Digital Transmission Licensing Administrator

DTCP2

Presentation to CPTWG
April 5, 2017

Need for DTCP2

- Studios require higher robustness content protection systems for newer higher resolution video formats
- DTCP2 developed for "Enhanced Image" (e.g., 4K, 8K, HDR) as well as current audiovisual formats
- Address marketplace concerns
  - Tighten distribution requirements for components
  - Promotion of renewability
  - Third party review option
  - Prompt revocation for materially non-Compliant products of non-Adopters and rogue Adopters

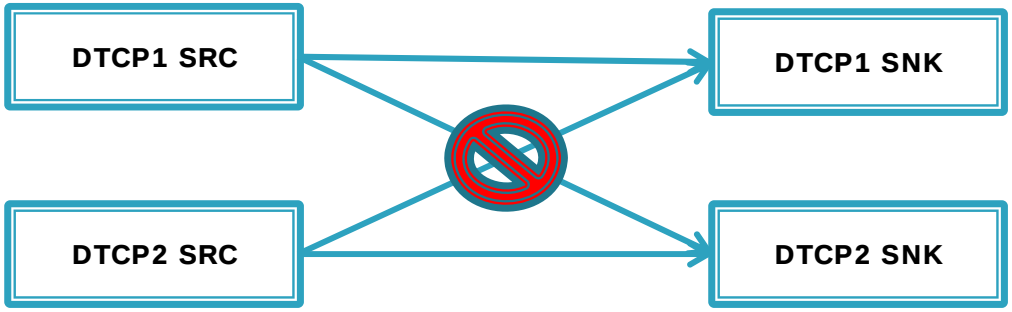
DTCP2 Protection Basics

- DTCP2 is a separate technology from currently-licensed DTCP platforms ("DTCP1")
- Embodied in a new, separate DTCP2 Specification
- Stronger cryptographic elements than DTCP1
- DTCP2 Core Functions implemented in hardware
- Meets or exceeds MovieLabs requirements for link protection systems

DTCP2 - Cryptographic Elements

- NIST P-256 Elliptic Curve
  - Increased cryptographic strength over existing curve
- AES-128 encryption
- SHA-256
  - Increased hash authentication over current SHA-1
- One type of Authentication (similar to Full Authentication in DTCP1)
- NIST SP 800-90A Rev1 for DRNG

Distinct from DTCP-IP



DTCP-IP and DTCP2 do not interoperate as they use different sized elliptic curves.

Four New DTCP2 Tokens

- "L2-Only" Token
- "EI" (Enhanced Image) Token
- "HDR" Token
- "SDO" (Standard Digital Output) Token, set per upstream requirements, consistent with other outputs
- Perpetuate protections downstream

L2-Only Token

- Settings
  - 0 = Content may be protected using L1 or L2
    - Protected output permitted as Enhanced Image or Non-Enhanced Image
  - 1 = Content shall be protected using L2
    - May be downconverted to non-EI but must be protected using L2

- "L2" requires higher level Compliance and Robustness Rules.
- "L1" requires DTCP1 level Compliance and Robustness Rules.

Note: Both L1 and L2 permit output using current and future content protection technologies approved per change management.

EI Token

- Settings
  - 0 = Content is Non-Enhanced Image
  - 1 = Content is Enhanced Image

  - "Enhanced Image"
    - i.e., audiovisual works with image quality surpassing "HD" audiovisual works (i.e., resolution at <=1920x1080 pixels, standard color space for HD quality (BT.709), and standard peak luminance for HD quality (100 nits)).
  - "Non-Enhanced Image"
    - i.e., image quality at or below HD audiovisual works

HDR Token

- Settings
  - 0 = Content with HDR may be downconverted to SDR
  - 1 = Content with HDR may not be downconverted to SDR (unless permission is signaled using non-DTCP2 methods)
- HDR Token of 1 requires use of SDR version available to the Sink Device, to avoid problems caused by HDR-to-SDR downconversion or displays that do not support HDR

SDO Token

- Inherits SDO as set by content owner under AACS2 rules
- Settings
  - 1 = Content may be passed to any Approved L1 or L2 output

Logic for Tokens

- Source device should apply tokens consistent with other outputs permitted by upstream rules
  - i.e., upstream technology should similarly restrict the same content when passed to other technologies
- Devices should respond logically to token combinations
  - Examples:
    - If upstream technology permits L1 output of EI content, then HDR token should be deemed non-asserted (Don't Care)
    - If upstream technology sets SDO token, then L2-Only token and HDR token should be deemed non-asserted (Don't Care)

