

# DRM for the A/V Professional

## Table of Contents

What is DRM?.....	2
HDCP and AACs – Separate DRM Protocols That Work Together .....	3
Analog Outputs.....	6
Computers .....	6
Conclusion .....	7

## Abstract

Digital Rights Management - DRM is used by owners and holders of intellectual property to enforce restrictions on the use of their copyrighted content. A/V professionals and their customers need to be aware of DRM, the relevant restrictions on the playback of protected material in public and commercial spaces, and the potential impact on A/V system design and operation. This paper will discuss the two prevalent DRM protocols in use, AACs - Advanced Access Content System, used to protect digital music and video content, and HDCP - High-bandwidth Digital Content Protection, for securing digital interfaces including HDMI, DVI, and DisplayPort.

white paper

## What is DRM?

DRM - Digital Rights Management is used by owners and holders of intellectual property to enforce restrictions on the use of their copyrighted content. In the A/V industry, DRM is used to secure digital music and video content to prevent unauthorized playback or copying. For digital video content protection, the most prevalent DRM systems are HDCP - High-bandwidth Digital Content Protection, and AACS - Advanced Access Content System. HDCP is an encryption protocol applied to digital interfaces including HDMI, DVI, and DisplayPort. AACS is a standard for encrypting high definition optical discs that also works in conjunction with HDCP.

DRM exists to protect the rights of content creators and owners to receive compensation for their initial ideas and subsequently bring them to market. Movies and music are the most recognized source content within the A/V industry that is impacted by DRM enforcement. An individual who purchased a copy-protected Blu-ray Disc, for example, is entitled to utilize that disc only within a personal-use environment, which extends to the home or other private viewing locale. For that movie to be played in a public space, additional licensing requirements must first be met. If that licensing has not been obtained, significant fines can be levied against the offender. These fines may very well extend to the owner of the installed system.

A/V systems in public spaces are the center of our industry, with installations taking place on a daily basis. It is for this reason that DRM considerations must be made and addressed at the earliest point of system design. The time when needs are being assessed for an A/V integration project is also the time to determine the functional requirements of a given system. This is when the sales engineer should ask the right questions and inform the prospective customer on the legalities involved with personal-use devices and/or material being used in public and commercial spaces. The old, familiar adage of "Just because one can, doesn't mean one should" is fully appropriate in this case. HDCP-compliant systems are increasingly being requested by customers and integrators alike. This type of system could be used to show protected content in public spaces. Therefore, users should be made aware of the potential issues that may arise from inadvertent public display of private-use, content-protected materials. During system commissioning and training, the integrator should consider educating system operators, and even include discussion of DRM and content protection within system documentation. Of course, this is not as much of an issue for residential installations, where the entire system is generally intended for personal use.

## HDCP and AACS – Separate DRM Protocols That Work Together

HDCP is designed to prevent unauthorized access of protected video content and to enforce restrictions on authorized playback. HDCP-enabled video sources, such as Blu-ray Disc players, PCs, and other digital media devices, always undergo a three-step process to protect the video from unauthorized access:

**1. Authentication:** The video source determines that all devices connected to its outputs are authorized and able to receive encrypted video. This is accomplished by means of an initial authorization handshake protocol, where cryptographic public keys, KSV - Key Selection Vector, and encrypted messages are exchanged between the source and the downstream devices connected to its outputs. The HDCP 1.3 specification calls for a maximum of 127 simultaneous devices connected downstream from the source, and up to seven allowable levels of repeater devices between the source and the display - also known as the sink. The source uses the initial handshake protocol to determine that these system size restrictions are not violated. HDCP version 1.3 is the currently implemented specification. As will soon be discussed, the latest version, HDCP 2.0, further restricts the allowable maximum number of simultaneous devices and repeater levels.

**2. Content Encryption:** After the source authenticates that all downstream devices are HDCP compliant and in good standing, and that no system size restrictions are violated, the source sends encrypted video downstream. The source periodically revises the encryption key for the video as an additional security measure.

