HDCP — the FTA broadcasters' perspective

*Note from the Editor: This article outlines the views of several European broadcasters on HD content protection using HDCP. The views of EICTA – the European CE equipment manufacturers association – are presented in a **separate article** published in this edition.*

Jean-Pierre Evain
European Broadcasting Union

The first HD services have now been deployed on pay-TV platforms using content-protection measures such as HDCP, in accordance with contractual obligations mandated by the production studios. Before long, free-to-air TV platforms will also become involved in HDCP.

This article provides technical information on the HDCP system, which is used to protect the HDMI link from a set-top box to a display device (HDMI is the HDTV equivalent of the familiar "SCART" connector used with standard-definition television). The article also explains "what HDCP is" and "what it is not", and outlines the views of several different European broadcasters on methods for controlling content protection.

HDCP over HDMI: a de facto standard

HDMI – which has now supersed ***DVI*** in consumer electronic products – is a high-bandwidth interface between an HDTV transmitter (e.g. a set-top-box) and an HDTV repeater/receiver (e.g. a display device). Such interfaces are often referred to as "display links", with DVI more commonly being found on personal computers. The HDMI interface can transmit HD digital video at bitrates up to 2.23 Gbit/s[1] at 720p or 1080i resolution, and up to eight channels of digital audio, sampled at 192 kHz with 24 bits per sample.

Although technically challenging, HDMI is clearly of interest to pirates for accessing high-quality content sources in order to produce unauthorised copies. This is where ***HDCP*** comes in: it protects the content by encrypting the signal that is being carried over the HDMI (or, indeed, DVI) link to the display device.

HDCP is a proprietary technology from Intel Corporation, described in a specification that can be implemented under licence from the "Digital Content Protection LLC" (a subsidiary of Intel). The specification and licensing conditions can be found at **www.digital-cp.com**.

1. The current version of HDMI has a maximum bitrate limit of 4.95 Gbit/s but that figure will be extended to 10.2 Gbit/s in a later version of the interface.

As shown in *Fig. 1*, up to 128 devices can be used simultaneously, provided that each piece of equipment is (1) HDCP-compliant and (2) recognized (authenticated) as a valid secure implementation. In the context of broadcasting, the *Upstream Content Control Function* is the signalling information delivered from the broadcast stream (e.g. DVB's free-to-air signalling for content protection and copy management – CPCM).

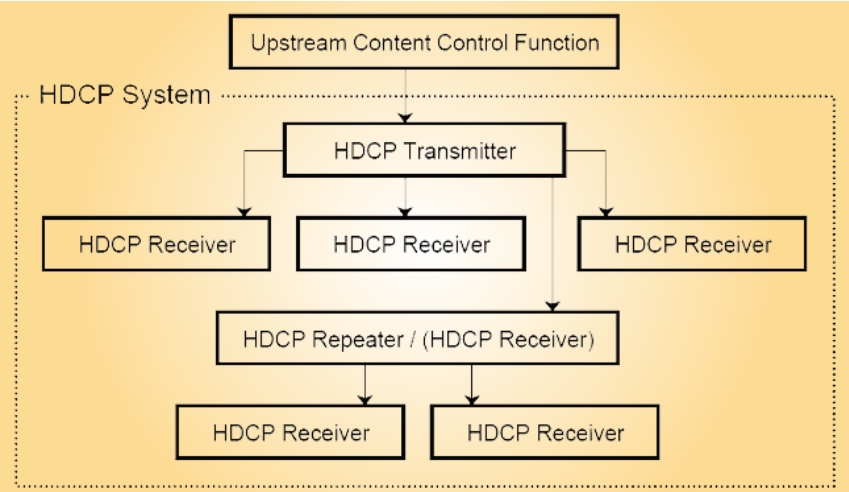

Figure 1
Example of interconnection of HDCP compliant devices

HDCP is based on linear Authentication and Key Exchange (AKE), a process familiar to cryptologists. The AKE process involves the exchange of secret keys that are unique to each and every device. The authentication process assesses the validity of these keys including a revocation control. If the AKE process succeeds, content is encrypted by the transmitter over the link and delivered to the receiver which decrypts it according to rules securely set up during the authentication process, and displayed. If the AKE process fails, the display will probably remain black. Other options are possible such as downscaling the content resolution, which doesn't seem to be widely implemented today.