Results of Token Combinations

L2-Only Token	HDR Token	EI Token	Output Results
1 (Asserted)	1 (Asserted)	*Don't care*	•L2 required •No downconversion to SDR •L1 not permitted
1 (Asserted)	0 (Not Asserted)	*Don't care*	•L2 required for both Enhanced Image and Non-Enhanced Image •Downconversion to SDR permitted •L1 not permitted

Results of Token Combinations

L2-Only Token	HDR Token	EI Token	Output Results
0 (Not Asserted)	*Don't Care*	1 (Asserted)	•L2 required for Enhanced Image •L1 permitted for Non-Enhanced image downconverted from Enhanced Image
0 (Not Asserted)	*Don't Care*	0 (Not Asserted)	•L2 and L1 permitted

DTCP2 – Licensing

- New DTCP2 Specification
  - Mapped initially to IP
- New DTCP2 Adopter Agreement
- New Compliance and Robustness Rules for Adopter Agreement
- Addendum to Content Participant Agreement
- IP Statement
  - Enables any content owner to require DTCP2 encoding without license or fee

DTCP2 Adopter Agreement

- Standalone DTCP2 agreement
  - Procedural Appendix, Confidentiality Agreement, Compliance Rules, Robustness Rules, Robustness Verification List

- Major New Elements:
  - Election of Renewability or Third Party Review of the Robustness Verification List
  - Additional Revocation Criteria/Safe Harbor
  - Greater controls over distribution of Licensed Components that contain DTCP2 Keying Material

Two Levels of Compliance and Robustness Rules

- **L2** requires higher levels of robustness and output/recording protection
  - Compliance Rules require higher output protection (such as HDCP2.2 and DTCP2); analog output not permitted
- **L1** permits handling of content in a manner equivalent to current DTCP-IP
- Robustness Rules require DTCP2 "Core Functions" to be implemented in Hardware for both L1 and L2

Renewability or Third Party Review

Adopter chooses one of the following:

- Make DTCP2 Implementation Core Functions Renewable
  - Exempt for portions implemented in physical hardware
  - Complete and submit Robustness Verification List to DTLA's agent
- Submit Robustness Verification List and Supporting Documentation for Third Party Review
  - Obtain Certificate confirming compliance of RVL with Robustness Rules.
  - No Revocation based on non-compliance of Implementation that passes Third Party Review ("Safe Harbor")
- Hybrid (non-Renewable portions of Renewable Implementations)

Implementation ID

- Identifies Adopter and DTCP2 Implementation
- Five Byte field
  - Adopter ID (3B) assigned by DTLA
  - Implementation Number (2B) assigned by Adopter
- Cannot use same Implementation ID for different Implementations
- Optional for Certain Cases
  - Can use instead Common Device Certificate or substantially contiguous sequential numbering of Unique Device Certificates

Licensed Components (1)

- Licensed Components without Keying Material can be sold to Fellow DTCP2 Adopters and Have Made Parties.

Licensed Components (2)

- Licensed Components with Keying Material can be sold to Fellow DTCP2 Adopters (and their Have Made Parties) for incorporation into that Fellow DTCP2 Adopter's Licensed Products
  - Fellow DTCP2 Adopter orders the Keying Material, or
  - Sale by Approved Licensed Component Adopter

Licensed Components (3)

- Licensed Components with Inactive Keying Material can be distributed to Fellow DTCP2 Adopters, and Adopter's Have Made Party
  - Rendered operational by activation under control of Adopter that distributed such Licensed Components
- Recordkeeping and reporting requirements apply to Licensed Components with Keying Material and with Inactive Keying Material

Additional Revocation Criteria

- If DTCP2 keying material appears in non-compliant non-Adopter products
- Non-compliant Renewable Implementations (after reasonable time to release Update)
- Products deliberately designed to allow unauthorized unprotected output or copying of Decrypted DT Data
- Where material noncompliance causes material and adverse effect re DTCP2 protection, likely to result in commercially significant harm to Content Participants

Reciprocal Non-Asserts

- DTCP Adopters have Addendum option to grant and receive reciprocal non-assertions of Necessary Claims from DTCP2 Adopters and DTCP2 Content Participants
- DTCP2 Adopters grant reciprocal non-assertions of Necessary Claims to DTCP Adopters that sign Addendum and DTCP2 Content Participants

Addendum for Content Participants

- Applies CPA provisions to DTCP2
- Adds right to encode new tokens (L2-Only, Enhanced Image, and HDR)
- Applies additional Revocation Criteria from DTCP2 Adopter Agreement

DTCP2

Questions?