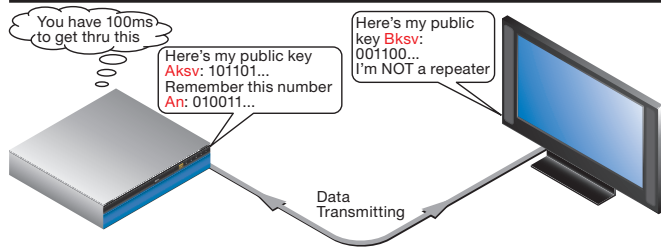
**3. Renewability:** Since HDCP relies on digital encryption using secret keys, the system can be circumvented if the secret keys residing in HDCP-licensed products fall into the wrong hands. Therefore, a means has to be established to revoke any compromised keys. The HDCP administration authority, Digital Content Protection, LLP can add a list of public keys of compromised products to video content such as Blu-ray Disc. Video sources will read this data, store it in non-volatile memory, and compare the public keys of any downstream devices against this revocation list. If any key matches, no video will be transmitted.

Figures 1 and 2 on the next page provide a step-by-step illustration of the communications that occur between source and sink devices within an HDCP-based system.

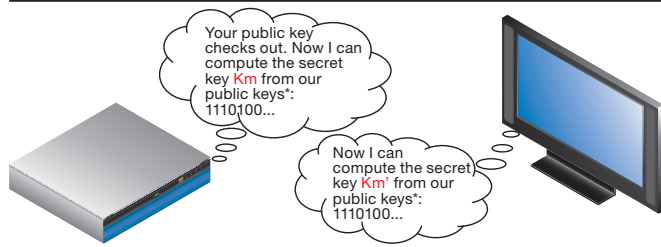
The multi-step process of HDCP authentication can take several seconds to complete. This is a primary reason for the perceived sluggishness of some digital video systems, especially during startup and when video signals are switched or re-routed, requiring HDCP re-authentication. The best switching performance can be realized in HDCP-compatible video equipment built to minimize re-authentication through careful internal design and proper deployment of HDCP processing components.

Communication process that occurs between source and sink devices within an HDCP-based system.

Initial Key Exchange

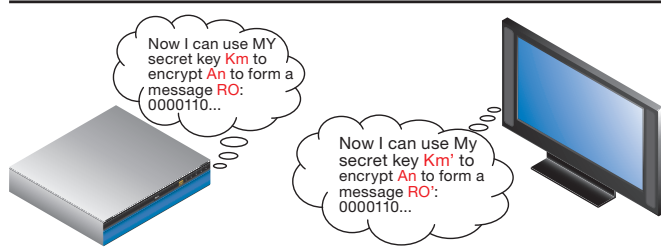


Calculate Shared Secret Keys

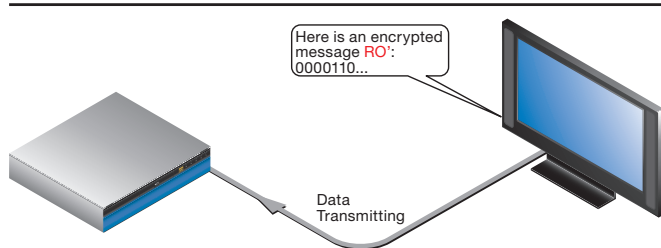


\* Km and Km' are computed using each device's private key along with the public keys of both devices. This is a special calculation that results in matching Km=Km' IF all the keys are valid.

