

DTCP-IP and the “AllVid” NOI

The Commission’s “AllVid” Notice of Inquiry suggests that the DTCP-IP technology could protect content output from the AllVid adapter to devices connected on the home network.¹ In its Comments and Reply to the NOI, DTLA welcomed the Commission’s suggestion, and explained in detail how the DTCP technology and licensing terms were well-suited to that purpose. Upon reviewing others’ comments and replies to the FCC, DTLA observed some misconceptions about DTCP-IP. To better inform further discussion of the Commission’s proposal, DTLA addresses five points below:

- DTCP-IP and Conditional Access both fit in an AllVid environment.
- DTCP-IP accommodates Content Owners, MVPDs, and Consumers.
- DTCP facilitates interoperability on the home network.
- DTCP will assure downstream protection of AllVid-delivered content by all devices on the network.
- DTCP enables renewability for DTCP and other protection technologies.

1. DTCP-IP and Conditional Access both fit in an AllVid environment.

DTCP-IP protects the home network, and does not replace or interfere with communications between the AllVid adapter and the MVPD system.

The AllVid adapter concept creates a line of demarcation between communications downstream to the home network and upstream to the MVPD. Conditional access technologies selected by the MVPD protect communications upstream between the “head end” and the adapter. This includes transmission of commands from the AllVid to the MVPD, as well as content and business offers from the MVPD to the consumer. DTCP-IP would reprotect program content output downstream from the AllVid adapter to the home network.

Not all communications between the AllVid adapter and devices on the network need to be encrypted.

In accordance with the Commission’s Encoding Rules (or content owner instructions), some programs would not be protected on the home network. Data, such as remote control commands between the AllVid adapter and devices connected to the network, also would not need to be protected using DTCP.

¹ *In the Matter of Video Device Competition; Implementation of Section 304 of the Telecommunications Act of 1996: Commercial Availability of Navigation Devices; Compatibility Between Cable Systems and Consumer Electronics Equipment*, MB Docket No. 10–91; CS Docket No. 97–80; PP Docket No. 00–67; FCC 10–60, 75 Fed. Reg. 27264 ¶ 28 (May 14, 2010).

2. DTCP-IP accommodates Content Owners, MVPDs, and Consumers.

DTCP-IP is flexible and can accommodate new business models.

DTCP-IP currently has available capacity to carry additional and more nuanced content usage rules for new business opportunities. DTLA is continuing to work cooperatively with content owners and MVPDs to define carriage of information that will enable new business models.

A forthcoming update to the DTCP Specification (called “DTCP+”) will facilitate definition of new and more granular rules and states that can be delivered to devices in a format-agnostic way. DTCP+ includes a Digital Only Token to implement selectable output control to facilitate early-window home access to theatrical motion pictures, pursuant to a recent Media Bureau waiver order.² DTCP+ also will include a “CopyCount” feature for delivery of a specified number of copies, and Remote Access capabilities.

DTCP-IP supports reasonable and customary consumer uses.

Content protected with DTCP-IP can be sent to all DTCP-enabled devices in any room of the house, including portable devices. DTCP conforms with the Commission’s Encoding Rules, which preserve consumers’ reasonable and customary rights to record audiovisual content for their personal use.

- Content marked “Copy Freely” will not be protected with DTCP. This setting must be applied to terrestrial broadcast channels and can be applied to any content.
- Content marked Copy One Generation can be recorded by devices on the home network, such as DVRs or Blu-ray recorders; but those copies cannot be copied again. This setting can be applied to pay subscription channels, or other pay content.
- Copies can be moved from an impermanent medium such as a DVR or hard disk to another DVR or portable device, or to a permanent medium, like a recordable Blu-ray or DVD disc.
- Copy Never setting only can be applied to pay-per-view or video-on-demand.

3. DTCP facilitates interoperability on the home network.

DTCP-IP can interoperate with many protection technologies.

DTCP is designed as a “bridge” to convey content protection usage rules between devices, including between devices that use otherwise incompatible protection systems.

² See *In the Matter of Motion Picture Ass’n of America, Petition for Expedited Special Relief, Petition for Waiver of the Commission’s Prohibition on the Use of Selectable Output Control*, (47 C.F.R. § 76.1903), Memorandum Opinion and Order, CSR-7947-Z, MB Docket No. 08-82 (May 7, 2010).