HDCP is a de facto standard as most manufacturers have licensed the technology from the Digital Content Protection LLC group and abide by contract to a certain number or implementation rules and obligations. DVB has adopted HDMI with HDCP as the associated protection mechanism. Furthermore, HDCP is mandated by EICTA in order to obtain the right to use the "HD Ready" logo.

HDCP content protection

Why?

The main reason for using HDCP is to prevent content being exposed and accessed in the clear, over high-bandwidth high-quality digital interfaces from which material could be extracted e.g. to produce unauthorised copies.

What?

HDCP is a security tool for "content protection". It is not a "copy management mechanism", used to carry and enforce usage restrictions. A copy management mechanism may in turn require the use of security tools such as HDCP to "protect" content. The fact that HDCP is activated has no other meaning than "this content can only be accessed by compliant and authenticated devices" and shall not be subject to interpretation of derived usage restrictions (e.g. "copy never" or "do not redistribute over the Internet"). It is essential to understand, without any ambiguity, the precise nature and specific role of HDCP.

Example: Let's imagine an interface (e.g. other than HDCP) connecting a set-top-box to a PVR. In the case where "copy never" applies to some content, a compliant PVR will not allow copying of this content, by means of deactivating the recording function. Conversely, content may be encrypted over the link between the two devices to prevent tampering with it for unauthorised copying purposes. However, although content might be protected over this link, e.g. if no copy restriction

applies, it shall still be possible to make a copy of this content. Hence “content protection” is not the same as “copy management”.

The actual usage restriction associated with the activation of HDCP is “unauthenticated access to content through this interface is not allowed”. However, a content protection axiom would state that HDCP should be activated whenever content is subject to a usage restriction.

By whom?

The decision to apply or not any content protection and copy management is the decision of the content owner, which subsequently becomes a contractual obligation when content is licensed to service providers e.g. free-to-air or pay-TV broadcasters. Broadcasters are themselves often owners of the content that they produce and to which they may decide not to systematically, if at all, apply content protection and copy management. One should know the potential implications of activation or deactivation of HDCP on user access to “protected” content. The conditions under which HDCP might be used and how it might be used is subject to different circumstances and needs.

As a first example, this article focuses on free-to-air broadcasting but it is interesting to note that certain pay-TV operators wish to have the flexibility to activate HDCP on a content-by-content basis, while it is *deactivated* by default! Other pay-TV operators have specified their proprietary set-top-box boxes with HDCP being *activated* by default.

As far as free-to-air is concerned, different positions have been expressed that correspond to different market and regulatory situations:

Scenario 1

“Free-to-air” (FTA) or “clear-to-air” (CTA). In both cases, access is granted but limited to a particular geographical location when FTA content is delivered in scrambled form. FTA content that has been “protected” for delivery can remain protected after acquisition through the activation of HDCP, which could occur through signalling in the conditional access system (as for pay-TV), or by default in the receiver. There is also a need to be able to deactivate HDCP (and subsequently any similar content protection mechanism) for some content. Content could remain in the clear after geographical delivery unless otherwise instructed through proper “DVB free-to-air signalling information”.

Scenario 2

For CTA content delivered in the clear, some EBU members want HDCP being deactivated by default on CTA-capable devices. If a set-top-box gives access to CTA content and pay-TV content, independently of each other, it should be possible to activate or deactivate HDCP according to the default state originally set unless otherwise instructed through proper “DVB free-to-air signalling information”. HDCP deactivation should preferably be the default condition for such CTA set-top boxes in a horizontal market.

Abbreviations

AKE	Authentication and Key Exchange	**DVI**	Digital Visual Interface
CPCM	(DVB) Content Protection and Copy Management	**EICTA**	European Information, Communications and Consumer Electronics Technology Industry Association
CTA	Clear-To-Air		
DCP-LLC	Digital Content Protection LLC licensing group	**FTA**	Free-To-Air
DTCP	Digital Transmission Copy Protection	**HDCP**	High-bandwidth Digital Content Protection
DVB	Digital Video Broadcasting http://www.dvb.org/	**PVR**	Personal Video Recorder
		SRM	System Renewability Message

Scenario 3

Some CTA broadcasters would prefer HDCP being activated by default with the flexibility to deactivate it for certain content through proper “DVB free-to-air signalling information”.

