



August 7, 2015

Cheryl Tritt, Chair  
Downloadable Security Technology Advisory Committee  
Federal Communications Commission  
445 12<sup>th</sup> Street, SW  
Washington, D.C. 20554

Re: Supplemental Information concerning Elements of Current DTCP and DTCP-2 for  
Downloadable Security Technology Advisory Committee, MB Docket 15-64

Chairwoman Tritt:

Digital Transmission Licensing Administrator LLC (“DTLA”) is the entity that develops and licenses the DTCP digital transmission content protection “link protection” technology. We have been following the DSTAC discussions concerning the potential role of link protection and DTCP in a downloadable security solution, as referenced in the draft reports of Working Groups 3 and 4, and in presentations and comments at the August 4 meeting. DTLA appreciates the interest of DSTAC members in DTCP and the in-progress improvements to DTCP technology, and we agree that DTCP technology can fulfill an important role in an end-to-end protection solution for audiovisual content delivered by service providers to consumer home and personal networks.

In light of the comments about DTCP in the draft reports and the August 4 meeting, DTLA wishes to submit additional information concerning the current capabilities of DTCP, and the work well underway for the next version of DTCP known as “DTCP-2,” that we hope will prove useful to the Committee’s work.

***Background and Basics.***

DTCP arose from inter-industry working group efforts to identify technologies capable of re-protecting audiovisual content received by a consumer in a protected format (e.g., from a cable or satellite transmission service or protected media such as DVD). Since the initial release of DTCP in 1998, DTLA has evolved DTCP technology and robustness of DTCP to better accommodate new business models and usage rules.

DTCP has five key elements: (1) industry-standard AES-128 encryption to protect content when transmitted between devices and on a home and personal network; (2) robust authentication to ensure that only devices compliant with the DTCP Specification access DTCP-protected content; (3) localization techniques to permit only authorized retransmissions from the home and personal network; (4) secure conveyance of usage rules governing the scope of permitted access, display, retention, recording, copying, and retransmission of protected content; and, (5) effective license protections to ensure that content protected by DTCP remains protected thereafter by technologies and license rules at least as stringent as those for DTCP. DTCP has been mapped to various media transmission protocols, including Internet Protocol (“DTCP-IP”).

DTCP is designed to enable a high degree of interoperability between different content protection systems. “Upstream” providers, such as motion picture studios and MVPDs, and protection technology providers such as AACS LA, CableLabs, and DVD Copy Control Association, currently approve the use of DTCP to re-protect content they distribute in encrypted formats to consumers and customer premises equipment. Under DTCP license requirements, DTCP-protected content only can be output to devices that thereafter will perpetuate that protection (using DTCP or other equally-robust technologies). Usage rules applied “upstream” can be carried securely using DTCP to “downstream” devices that display or record the content using other protection technologies. A list of technologies approved to re-protect content delivered using DTCP is posted on DTLA’s website, at <http://www.dtcp.com/approvedtechnologies.aspx>.

DTLA licenses DTCP on a reasonable and non-discriminatory basis, to more than 170 companies worldwide. It has Content Participant Agreements with three major motion picture companies who review any proposed technology or license changes that could affect the integrity of protections afforded by DTCP. DTLA’s license agreements and non-confidential versions of the DTCP Specifications are posted at <http://www.dtcp.com>.

In December 2011, DTLA released four major enhancements to DTCP, which commonly are referred to as “DTCP+.” These enhancements are:

- *Content Management Information (“CMI”)* formats can convey rich usage rules to support a variety of content owner or service provider business models.
- *Copy Count* enables content providers to offer consumers the ability to make no more than a defined number of copies of particular content.

- *Digital Only Token* facilitates business models (e.g., early-window access) that only allow content to pass through protected digital outputs.
- *Remote Access* enables protected out-of-home access to certain content from home source devices.

CableLabs approved use of the first three DTCP+ enhancements in the DFAST and <tru2way> license agreements, and informed DTLA that it is unnecessary for DTLA to obtain CableLabs approval for Remote Access as it is outside the scope of their output approval process.

