Digital Transmission Content Protection (DTCP)

Overview of DTCP and DTCP2 Compliance and Robustness

June 2018

Overview

- Protects audiovisual content on Home and Personal Network
  - “Link” Protection
  - Interoperable Solution
  - Technology and License Requirements
- Two types co-exist:
  - DTCP for up to High Definition Content
  - DTCP2 also for Enhanced Definition Content
    - UHD 4K, 8K, High Dynamic Range
  - DTCP and DTCP2 are not interoperable.
- Information at www.dtcp.com

DTCP is “Link” Protection

- DTCP/DTCP2 protect content as transmitted between devices and between content protection technologies across home and personal networks
- Content is received in protected form, examples:
  - Cable or satellite conditional access
  - Blu-ray with AACS
  - DVD with CSS
- Content protected with DTCP/DTCP2 can be re-protected for storage or output protection using robust interoperable technologies

From Protected Sources to a Protected Home Network

BROADBAND
Entertainment,
E-Business, Services

MEDIA
Pre-Recorded Content
Personal Media

BROADCAST
Services,
Entertainment

DTCP Multi-Industry Support

DTCP:

- Worldwide Adopters (Licensees)
  - Chip manufacturers
  - TV, manufacturers
  - Cable and satellite box manufacturers
  - Player and recorder manufacturers
  - Mobile device manufacturers
  - Home Media Servers and Adapters

DTCP2:

- Licensing began in July 2017

DTCP/DTCP2 Specifications

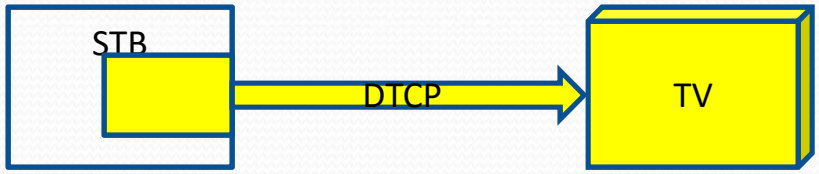
- DTCP Rev. 1.71 (February 2015)
  - Supplements include IP, HLS, MOST, USB, Wireless HD
- DTCP2 Rev. 1.0.1 (January 2018)
- Non-confidential versions can be downloaded for review
  - DTCP -- http://www.dtcp.com/specifications.aspx
  - DTCP2 -- http://www.dtcp.com/specifications2.aspx

Technical Elements

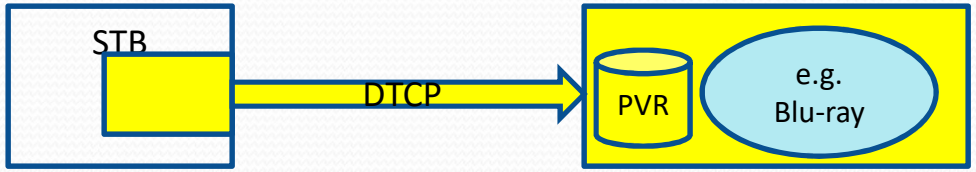
- Authentication and Key Exchange (AKE)
  - More robust Elliptic Curve parameters in DTCP2
- AES-128 Content Encryption
- Localization preventing unauthorized redistribution outside the Home and Personal Network
  - Remote access permitted
- System Renewability/Revocation
- Conveys Content Usage Rules
  - Permitted outputs
  - Scope of permissible recording

DTCP/DTCP2's main features - examples

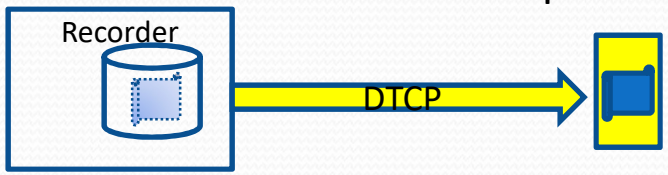
Streaming to a TV at home



Transmission to a recorder for PVR or removable recording such as Blu-ray



"Move" recorded content to a personal device



Remote access from a smart phone to recorded content at home

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

Five New DTCP2 Tokens

- "L2-Only" Token
  - Higher robustness required
- "EI" (Enhanced Image) Token
  - Greater than High Definition (e.g., UHD 4K, 8K)
- "HDR" Token
  - For High Dynamic Range content
- "SDO" (Standard Digital Output) Token
  - Set per upstream requirements
- "AET" Audio Enhancement Token
  - Permits digital audio transmission at higher quality

Implementation ID

- Identifies Adopter and DTCP2 Implementation
- Different Implementation ID to be used for different Implementations
- Optional where Adopter uses
  - Common Device Certificate or
  - Substantially contiguous sequential numbering of Unique Device Certificates

DTCP and DTCP2 Licensing

- Separate Adopter Agreements for DTCP and DTCP2
- Non-assertion Addendum for DTCP
  - Exchange and receive non-assertion covenants with DTCP2 Adopters and Content Participants
- Content Participant Agreement for DTCP with Addendum for DTCP2
- IP Statement
  - Enables any content owner to require DTCP or DTCP2 encoding without license or fee