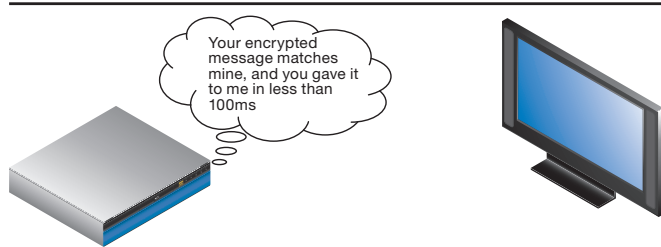
Encrypt a Message Using Secret Key



Receiver Demonstrates Secret Key Knowledge



Initial Authentication



Transmit Video

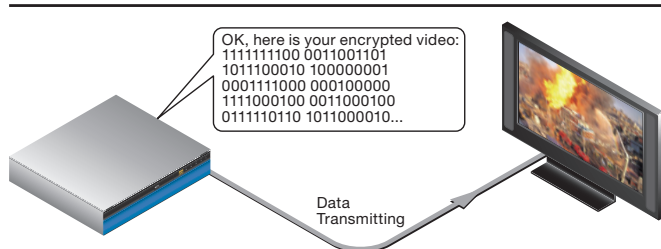
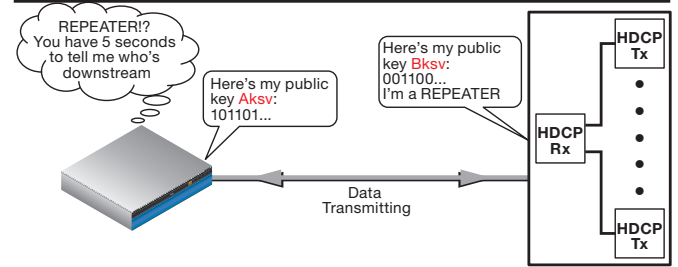
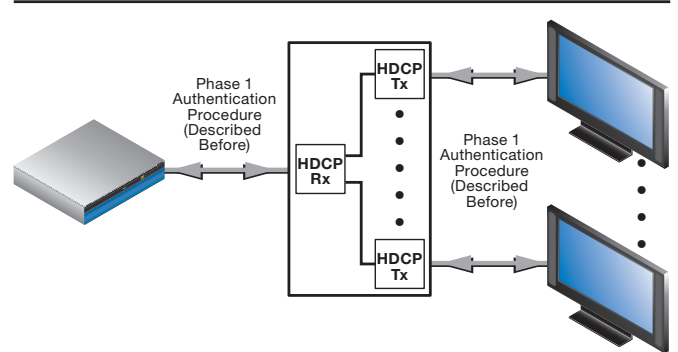


Figure 1. Phase 1

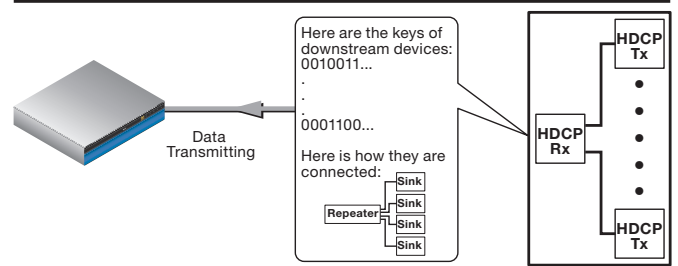
Initial Key Exchange



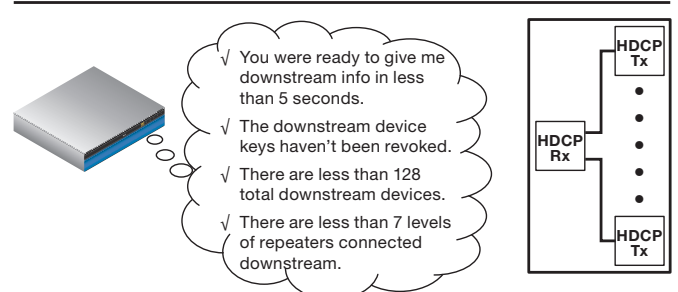
Repeater Performs Initial Authentication with Connected Devices - Downstream Device Keys are Collected



Repeater Reports Key List and Topology



Transmitter Validates Connections



Repeater Authentication Complete

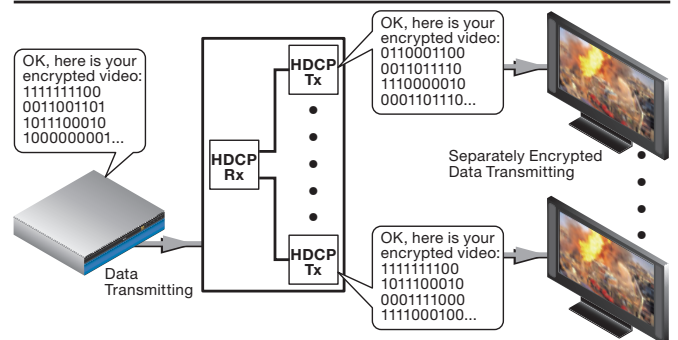


Figure 2. Phase 2

	HDCP 1.x	HDCP 2.0
<b>Encryption Method</b>	Specialized 56-bit symmetric system used for both authentication and video encryption	Authentication: Data security industry standard RSA 1024 and 3072-bit asymmetric system  Video encryption: Data security industry standard AES 128-bit symmetric system
<b>Applicable Interfaces</b>	DVI, HDMI, DisplayPort	Any two-way digital interface
<b>Maximum Downstream Receivers for Each Transmitter</b>	< 128	< 32
<b>Maximum Repeater Levels for Each Transmitter</b>	< 7	< 4
<b>Backward Compatibility</b>	Yes, no electronic components required	Yes, using specialized electronic HDCP-1.x-to-2.0 and HDCP-2.0-to-1.x converters
<b>Wireless Support</b>	Not specified	Explicitly specified with new locality check requirement