DTLA works closely with DLNA to support the VidiPath guidelines for streaming protected television programming to DLNA-certified devices. Currently, DTLA is developing DTCP-2 to meet content industry robustness requirements for the re-protection of content delivered to consumers as High Dynamic Range or with resolution above HD (“Enhanced Image” content).

We elaborate below on aspects of DTCP that may be relevant to the work of DSTAC.

***1. DTCP Content Management Information (CMI) carries rich content usage rules to support content and service provider business models.***

DTCP CMI formats enable content owners and service providers to convey more and more sophisticated content usage rules to accommodate particular business models. DTLA adopted CMI as a means to securely and interoperably transport these content usage rules in a manner agnostic to the transmission format being used. In addition to copy control information (“CCI”) and other usage rules carried in earlier DTCP descriptors, CMI formats currently also convey rules for Copy Count and Digital Only Token. Future CMI formats will carry data pertinent to usage rules for Enhanced Image content protected using DTCP-2. CMI is flexible and extensible enough to define new formats of usage rules to facilitate numerous content owner and service provider business models. As one example: DTCP’s existing Retention State field enables eight fixed periods for sell-through, rental, or limited-time viewing; but CMI is capable of conveying more granular date and time (e.g., calendar/clock) information to support such models.

Connected Licensed Products will use CMI where both the source and sink are CMI-capable. When communicating with devices compliant with earlier versions of the

Specification, the recommended default is to process the rules provided in simpler descriptors. (For example, a receiving device that does not support Copy Count could allow the making of copies if and as permitted by the CCI settings.)

Accordingly, DTCP with CMI today and in the future can securely convey a rich set of usage rules, defined to support new content owner and service provider business models, to compliant products that follow the specified usage conditions and requirements.

***2. DTCP Remote Access protects personal access to certain content outside the consumer's home network.***

In cooperation with its Content Participants, DTLA defined technical and license requirements whereby remotely-located devices can use DTCP to access certain content from home devices. Technical requirements are provided in DTCP Specification versions 1.7 and above. DTCP license agreements prescribe Compliance Rules terms and conditions governing Remote Access. Licensees can choose their preferred technologies implement these requirements. The requirements include:

- a. **Authentication.** A device that will be used to remotely receive content must first be authenticated locally with the remote source/server, so as to establish that the device does satisfy all DTCP authentication requirements when connected directly on the home network. The device certificate of the remote receiving device will be entered on the server's Remote Sink Registry, and the registered device thereafter can authenticate remotely with the home server. Up to 20 devices can be registered at a time. The process is described in Specification Volume 1 Supplement E at 10.7.
- b. **Compliance Rules.** Compliance Rules in the DTCP license agreement define what content may be accessed remotely. Remote access to consumer-recorded stored content is permitted either by streaming to the remote device (without making a remote copy) or by a Move of the copy from the home to the remote device (storing the copy locally without streaming). Home recording of a program must be complete before remote access to that content may begin. Remote access to "live" protected content is permitted only if the upstream service delivering the content affirmatively permits it. Absent such permission, the default is no retransmission of "live" protected content. Because this permission is granted

before the content is to be protected using DTCP, DTLA does not prescribe how the upstream service signals that permission to the navigation device; the service provider decides whether to offer that capability and how to affirmatively indicate permission to allow remote access to live transmissions. CMI can be used to convey downstream that affirmative permission condition.

- c. **Limits on Transmissions and Retransmissions.** A remote access source may concurrently transfer remotely-accessible content to no more than one sink function. Daisy-chaining is not allowed—the receiving sink may transmit the content to other devices within that receiver’s home network, but may not further make the content remotely accessible except in accordance with the above rules.

As with all changes to DTCP and its agreements, Remote Access was reviewed and accepted by our three motion picture studio Content Participants before its inclusion in DTCP+. DTCP Remote Access is used in other countries. DTLA knows of no impediment to United States consumers using Remote Access for content recorded or received from MVPD systems, using downloadable security.