Scenario 4

If FTA/CTA content is delivered as part of a pay-TV service to pay-TV set-top-boxes, the default HDCP state will be defined by the pay-TV operator as well as the possibility and mechanisms to activate or deactivate HDCP.

The above valid, but diverse, scenarios illustrate the need for HDCP (and similar content protection mechanisms) to be switchable on a content-by-content basis from one initial state (either “on” or “off” by default) to another.

When?

It seems logical to activate HDCP content protection when usage restrictions – such as limited access, copying, redistribution and consumption – apply, because unauthenticated access to content in the clear would allow circumventing these restrictions.

Conditional Access (CA) systems can play the role of Upstream Content Control Function that activates or deactivates HDCP content protection. In some cases, the simple fact that content is delivered in a scrambled form is sufficient to require the activation of HDCP. In other CA configurations, the same channel also carries usage restriction messages, which allows more flexibility such as the activation of HDCP on a content-by-content basis in set-top-boxes with HDCP “off” by default, or for deactivating HDCP for FTA content after acquisition.

DVB considers that CTA content shall be considered as “protected” as long as DVB free-to-air signalling is delivered alongside this content within the broadcast stream. DVB has specified free-to-air signalling to allow or prevent:

1) the redistribution of content over the Internet (control_remote_access_over_the_internet);
2) the scrambling of content (do_not_scramble);
3) the use of revocation lists (do_not_apply_revocation).

If the “do_not_scramble” flag is set to “true”, HDCP should be deactivated. It is acknowledged that, although originally designed to control DVB Content Protection and Copy Management (DVB CPCM) scrambling, this signalling should equally apply to HDCP and similar protection mechanisms independently of the implementation of DVB CPCM.

But when does it really become essential to control content protection over a high-bandwidth “display link”? The answer to that question lies principally in two key implementation features of HDCP, i.e. legacy compliance and revocation.

HDCP compliance

In a perfect world where all devices are HDCP compliant, the “normal” honest user experience would be unaffected by content flowing over the HDCP interface in a scrambled form or not. But there will be a legacy of early adopters with displays without HDCP or, not to be underestimated, displays with “early and not fully-compliant” HDCP implementations.

One of the reasons pay-TV operators switch HDCP “off” by default may have been to ensure access to owners of early displays and to overcome potential early interoperability problems.

FTA broadcasters should share the same concern.

The evolution of the HDCP specification might generate a new legacy ... and, in particular, a greater interoperability challenge – managing the "revocation" lists.

The revocation dilemma

In a fully HDCP-compliant world, having protection "on" by default wouldn't be such an issue if there weren't the additional burden of revocation which, in turn, would be less problematic if managed on a content-by-content basis as recommended by DVB. But HDCP (and other similar protection mechanisms such as DTCP) currently makes this more complicated.

Revocation consists of identifying devices that have been compromised and could be misused as a sink to access content and generate unauthorised copies. A device is "compromised' when (1) a device private key has been cloned and replicated in pirate devices or (2) the private key of that device has been made public (e.g. after being lost or stolen).

"Compromised" devices are identified by their individual keys, compiled into revocation lists which are typically distributed with the content (in the signal or with removable medias) in signed / authenticated "System Renewability Messages" (SRMs) but can also be embedded into new devices. This list is consulted during the HDCP authentication procedure and although the AKE process is successful, a device would not be granted access to content if blacklisted.

The Content Participant Agreement defines the conditions under which content owners who have signed the agreement may request revocation of devices. The responsibility for putting together these revocation lists is with the content owners. Broadcasters are obliged to transmit the lists and react accordingly by the licence contracts they have signed for HDCP.

