DIGITAL CONTENT PROTECTION

# HDCP White Paper

November 2008

## Digital Content Protection for New Home Theater Networking Scenarios

### Executive Summary

The consumer electronics industry has rapidly adopted High-bandwidth Digital Content Protection (HDCP) to protect digital content transmitted over digital interfaces like HDMI and DisplayPort. Now, usage models are emerging that let end users conveniently connect displays, devices, and home-theater systems via standard protocols and interfaces like TCP/IP, Wi-Fi, USB and Wireless Home Digital Interface (WHDI). Robust and proven technology is needed to protect content transmitted in these scenarios and HDCP is evolving to meet this need with a new set of specifications. The first of these specifications to be released are High-bandwidth Digital Content Protection *revision 2.0* Interface Independent Adaptation (HDCP IIA) and High-bandwidth Digital Content Protection *revision 2.0* on WHDI (HDCP on WHDI). Additional HDCP *revision 2.0* specifications for specific implementations will follow.

These specifications support transmission of compressed and uncompressed data and use strong, standards-based RSA public-key authentication and AES 128 encryption. Additionally, these specifications are designed to enable seamless integration with other HDCP implementations over interfaces like HDMI and DisplayPort through the use of converters. This white paper describes the role of HDCP *revision 2.0* specifications, how they protect content, their use in various devices as well as compatibility with other HDCP implementations.

## Introduction

High-bandwidth Digital Content Protection (HDCP) has proven to be a highly effective, low-cost solution for protecting digital content transmitted over wired digital interfaces. As a result, consumer electronics manufacturers have rapidly adopted HDCP over the HDMI interface; more than 1.3 billion device keys have been shipped to date.

Now, wireless and other usage models are emerging that let consumers conveniently connect displays and other devices comprising home-theater systems without the need for cables. New technology is needed to protect content transmitted wirelessly and over protocols like TCP/IP, and HDCP is evolving to meet this need.

## Overview

Like other HDCP implementations, HDCP *revision 2.0* specifications protect content at the final stage of the content distribution process. Content is encrypted as it flows throughout the home from source devices such as DVD players and notebook computers to display devices such as High-definition TVs (HDTVs).

HDCP *revision 2.0* specifications define a standard, interoperable method for supporting compatible protocols like TCP/IP and compatible wired or wireless interfaces including the ubiquitous Wi-Fi and USB standards as well as emerging wireless interfaces like WHDI currently shipping in many consumer devices. Previously, the only way to protect wireless interfaces was through the HDCP Approved Retransmission Technology (ART) process, which allows transmission over approved proprietary content protection technologies applied to wireless interfaces using transmitter-receiver pairs. These pairs must be distributed as a single licensed product, eliminating any interoperability with other devices. DCP, LLC will no longer accept submissions for ART technologies as of December 31, 2008.

While other implementations of HDCP effectively protect wired interfaces, new technology is needed for wireless interfaces due to the potential for interception and unauthorized content use. To provide this protection, HDCP *revision 2.0* specifications use strong, industry-standard public-key RSA authentication and AES 128 encryption.

Transmission of compressed content is protected, making it feasible to use relatively slow 50 to 200 Mbps wireless interfaces or faster 5 to 10 Gbps links.

HDCP *revision 2.0* specifications provide compatibility with other HDCP implementations so that consumers can combine various devices within their home or business. Like other implementations, HDCP *revision 2.0* is designed to be robust and low-cost.

## HDCP devices and topology

Systems protected by HDCP include three types of devices. Each device contains one or more HDCP transmitters and/or receivers.

**Sources** send content to be displayed; examples include DVD players, Blu-ray players and notebook computers. Sources have one or more HDCP transmitters. **Sinks** render the content for display, and cannot transmit content to other devices, therefore they have only receivers; an HDTV is a typical example. **Repeaters** accept content, decrypt it, then re-encrypt and retransmit the data; they have both receivers and transmitters. An A/V receiver is a typical example of a repeater.