### ***3. DTCP-2 will provide robust and effective protection for Enhanced Image Content.***

DTLA is developing DTCP-2 as a more robust digital transmission content protection system for Enhanced Image content. In general, the capabilities of today’s DTCP (including DTCP+ features) will be carried forward into DTCP-2, with a higher level of robustness equivalent to or greater than HDCP 2.2 , which has been approved as a digital output protection method for such content, consistent with MovieLabs recommendations pertinent to link protection. The main new attributes of DTCP-2 are summarized below.

- a. **Enhanced Authentication.** The DTCP-2 Specification will require use of a 256-bit Elliptic Curve for authentication. This robustness upgrade also will help ensure that DTCP-2 protected Enhanced Image content will be output only to products with equally high robustness.
- b. **Core Functions in Hardware.** DTCP-2 will require implementation in Hardware of core functions such as encryption/decryption, authentication, and storage and handling of cryptographic parameters).

- c. **New Compliance Rules.** Additional Compliance Rules for Enhanced Image content will include:
- i. A definition of Enhanced Image encompassing both HDR content and content with resolutions higher than HD; but excluding content that has been downresolved from an Enhanced Image to lower resolution.
  - ii. No analog output of an Enhanced Image will be permitted.
  - iii. Permitted outputs will be limited to digital outputs protected by technological methods approved for protection of Enhanced Image content.
  - iv. Recording of Enhanced Image content, and a Move of such recordings to other devices, will be permitted only where using technological methods approved for recording and Move of Enhanced Image content.

DTLA anticipates these efforts will be completed within the next several months. DTLA intends to obtain approval for DTCP-2 to re-protect Enhanced Image content received from “upstream” protection technologies, including AACS2 and technologies used to protect Enhanced Image content delivered by MVPDs. In the interim, DTLA understands that content providers have permitted some MVPDs to use DTCP-IP with additional robustness requirements for protected transmission of UHD content on the home and personal network.

***4. DTCP can protect content from outside the home to customer premises equipment.***

For more than a year, DTLA has been cooperating with companies interested in enabling the use of DTCP from head-end or cloud servers to DTCP-compliant customer premises equipment. This proposal has the benefit of streamlining the delivery process for both the server and client, by eliminating the need to descramble and re-scramble content when initially received in the home. The proponents envision that this proposal could be implemented compatibly on systems using the DLNA VidiPath guidelines.

The distinguishing feature of this application is that it relies on the content provider to assure the content is being delivered to an authorized consumer via the service provider’s network, in addition to DTCP authentication that affirms both the server and client are DTCP-compliant.

Cheryl Tritt, DSTAC Chair

August 7, 2015

Page 7

Initial evaluations show that such a DTCP or DTCP-2 “cloud-to-ground” implementation poses no greater risk of exposure of content, and we are aware of no “show-stoppers” to this proposal. Work on the fundamentals of this proposal is substantially complete. Should this method be of interest, DTLA would be pleased to facilitate cooperation with those companies contributing to this effort.

\* \* \*

DTLA hopes this information will prove useful to the work of the DSTAC, and request that it be distributed to all DSTAC members. Should you have any additional questions or comments, please feel free to contact us at your convenience.

Respectfully submitted,

*/s/ Stephen P. Balogh*

*/s/ Seth D. Greenstein*

*/s/ Michael Andre*

Stephen P. Balogh  
President, DTLA

Seth D. Greenstein  
Chair, DTLA Policy Group

Michael Andre  
Chair, DTLA  
Technical Working  
Group

CC: Brendan Murray  
Nancy Murphy  
WG3 FCC Liaisons Sagar Doshi, Julissa Marengo  
WG4 FCC Liaisons Scott Jordan, John Kiefer, Alison Neplokh  
WG3 Co-editors Adam Goldberg and Bruce McClelland  
WG4 Co-editors Brant Candelore and John Card II

Digital Transmission Licensing Administrator  
225 Cochrane Circle, Suite B Morgan Hill, CA 95037 Tel: +1 408-776-2014 Fax: +1 408-779-9291