CRESTRON DIGITALMEDIA DM™

HDCP White Paper:
How DigitalMedia™ Switchers Handle HDCP

CRESTRON®

HDMI and HDCP are new to the Pro-AV industry, and as a system designer it is very important to understand the implications of designing a system that integrates HDCP. This whitepaper is geared towards AV system designers, in order that they may have a more in-depth understanding of the challenges of HDCP – and how DigitalMedia deals with these challenges.

Definitions

For the purposes of this document, the following terms are defined:

Digital video – DVI, HDMI or DisplayPort

Downstream device – a device that is receiving content from the current reference point. For instance an AV receiver would be downstream of a Blu-ray player.

Upstream device – a device that is sending content to the current reference point. For instance a document camera would be upstream of a video switcher.

DM Tools – a software application installed within Crestron Toolbox™ that provides status of the signals routed through a DM switcher.

KSV – Key Seletion Vector; this is the unique ID sent from devices that receive HDCP-protected content to the HDCP source. It is sometimes called an HDCP key.

HDCP – High-bandwidth Digital Content Protection – a form of copy protection used on uncompressed video interfaces such as HDMI, DVI and DisplayPort.

Sink – A device that renders content so it can be viewed (i.e. display.)

Source – A device that sends the content to be displayed.

Blacklist – A list of revoked KSVs that HDCP sources receive from their content provider. These KSVs identify noncompliant devices that are no longer allowed to receive content.

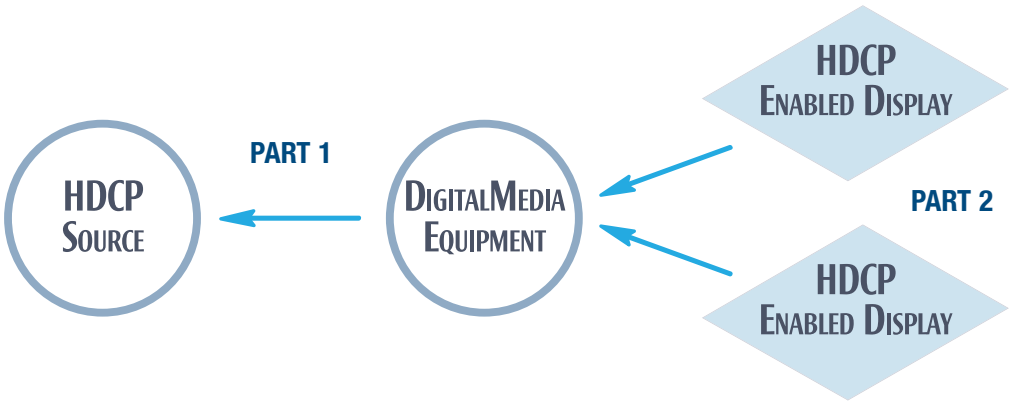
HDCP Overview

HDCP encryption is another complicating factor in HDMI installations. The HDCP system has three main parts:

1. HDCP source authenticates the immediate downstream device
2. HDCP source authenticates each downstream HDCP device to make sure they are authorized to receive the content
3. Each HDCP link encrypts the content to prevent interception during transmission

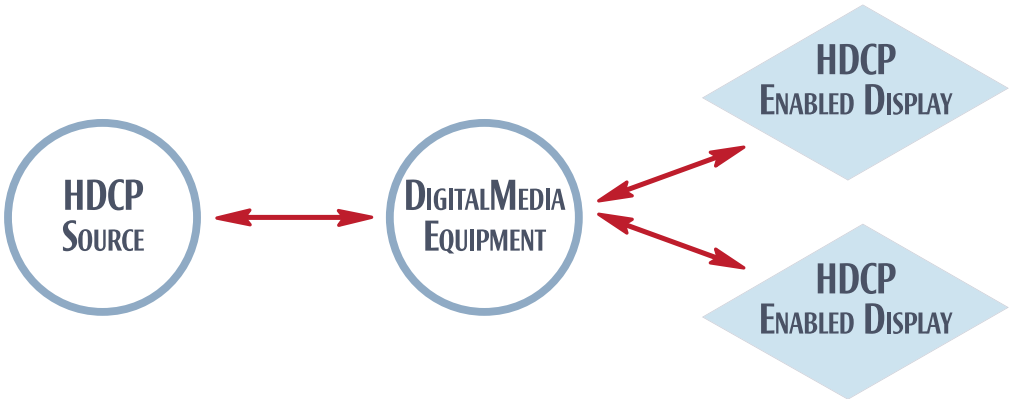
Authentication ensures that all devices receiving the content are licensed and authorized. Only after successful authentication can the display output the audio and video streams.

PARTS 1 & 2 - HDCP AUTHENTICATES EACH DEVICE VIA THE SOURCE



PART 3 - HDCP ENCRYPTS EACH INDIVIDUAL SEGMENT OF AN AV TRANSMISSION

During part 3 of authentication, each individual HDCP link (shown in red) is encrypted and managed separately.