Table 1. Major changes in HDCP 2.0

	DVDs (CSS)	Blu-ray Discs (AACs)
<b>Encryption Method</b>	Specialized 40-bit stream cipher	Data security industry standard AES 128-bit symmetric system
<b>Player Revocation</b>	All players in a model range are revoked	Individual players can be revoked
<b>Disc Copy Prevention</b>	Hidden disc lead-in area prevents bit-for-bit disc copy	Encrypted volume ID prevents bit-for-bit disc copy
<b>Output Signal Scrambling</b>	Macrovision applied at analog outputs	HDCP applied at digital outputs  Macrovision applied at analog outputs
<b>Managed Disc Copying</b>	No provisions	Authorized copies are possible by connecting to AACSLA server and obtaining permission (details to be finalized)
<b>Analog Sunset</b>	No provisions	Players manufactured after 2010 may not have high definition analog outputs  Players manufactured after 2013 may not have any analog outputs

Table 2. Differences between CSS and AACs encryption

The HDCP standard was greatly revised in October 2008 with the release of HDCP 2.0. Subsequently, in May 2009, HDMI 1.4 was released, but did not call for compatibility with HDCP 2.0. At this point, the timing for products to adopt the HDCP 2.0 standard is uncertain.

Until the introduction of HDCP 2.0, the basic protocol of HDCP had not changed substantially. The only major differences between HDCP versions 1.0 through 1.3 is in the types of physical A/V connections. HDCP version 1.0 applied to the DVI interface. Version 1.1 incorporated HDMI, and support for DisplayPort was added for version 1.3. With the release of version 2.0, HDCP became interface-independent, and can be applied to any two-way digital transmission between sources and displays, wired or wireless, compressed or uncompressed. See Table 1.

HDCP 2.0 calls for many other important changes. For wireless connections, HDCP 2.0 adds a locality check to the authentication protocol, to ensure that only devices nearby will be able to receive protected content. Furthermore, HDCP 2.0 replaces the specialized 56-bit HDCP 1.x encryption scheme with two standard algorithms from the data security industry: for authentication, an RSA system with 1024 and 3072-bit keys; and for content encryption, a 128-bit AES - Advanced Encryption System. In addition, the maximum number of connected devices is reduced to 32, and the maximum level of repeaters is reduced to four. As a result of all these changes, HDCP 2.0 is not directly backward compatible with HDCP 1.x. The new specification provides for converters between HDCP 1.x and HDCP 2.0 devices to support mixed A/V systems with devices that comply with both versions. An existing A/V system incorporating HDCP 1.3 will require converters if newly acquired HDCP 2.0 devices are to be incorporated into the system.

AACS is the DRM standard adopted for Blu-ray Disc. AACS is designed to protect Blu-ray Disc content similar to the way that the CSS - Content Scramble System protects commercial DVDs, but with additional features. Both AACS and CSS encrypt the video data on-disc, so that only authorized players can read the content. See Table 2. Both AACS and CSS prevent unauthorized copying of commercial Blu-ray Disc and DVD, and both systems have mechanisms for revoking compromised players. AACS offers greater protection than CSS in the following areas:

- AACS employs AES 128-bit encryption, while CSS implements 40-bit encryption
- AACS allows for the revocation of individual Blu-ray Disc players, whereas CSS can only revoke entire models of DVD players
- AACS encrypts the digital outputs of Blu-ray Disc players with HDCP

- AACS provides for the eventual elimination of analog video outputs on Blu-ray Disc players

The final AACS specification will include a provision for making authorized copies of Blu-ray Discs, whereby a recording device can connect to Internet servers at the AACS LA - AACS Licensing Administrator to obtain electronic permission to make a legitimate copy of protected content.

## **Analog Outputs**

The HDCP licensing agreement does not allow for analog video outputs on repeater or display devices, but does not restrict analog outputs for sources. Nonetheless, this does not preclude separate agreements that would prevent analog outputs on source devices. Such agreements could be negotiated on an ad hoc basis between content providers and hardware makers.