DTLA continues to work with proponents of other recording or output protection technologies to enable that interoperability. DTLA has not refused any interoperability request, and remains open to approving more, and more sophisticated, systems.

DTCP-IP works with a variety of interfaces.

DTCP-IP operates effectively over any interface that supports Internet Protocol, including physical interfaces like Ethernet and MoCA, and wireless interfaces. Audiovisual content delivered with DTCP-IP can then be output over other interfaces supported by DTCP such as IEEE 1394, WirelessHD, and USB. DTCP can be “mapped” to additional interfaces as well.

DTCP-IP is a two-way network communications protection technology.

DTCP operates over bidirectional digital interfaces. Every DTCP “source” that outputs content can be a “sink” that receives content, and vice versa. Therefore, protected communications between DTCP-enabled devices can be bidirectional.

4. DTCP will assure downstream protection of AllVid-delivered content by all devices on the network.

DTCP-IP technology and licensing assures end-to-end content protection on the home network.

In the AllVid environment, DTCP-IP would re-protect content that had been delivered via conditional access. DTCP-IP *technology* would encrypt that content as it is output from the adapter to other DTCP-enabled devices connected to the home network. DTCP-IP carries “Content Management Information” (“CMI”) that defines rules for how devices must continue to protect the received content, using DTCP or other protection systems. DTCP *license obligations* require all devices that receive DTCP-protected content to continue to protect it, consistent with the CMI, no less strongly than DTCP.

License obligations maintain a “chain of trust” for content owners throughout the home network.

DTLA licenses permit DTCP-protected content to be accessed or recorded only by devices that are no less protective than DTCP in terms of technology and licensing. The three major content owners that license DTCP (“Content Participants”) have the right to review and object to proposed interoperability, so as to assure that their content will remain protected on the home network to their satisfaction. Thus, the combination of robust DTCP technology and licensing terms assures MVPDs and content owners that content usage rules, including the Commission’s Encoding Rules, will be followed throughout the home network. Neither Commission rules nor the MVPDs need to control devices used to record DTCP-protected content.

5. DTCP enables renewability for DTCP and other protection technologies.

DTLA can “revoke” compromised devices.

DTCP uses a “revocation” method if a device’s unique certificate has been compromised (*e.g.*, by being cloned and inserted into multiple devices). Each connected device exchanges and examines a “system renewability message” file (“SRM”). If the certificate of a connected device appears on the list, other DTCP-enabled devices on the network will “ostracize” and will not exchange DTCP-protected content with the revoked device. DTLA has not revoked any device certificate to date because no such compromise has occurred.

DTCP-IP securely conveys SRM files for all content protection systems.

The ATSC standard A/98: System Renewability Message Transport defines how SRM files are conveyed through digital television signals. http://atsc.org/cms/standards/a_98.pdf. DTCP encrypts all data in that transport stream. Therefore, SRM files of other protection systems are protected by DTCP and securely conveyed downstream on the home network. As a result, devices that use other protection technologies are able to extract and respond to relevant SRMs.

A chain of licensing assures that DTCP-enabled devices read and respond to the DTCP.SRM file; the same will happen via an AllVid adapter.

DTCP’s Content Participants can distribute SRMs in recorded media, and their licenses with MVPDs require SRM carriage in transmissions. MVPDs transmit signals (including the SRM files) using conditional access. Licenses to decrypt the conditional access technology require that the DTCP.SRM be delivered to the DTCP source function. The DTCP Specification requires that the DTCP.SRM file will be processed and acted upon. All other SRMs delivered in the content stream (*e.g.*, the HDCP.SRM file) will be reprotected and passed downstream using DTCP-IP. Licenses for technologies that reprotect DTCP-protected data require the devices to process data necessary for operation of their respective technologies, including processing of their respective SRMs.

Content owners assure proper SRM operation through DTCP.

When making interoperability decisions, DTLA and Content Participants specifically review the proposed technology’s system for revocation or renewability. As noted above, DTCP Content Participants have the right to object to interoperability if another technology is not sufficiently robust, including if the technology does not provide for revocation. Consequently, any technology approved for interoperability with DTCP meets the content owners’ criteria for protection, including revocation.