Devices that re-transmit HDCP content must inform the source of all the downstream connections in the system. Every HDCP device has a unique ID, known as a KSV (Key Selection Vector), which must be passed to the source. The source will then verify that each device is not on its blacklist for unapproved devices before it transmits content.

WHO DECIDES WHEN CONTENT SHOULD BE HDCP ENCRYPTED?

The HDCP source initiates HDCP encryption. This decision may be based on the firmware of the device itself, or it may be based on the content that the device is transmitting. There are four general types of behavior for digital video sources:

1. **The digital video output will always be encrypted; if the link cannot be encrypted, then no content will be transmitted.** This category contains many Blu-ray players and cable boxes where the use of protected content is assumed so content protection is always enabled.

2. **The digital video output will be encrypted for some AV content but not others. In this category are some PC graphics cards and satellite boxes.** For instance, some DirecTV boxes will only turn on HDCP when a Video on Demand channel is selected, and turn it off when watching regular broadcast channels. Some PC graphics cards also fall into this category – they will only turn on HDCP when attempting to play back a Blu-ray or other piece of protected content.

3. **The digital video output will always be encrypted; if the link cannot be encrypted then a subset of functionality is provided.** This category contains Apple computers and some PC graphics cards. These devices will attempt to enable HDCP all the time, even when it is not required. If they cannot enable HDCP, then the source can still be used for all functions that do not require playing back protected content (such as Blu-rays or some iTunes video content).

4. **The digital video output is never encrypted.** This category contains devices that do not play back protected content, such as document cameras or PCs running Windows XP or earlier.

Each DigitalMedia digital video input supports HDCP, so when a source device is connected to DM it will determine that it may encrypt the video stream with HDCP if it wishes – same as any HDCP-enabled display.

HDCP ENCRYPTION ON DIGITALMEDIA OUTPUTS

DigitalMedia will encrypt the video stream on each output only if the source is HDCP encrypted. This means that an unencrypted stream from a document camera will not be encrypted as DigitalMedia routes that content to a display. Whether the display supports HDCP or not, the display will show the video.

If the source content is encrypted with HDCP, the DigitalMedia switcher will report that on the front panel and in DM Tools. The DM switcher will then attempt to authenticate with each device to which the source is routed. If the device connected to the output cannot be authenticated, the DM switcher will route a black frame instead and indicate the failure on that output in the following ways:

- Error message on the front panel
- Red line in DigitalMedia tools
- Trigger the HDCP_Blanked_fb signal in SIMPL Windows™

If one output of a DigitalMedia switcher cannot authenticate with the downstream device, ONLY that output will not receive content. All other outputs will receive content as normal. Common causes for this are that the display is powered off or switched to a different input. In addition, this will happen if the display does not support HDCP.

HDCP, KSVs AND DIGITALMEDIA

As per part 2 of the HDCP specification, DigitalMedia will send a KSV from each downstream device to an upstream source. The HDCP specification allows for up to 127 KSVs to be routed to sources, but current sources usually support far fewer.

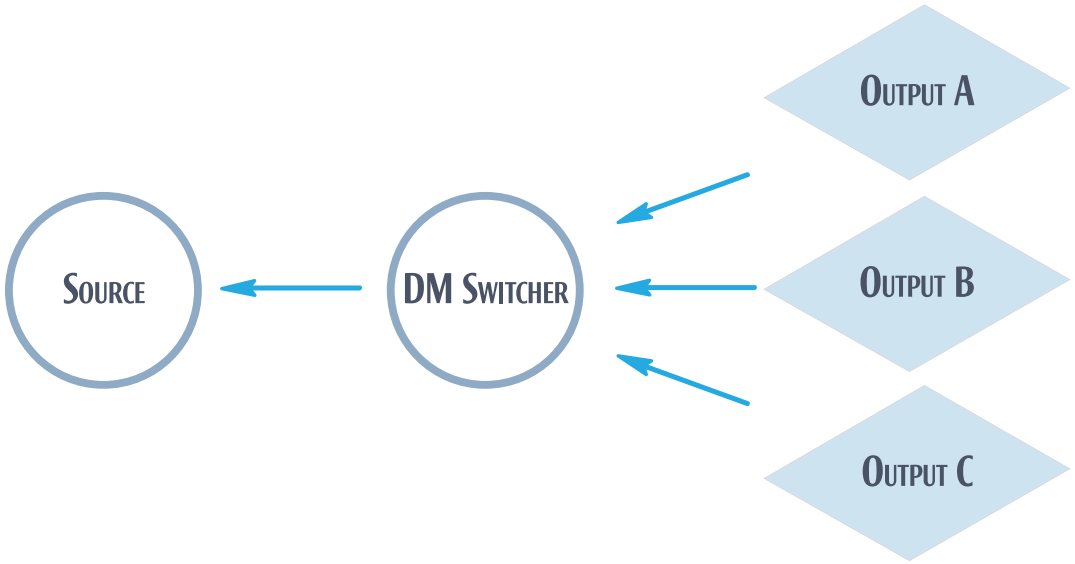
All sources have a hard limit on the number of displays that can be connected, due to a limit in the number of KSVs they will accept from downstream devices. If a repeater presents a source with too many KSVs, the source stops transmitting content. Unfortunately, KSV limits are not an advertised feature. Problems will not be noticed until a source is routed to an extra repeater or display, at which point audio and video drops out inexplicably in all connected rooms, typically without so much as an error message.