Although version 1.1 of the HDCP specification was not specific about revocation list management, version 1.2 defines a "device-based" revocation mechanism. This means that revocation lists must be permanently stored into devices. Revocation lists are updated each time a device receives a more recent list either with the content or when interconnected with another device (e.g. a new device with a preloaded revocation list) either directly or through a home network. According to this specification, revocation is "per device" and not "per content".

SRMs are signed using a public key delivered by the Digital Content Protection LLC group. They do not require particular protection to be transmitted. FTA/CTA broadcasters should be asked to collaborate in the delivery of such lists if they require the activation of HDCP.

A buffer of 5 KBytes restricts the number of keys that can be stored in a device to one Vector Revocation List (the individual 40-bit keys of 128 devices), which has a limiting effect on the bandwidth needed to carry the SRMs and its cost for broadcasters. One key of one device can actually deactivate thousands of devices sharing a compromised key.

Crypto-analysis has demonstrated that HDCP could be considered "broken" if 40 keys are compromised. A new version is in preparation, which would justify the handling of more than 128 devices, as envisaged in the HDCP specification. But the use of this new version may raise compatibility and legacy issues.

Why is device revocation dangerous for FTA broadcasters?

If a receiving device that gives access to both free-to-air and pay-TV services has been instructed to blacklist some equipment (e.g. a display) for pay-TV content, then "per device" revocation would result in turning the screen black for pay-TV but also free-to-air services. In this context, the black-screen threat is not in favour of HDCP being set "on" by default. However, a solution has been agreed within DVB by defining the free-to-air signalling flag "do_not_apply_revocation", which allows deactivating revocation on a "per content" basis for the associated FTA/CTA content. Obviously, this solution requires being implemented by HDCP to be effective.

Summary

Like pay-TV operators, FTA/CTA broadcasters across Europe see different possible uses of HDCP but would like the flexibility to activate or deactivate it on a "per content" basis. This is a requirement already endorsed by DVB for more generic "content protection and copy management".

HDCP is only "content protection" and not a "copy management" scheme. Usage restrictions cannot be derived or interpreted from the activation of HDCP but, in principle, HDCP would be activated when usage restrictions apply to content.

HDCP is a de facto standard that has been implemented differently in various proprietary implementations for pay-TV. Meeting the needs of "FTA" broadcasters in the long term, in a horizontal market, may require some adaptation to those currently developed for pay-TV.

In a fully HDCP-compliant world, having content protection "on" by default would not be a problem, notwithstanding the additional burden of revocation. This in turn would be less problematic if managed on a "per content" basis. But HDCP (and other similar protection mechanisms such as DTCP) has opted for "device-based" revocation. In such conditions, pay-TV set-top-boxes that are revoked to protect pay-TV premium content will no longer deliver FTA content to users unless using the DVB FTA switching flag. This must not prevent FTA broadcasters being involved in the revocation decision-making process – to counter-balance the market impact of such actions. FTA broadcasters would be asked to collaborate in the delivery of revocation messages if they require the activation of HDCP.

DVB has agreed a "free-to-air signalling scheme", which offers a solution to several of the key issues mentioned in this article and, more particularly, concerning HDCP activation and "per content" revocation. It is strongly advised that future HDCP implementations respond to such signalling, if not already.

One issue of serious concern to potential FTA broadcaster-users of HDCP is the lack of stability of the specification. The specification has already changed from version 1.1 to version 1.2 and 1.3. There are critical legacy and interoperability issues. The value of HDCP will be weakened if the specification and compliance rules are being changed without open consultation.

Jean-Pierre Evain joined the EBU's Technical Department in 1992 to work on "New Systems and Services", having spent six years in the R&D laboratories of France-Télécom (CCETT) and Deutsche Telekom.

Mr Evain manages all EBU metadata activities. He represents the EBU in several DVB groups regarding metadata as well as Copy Protection and Digital Rights Management. He also represents the EBU in the IPTC consortium (news metadata).

References

1. High-Bandwidth Digital Content Protection System, revision 1.1, 9 June 2003
2. High-Bandwidth Digital Content Protection System, revision 1.2, 13 June 2006
3. High-Bandwidth Digital Content Protection System, revision 1.3, 21 December 2006
4. Conditions for High Definition Labelling of Display Devices, 19 January 2005 (www.eicta.org)