HDCP *revision 2.0* allows sources, repeaters and sinks to be connected together in a tree shaped topology with up to four levels and a total of 32 devices. Encrypted HDCP content flows through the tree over HDCP-protected interfaces. This allows many different arrangements: sources can wirelessly transmit protected content to multiple displays, for example, as shown in Figure 1. Multiple sources can also wirelessly transmit protected content to a single sink as show in Figure 2.

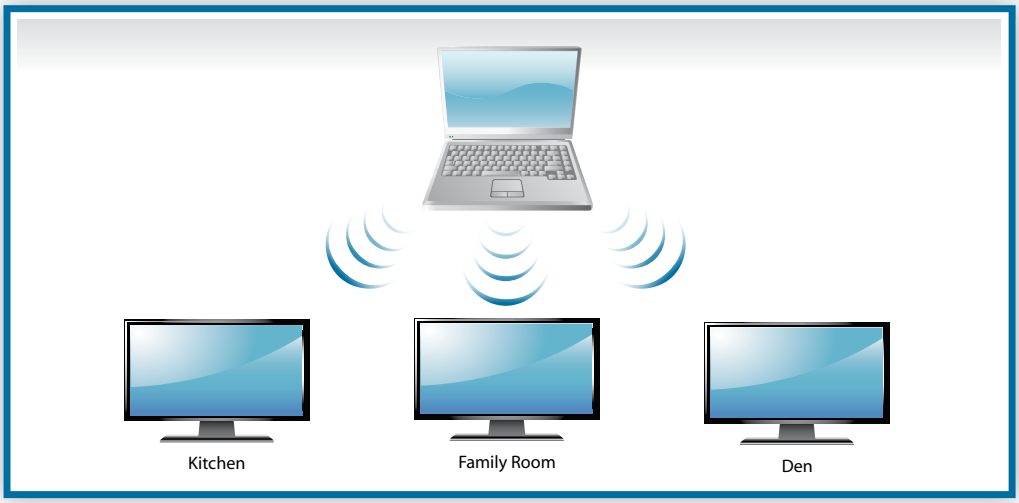



**Figure 1.**
**Notebook pc simultaneously transmitting HDCP-protected content wirelessly to multiple displays in different rooms within a home.**

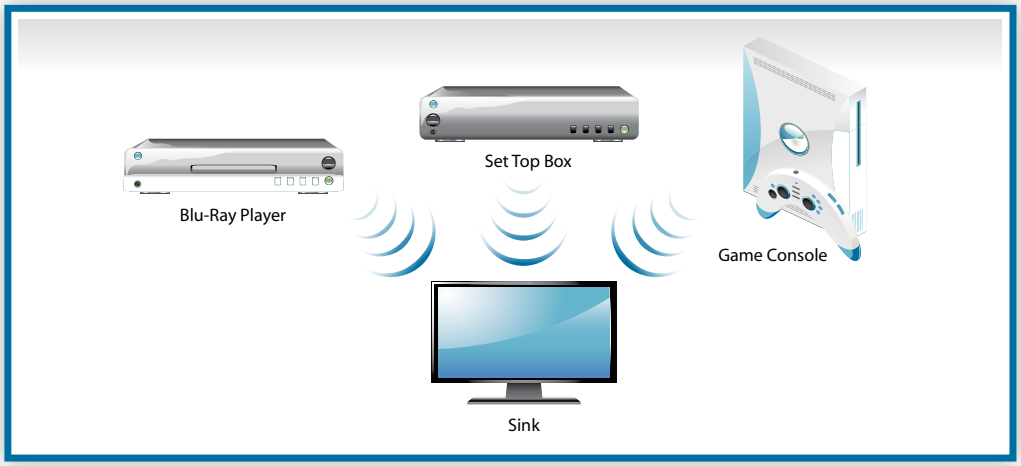



**Figure 2.**
**Multiple sources transmit HDCP-protected content to a single Sink.**

Converters: Repeaters can also act as converters, which allow seamless integration of devices with various wired and wireless interfaces. Consumers can add wireless devices to existing HDCP-enabled wired home networks, or install new systems that combine wired and wireless devices, as shown in Figures 2 and 3. Converters handle protocol conversion and allow sharing of topology information among the devices.