To deal with this issue, DigitalMedia has a method to determine the number of HDCP KSVs that each source supports called HDCP Check. This function can be run from the front panel of a DM switcher or from DM Tools.

MANAGING KSVs

Once DigitalMedia knows the number of downstream KSVs that the source can support, it will never route more than that number to the source. This ensures that the source does not go into a failure mode from receiving too many KSVs.

The HDCP specification requires that any HDCP enabled switcher report downstream KSVs to the source from devices that are receiving content. However, if a new route is added, an additional KSV must be transmitted to the source – and so in this scenario the source must restart authentication from part 1. This functionality has caused much grief in other manufacturers' HDMI switchers. To remedy this, DigitalMedia transmits as many KSVs as possible to the source, whether the sink devices are receiving content or not. Here is an example:



A source is routed through a DigitalMedia switcher to devices A, B and C – the source only supports 2 downstream KSVs. When the source is routed to A and B, the DM switcher will send KSV A and B to the source. If route B is broken, DM will continue to send KSV B to the source. When the source is routed back to B, the KSV has already been sent to the source so re-authentication is not performed.

Now lets say you add output C to the route, so the source is going to outputs A, B and C. DigitalMedia knows that the source only supports 2 KSVs so it will blank output C – the new route. If B is then unrouted, C will be unblanked and KSVs A and C will be transmitted to the source. In this way DigitalMedia optimizes the KSVs that are sent to each source by routing as many as possible, from the most recent routed destinations.

By July 2010, most source devices will support at least 16 downstream KSVs, so each source can be routed to 16 destinations simultaneously.

Third-Party Equipment

USING THIRD-PARTY DEVICES WITH DM

Crestron does not recommend integrating any third-party HDMI switchers with DigitalMedia because of the effect that they can have on system behavior. Third party devices have their own methods for managing KSVs that will affect how the DM system functions. A third-party processing device, such as a switcher or distribution amplifier used in between a DM output and a display may cause that display to lose video unnecessarily while that device transmits KSVs. A third-party processing device used between a DM input and a source will negate the effect of QuickSwitch HD and the HDCP check – so DM cannot manage the KSVs appropriately.

USING THIRD-PARTY CABLE WITH DM

DigitalMedia was designed from the ground up as a digital video routing system. Even the cable has been optimized for the digital video signals. Using third-party cable can have negative effects in two ways:

1. **Cable bandwidth.** DigitalMedia transmits video signals at over 1GHz. Therefore, DM cable is manufactured and verified to support signals at up to 1.2GHz. Even the best CAT6a cable is only rated to 625MHz – which is perfectly appropriate for 10-gig Ethernet applications, but not for digital video. It is impossible to know the performance of these CAT6a cables when used to carry DigitalMedia signals and so we cannot guarantee the performance of the DM system without DM cable. Some symptoms of inferior cable is that video works at lower resolutions (1080i but not 1080p) or that video does not work when HDCP is enabled.

2. **Cable Shielding.** DigitalMedia cable has been designed with a double-shield and the DM connectors were selected for their ability to shield against external interference. Shielding is a very important factor in digital video systems, especially when compared with systems that traditionally use unshielded cable such as Ethernet or analog video. This has to do with the signal's ability to recover from errors caused by transient electrical interference.

The only way to guarantee that a DigitalMedia system will perform as intended is to using Crestron DM equipment and cable in-between every source and sink.

Crestron World Headquarters
15 Volvo Drive
Rockleigh, NJ 07647
800.237.2041
201.767.3400
Fax: 201.767.1903
crestron.com

Crestron International Headquarters
Oude Keerbergsebaan 2
2820
Rijmenam
Belgium
+32.15.50.99.50
Fax: +32.15.50.99.40
crestron.eu

Crestron Asia Headquarters
Room 2501, 25/F, Westin Centre
No. 26 Hung To Road
Kwun Tong
Hong Kong
+852.2341.2016
Video Ph: +852.2373.7530
Fax: +852.2344.0889
crestronasia.com

Crestron Latin America Headquarters
Blvd. Manuel Avila Camacho No 37-1A
Col. Lomas de Chapultepec
CP 11560 México DF
+55.5093.2160
Fax: +55.5093.2165
crestronlatin.com

Printed in USA Doc.4588 10/10

Products manufactured in the United States.