However, the AACS licensing agreement is very specific about analog outputs and provides for several measures to control them. Blu-ray Disc titles that support AACS have usage rules data embedded in them that allow the content producer to limit the analog output resolution by invoking the ICT - Image Constraint Token, or even to disable the analog outputs entirely by invoking the DOT - Digital Only Token. As of the fourth quarter of 2009, no Blu-ray Disc titles have included these restriction tokens, but this may change with future releases. The AACS license agreement also provides for an "analog sunset" for newly manufactured Blu-ray Disc players, such that models manufactured after 2010 can only include standard definition analog outputs, and after 2013, no Blu-ray Disc players may be manufactured with any analog outputs.

## **Computers**

There are numerous DRM schemes for computers. The computer industry is a major source of innovation for content creation as well as for unauthorized reproduction of that content. Computer DRM methods have been devised to protect software, digital music, digital video, digital books, games, etc. The present discussion will be limited to video content played on a computer and the associated DRM schemes therein. These DRM schemes are mainly for preventing unauthorized access to protected commercial video such as Blu-ray Disc or downloaded content including movies or TV shows. But non-commercial video files can also be protected with DRM, if the content creator has access to DRM technology. The DVI, HDMI, and DisplayPort outputs of computers should have no DRM restrictions when the content being played is not protected.

As of the fourth quarter of 2009, for Blu-ray Disc playback, only PCs running Windows® operating systems have software authorized to play Blu-ray Discs.

The same AACS and HDCP restrictions apply for PC Blu-ray Disc playback as for standalone players. Thus, a PC must be equipped with a video card that is capable of HDCP encryption. An A/V device with digital video inputs must support HDCP, if a user expects to connect such a PC to it and play commercial Blu-ray Discs.

The market for authorized downloads of commercial video content is crowded with companies and products, with frequent turnover of market entries and exits. Current market players include Amazon, Apple iTunes, Blockbuster, Netflix, and Vudu, to name just a few. These companies offer a plethora of options for the end user. Movies or TV shows can be rented or purchased, some in high definition, but most in standard definition. The video may be either streamed or stored locally to a computer, a networked set-top receiver, Blu-ray Disc player, a video game console equipped with a hard drive, or even a display with Internet access capability. The one constant among all these different options is the existence of DRM for protected content, which is used to restrict the allowable viewing duration of “rented” video content and the ability to transfer the video to different computers. In the case of protected HD video downloads, HDCP support is required on any device that is playing the video. Therefore, a display with digital video inputs must support HDCP if a user expects to connect a computer to it and play downloaded commercial HD content.

## Conclusion

Any A/V system that is intended to support playback of protected video content, such as Blu-ray Disc and consumer-purchased HD video downloads, must be compliant with the associated DRM. Since DRM implementations such as HDCP and AACS are meant to restrict what the end user can do with protected content, it makes sense for the A/V professional to inform the end user of these restrictions at the outset. Such restrictions include limiting the number of simultaneous displays for content-protected video playback, disallowing recording or copying, and disabling analog outputs. For example, an A/V system may have the capability to distribute HDMI video to 16 displays and provide analog video recording. These functions will always be available when a PC with HDMI output is connected for PowerPoint presentations and other non-protected material. But once a protected Blu-ray Disc is inserted into the PC for playback, HDCP and AACS restrictions may disable output to several displays and to the recorder.

Since many large-scale A/V systems can display unencrypted video on a large number of displays, freely distribute analog signals, and provide video recording capabilities, end users of such systems must be made aware that some system functions may not be available when playing DRM-protected content.

Extron Electronics, headquartered in Anaheim, CA, is a leading manufacturer of professional AV system integration products. Extron products are used to integrate video and audio into presentation systems in a wide variety of locations, including classrooms and auditoriums in schools and colleges, corporate board rooms, houses of worship, command-and-control centers, sports stadiums, airports, broadcast studios, restaurants, malls, and museums.

For additional information, please call an Extron Customer Support Representative at: 800.633.9876 (inside USA and Canada only) or 714.491.1500 for Extron USA; +800.3987.6673 (inside Europe only) or +31.33.453.4040 for Extron Europe; +800.7339.8766 or +65.6383.4400 for Extron Asia; +81.3.3511.7655 for Extron Japan.

[www.extron.com](http://www.extron.com)

© 2010 All rights reserved.