**Figure 3.**
**A source wirelessly transmits HDCP-protected content to a Repeater/ Converter, which transmits the content to a Sink via HDMI.**

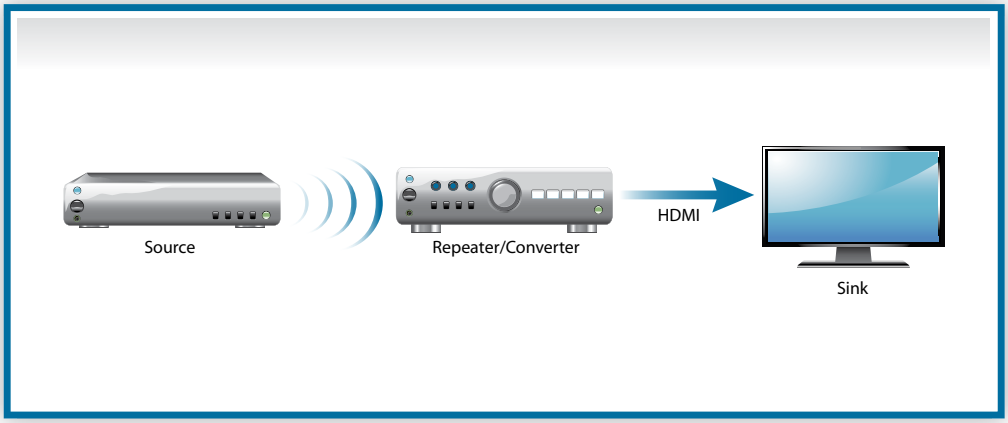
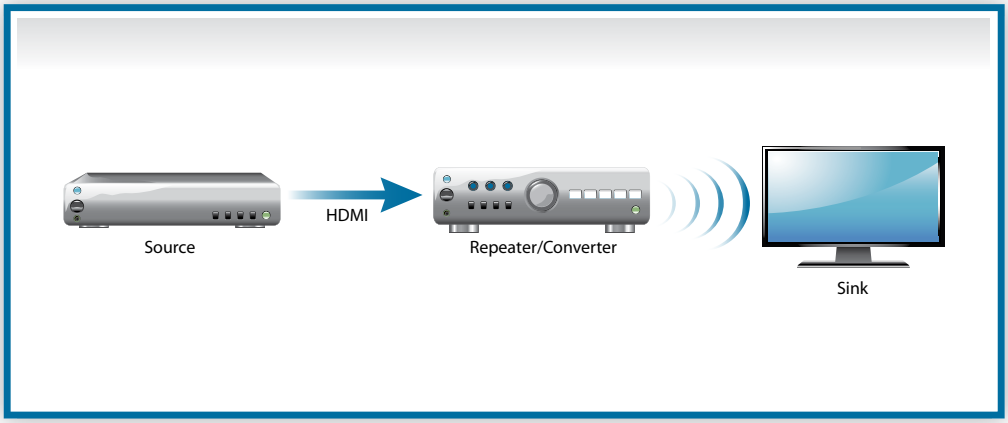



**Figure 4.**
**A source transmits content to repeater/converter via HDMI, which transmits HDCP-protected content wirelessly to Sink.**




## How HDCP *revision 2.0* specifications work

HDCP protects content using authentication and encryption. Before sending HDCP-protected data, each transmitting device authenticates the receiving device to confirm that it is authorized to receive the content. The transmitter then encrypts the data stream to prevent eavesdropping and sends it to the receiver.

HDCP *revision 2.0* specifications include several important new security features to provide strong protection for content transmission over wireless interfaces and standard protocols. Authentication uses RSA public key encryption. Each transmitter contains a 3072-bit public key issued by DCP, LLC. Each receiver contains a public key certificate signed by DCP, LLC. This includes a 1024-bit public key and a unique 40-bit receiver ID. The receiver also contains a 1024-bit private key.

All devices share a 128-bit secret global constant necessary to generate valid encrypted content.

HDCP *revision 2.0* also adds encryption based on the AES 128 standard, and a locality check to ensure that all wireless devices in the HDCP system are within a local environment, such as a home.