Adopter Agreement

- **Compliance Rules**
  - Technical requirements specify the treatment and processing of protected content transported using DTCP/DTCP2. For example:
    - Rules for storing protected content
    - Rules for temporary retention of protected content
      - (e.g., PVR pause, Rental)
    - Rules for output of protected content to permitted outputs
    - Rules for "moving" content from temporary storage to permanent storage
    - Rules for remote access

Adopter Agreement

- **Robustness Rules**
  - Technical description of how licensed products must be designed and manufactured to frustrate attempts to defeat the content protections of DTCP and DTCP2
  - Levels of Robustness Rules:
    - DTCP has one level.
    - DTCP2 requires—
      - "L1" Rules basically the same as DTCP
      - More stringent "L2" Rules
      - Hardware Root of Trust
      - Secure Execution Environment
  - Robustness Verification List guides manufacturer compliance with DTCP2 Robustness Rules requirements

Adopter Agreement

- **Revocation**
  - Unique device certificate may be revoked if found to breach prescribed criteria in Adopter Agreement, including:
    - Loss, theft, cloning of device certificate and key (DTCP1 and DTCP2)
    - Device Key and Certificate in Non-Adopter product (DTCP2)
    - Deliberate design to allow unauthorized copying or output, or material noncompliance causing commercially significant harm (DTCP2)
  - Common device certificate may be revoked either if breach of criteria, or at any time commencing 48 months after issuance (DTCP and DTCP2).

Certificate Revocation

- Purpose: Preclude exchange of DTCP and DTCP2 protected content with revoked devices
- Devices receive and process System Renewability Messages (SRM) that lists revoked Device Certificates.
- Licensed products exchange SRMs after authentication is completed.
- SRMs generated by DTLA.

Renewability and Review

- For DTCP2, manufacturer must elect whether to –
  - Make Implementation Renewable, or
  - Submit Implementation to a Third Party Review Authority for independent robustness review

Renewability (DTCP2)

- “Renewable” products can update implementation of DTCP2 Core Functions
- Renewable implementations that become compromised shall be renewed
  - Implementation may be revoked after commercially reasonable time to complete renewal

Robustness Review (DTCP2)

- Non-renewable portions of Implementations must have Review process before product launch.
- Review by independent security firm to determine compliance with DTCP2 Robustness Rules
  - Based on completed Robustness Verification List and supporting documentation
- Can choose from Review firms approved by DTLA
- Implementations that pass Review generally will not be revoked
  - Benefit for Review

DTCP2 Component Supply Chain Control (1)

- Licensed Components without Keying Material can be sold only to DTCP2 licensees and "have made" parties
  - Keys can be installed only by Adopter or have made party manufacturing Licensed Product
- Licensed Components with Keying Material cannot be sold by Adopter unless—
  - Buyer is a Fellow DTCP2 Adopter who orders the keys from DTLA
  - Seller is a DTLA Approved Licensed Component Adopter who sells only to Fellow DTCP2 Adopter that manufactures Licensed Product

DTCP2 Component Supply Chain Control (2)

- Licensed Components with Inactive Keying Material
  - Non-operational as sold, activated following sale
  - Can be distributed to have made party or Fellow DTCP2 Adopter
  - Activation by DTCP2 Adopter using cryptographically protected remote communication or tool at time of manufacture of Licensed Product
- Recordkeeping Obligations for Licensed Components with Keying Material or Inactive Keying Material
  - When placing key orders, track and notify DTLA of past key usage and remaining inventory

Content Participant Agreement

- Content owners can sign agreements with DTLA for DTCP and DTCP2
- Benefits
  - Third party beneficiary rights, including injunctive relief against material breaches of the compliance rules or robustness rules.
  - Right to object to changes to DTCP/DTCP2 that could have a material and adverse impact on their rights.
  - Right to request revocation, when one of revocation criteria is met.
- Three Content Participants for DTCP and DTCP2: Sony Pictures Entertainment, Warner Bros., Disney Technology and Licensing

Encoding Rules

- Limits “Copy Never” encoding in Major Recorder Markets (i.e., Japan, UK, EU, Australia, NZ)
- Parity of protection among comparable technologies for same means of distribution
- For DTCP2, requires proper application of DTCP2 Tokens (Enhanced Image, HDR, L2, AET)
- Encoding Rules also reflected in IP Statement

Summary

- DTCP and DTCP2 protect against unauthorized redistribution and copying.
- Promotes home and personal network interoperability and transport of protected commercial content
- Separate Adopter Agreement licenses for DTCP and DTCP2.
- DTCP and DTCP2 co-exist and are not interoperable.
- Robustness Rules and Renewability/Review required (DTCP2 only) to ensure product robustness against attacks
- Strict supply chain obligations for DTCP2 Licensed Components with keys

Further Information

- http://www.dtcp.com to download:
  - Non-confidential versions of DTCP Specification and all Supplements and DTCP2 Specification
  - License Agreements for DTCP and DTCP2
  - List of approved output and recording technologies
- Questions to dtcp-services@dtcp.com

Digital Transmission Content Protection DTCP and DTCP2