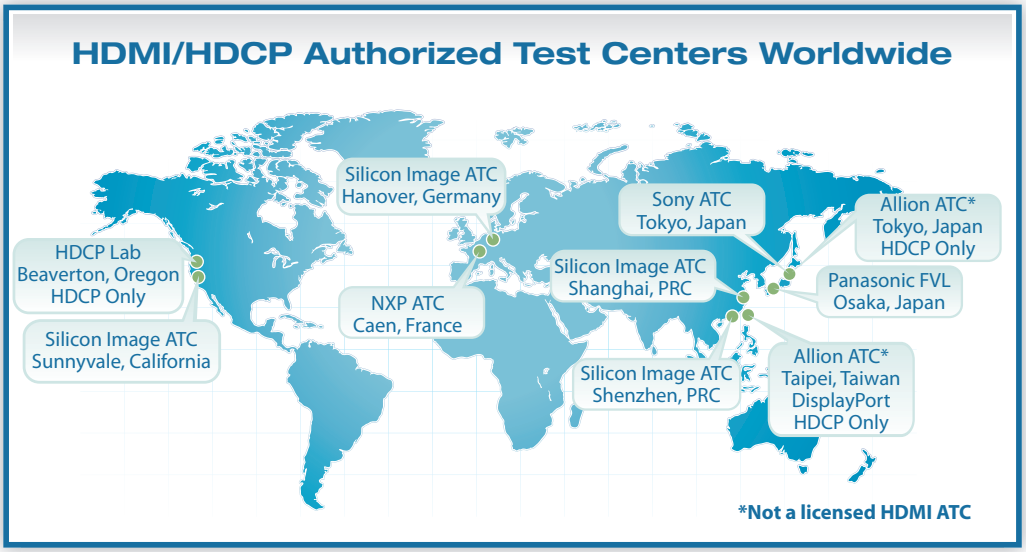
To enable a positive consumer experience, content protection must be transparent. This means that products must interoperate smoothly.

Manufacturers are responsible for ensuring that their products comply with the HDCP specification and are interoperable. The license agreement does not specify a requirement for testing, but DCP recommends that manufacturers test products sufficiently early in design, as well as during production, to avoid product compliance redesign delays.

For testing to the compliance specification, manufacturers may send products to an HDCP Authorized Test Center. There are currently 10 of these worldwide, as shown in Figure 5. Most centers also test HDMI compliance. These centers perform standardized tests, but do not test all the requirements necessary to create a compliant product. Completion of tests, therefore, does not guarantee that a product is fully compliant, and there is no process for certifying that products comply.

To enable interoperability, manufacturers may take part in periodic plugfests -- industry events at which different manufacturers test the interoperability of their products. Plugfests provide a confidential setting in which manufacturers can test how well individual products work together.

Figure 5.
Worldwide HDCP test lab locations



Futures

As the consumer electronics and PC industries continue to evolve, developing new and better products and interfaces, and the need for a robust content protection system remains necessary to enable the flow of high value content. HDCP is evolving to meet that need.

Today, HDCP is being applied to wireless interfaces through the ART process. Newer versions of HDCP will work directly over these interfaces, as well as other emerging wireless and wired interfaces.

Next-generation HDCP technology will include enhanced features such as reduced key complexity for source devices, state-of-the-art encryption and authentication, support for both compressed and non-compressed content streams, and backwards interoperability with existing HDCP devices through the use of active components.

Next-generation HDCP technology will continue to support the same usage models, protecting content over the last link of the distribution chain. The goal of HDCP is to remain unnoticed by users during normal operations of audiovisual device operations, while delivering robust protection against non-authorized uses. HDCP is designed to be a low-cost, robust solution that meets the needs of the content industry as well as implementers.

Conclusion

Content providers require assurance that high-value digital content is adequately protected. HDCP is an essential link in that chain of protection, and manufacturers are widely adopting it as an integral part of home theater systems. Testing enables content protection to be transparent to the consumer while providing a level of comfort to those manufacturers interested in complying with the HDCP License Agreement. HDCP is evolving to meet future needs.


DIGITAL CONTENT PROTECTION
DCP