### Authentication Steps

**Authentication and Key Exchange (AKE).** The HDCP transmitter verifies the receiver's public key certificate and receiver ID. Then the devices exchange a shared master key. This stored key is used to accelerate subsequent communications between transmitter and receiver via a process called pairing.

**Locality check.** The top-level HDCP transmitter ensures that content is only transmitted locally by measuring the round trip time (RTT) for a pair of messages sent between the transmitter and receiver. The transmitter determines whether the RTT is within the acceptable limit defined for that specific wireless interface. If so, this verifies that all downstream devices in the HDCP system are within a local environment.

**Session Key Exchange.** The receiver has now been authenticated, so the transmitter sends an encrypted shared session key to the receiver. This secret key is used to encrypt and decrypt content that the transmitter subsequently sends to the receiver.

**Authentication with Repeaters.** If the receiving device is a repeater, there is an additional authentication stage. The repeater assembles a list of all downstream receiver IDs, as well as the number of levels and number of devices in the tree. This enables the transmitter to determine whether the maximum tree size has been exceeded and whether any downstream device in the tree has been revoked.

### Transmitting Content

The transmitter encrypts data using its AES 128 module in counter mode, which provides very high security and is fast enough to handle high-bandwidth data. AES operates in counter mode, which accelerates encryption by pre-computing values and performing operations in parallel, so that potentially several AES modules could work together to support even higher speed links.

## Revocation

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.

During authentication, the top-level transmitter checks each Receiver ID against this revocation list. For interoperability reasons, all implementations of HDCP have Receiver IDs in exactly the same 40-bit format, called the Key Selection Vector (KSV). This means any HDCP-enabled device can work together seamlessly to check the validity of all devices in the HDCP system.

## Licensing

To use HDCP *revision 2.0* specifications, manufacturers need to license them from DCP, LLC. Current HDCP adopters simply need to sign an addendum to the HDCP License Agreement and are not required to pay additional fees. New adopters will need to sign the HDCP License Agreement as well as the addendum.

## New Key Delivery System

DCP, LLC has implemented a new electronic key delivery system in conjunction with Certicom Corp., a security software vendor. The new system will streamline the process for obtaining HDCP keys over the Internet. The ordering process will have few changes, however licensees now have the option of two different delivery methods. They can download keys over the Internet directly from DCP, LLC, or have keys shipped by courier on DVD. If the licensee is a current Certicom KeyInject® customer, the new system is considered a "Product Update" under Certicom's product support terms.

**Electronic Delivery.** If a licensee chooses Internet delivery, DCP, LLC notifies the licensee by email when their order is ready to be downloaded. The licensee can then retrieve the HDCP keys using a software application licensed separately from Certicom Corp., a third-party security software vendor.

**Obtaining Software.** The licensee obtains the secure-download software directly from Certicom Corp. The software license, terms of use and a USD 1,500 annual subscription fee are pre-set and approved by DCP, LLC and Certicom Corp. The annual subscription fee includes a software installation package, user documentation, digital certificate, email support and upgrades.

**Download Security.** With both key delivery options, keys are delivered wrapped in an OpenPGP encrypted file format. There are additional security layers built into the electronic delivery system. The download software application uses the TLS security protocol with a cipher suite at the 128-bit security level. The TLS protocol is configured for mutual authentication, which requires every licensee to have a digital certificate. A digital certificate is included in the download software subscription fee and is re-issued annually to the licensee by Certicom's Certificate Authority, contingent on approval from DCP, LLC.

**Automation.** The secure download application is scriptable and available on Windows and Linux platforms. After download is completed and validated, the application will send an email alert. Optionally, the application can also be configured to launch a pre-defined script to unwrap the PGP encrypted file and load the HDCP keys into a secure manufacturing automation system, like Certicom's KeyInject® for HDCP product.

## Conclusion

Consumers are increasingly using home theater networking scenarios that require the transmission of digital content over wireless interfaces and standard protocols like TCP/IP and Wi-Fi. Robust protection must exist in the wireless home network for commercial content producers to permit content to be transmitted over these networks. HDCP *revision 2.0* specifications are designed to provide this strong protection at low cost while offering seamless compatibility with existing HDCP-enabled devices.


DIGITAL CONTENT PROTECTION
DCP