Digital Transmission Content Protection (DTCP)

Technical and Licensing Overview

Digital Transmission Licensing Administrator

Overview

- DTCP as part of Home Network Protection Framework
  - “Link” Protection
  - Technology and Licensing Chain
- DTCP
  - Technical Elements
  - Licensing Elements

What is DTCP?

- Method of protecting audio and audiovisual entertainment content on home and personal network over high-bandwidth bidirectional digital interfaces
- Created by 5 companies – Hitachi, Intel, Matsushita, Sony and Toshiba (the “5C”)

From Protected Sources to a Protected Home Network

BROADBAND
Entertainment,
siness, Services

MEDIA
Pre-Recorded Content
Personal Media

Home Network

BROADCAST
Services,
Entertainment

DTCP is “Link” Protection

- DTCP was developed to be one link in a chain of technologies and licenses.
- Protected content that enters the home is delivered to devices that also protect content stored and enjoyed across home and personal networks.
- Flexible, extensible and interoperable.

DTCP Multi-Industry Support

- Motion picture studio support
- More than 140 licensees worldwide
  - Chip manufacturers
  - TV manufacturers
  - Cable and satellite box manufacturers
  - Recorders
  - Home Media Servers and Adapters

DTCP Authorized Uses

- CableLabs approval of DTCP-IP and DTCP-1394 for uni- and bi-directional digital cable products
- Japan Digital Terrestrial TV and Digital Satellite TV
- DVD CCA Approval of DTCP for IP, MOST and IDB 1394, and IEEE 1394 for CSS-enabled DVD players
- Outputs from DVD and D-VHS recorders
- DLNA and OMA/CMLA approval for DTCP-IP
- HANA approval for DTCP-1394
- Output from AACS-enabled HD DVD & Blu-ray players

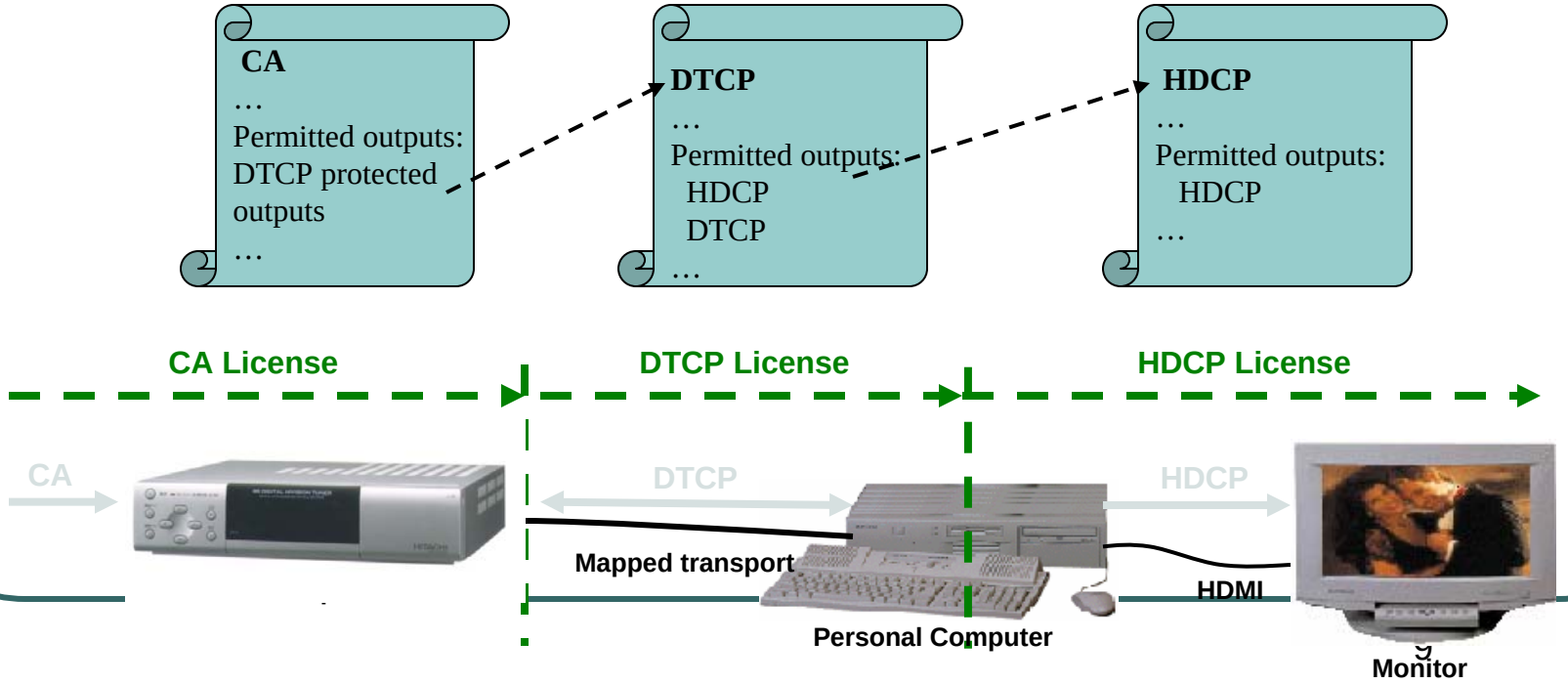
DTCP Interoperability

- Protected retransmission over HDCP (HDMI, DVI), Windows Media DRM* and DTCP over other protocols
- Protected storage on
  - D-VHS
  - CPRM (for DVD-R/-RAM/-RW and SD Card)
  - CPS for BD-RE
  - VCPS (for +R/+RW)
  - MG-R(SVR) for Memory Stick PRO / Hi-MD
  - Windows Media DRM*

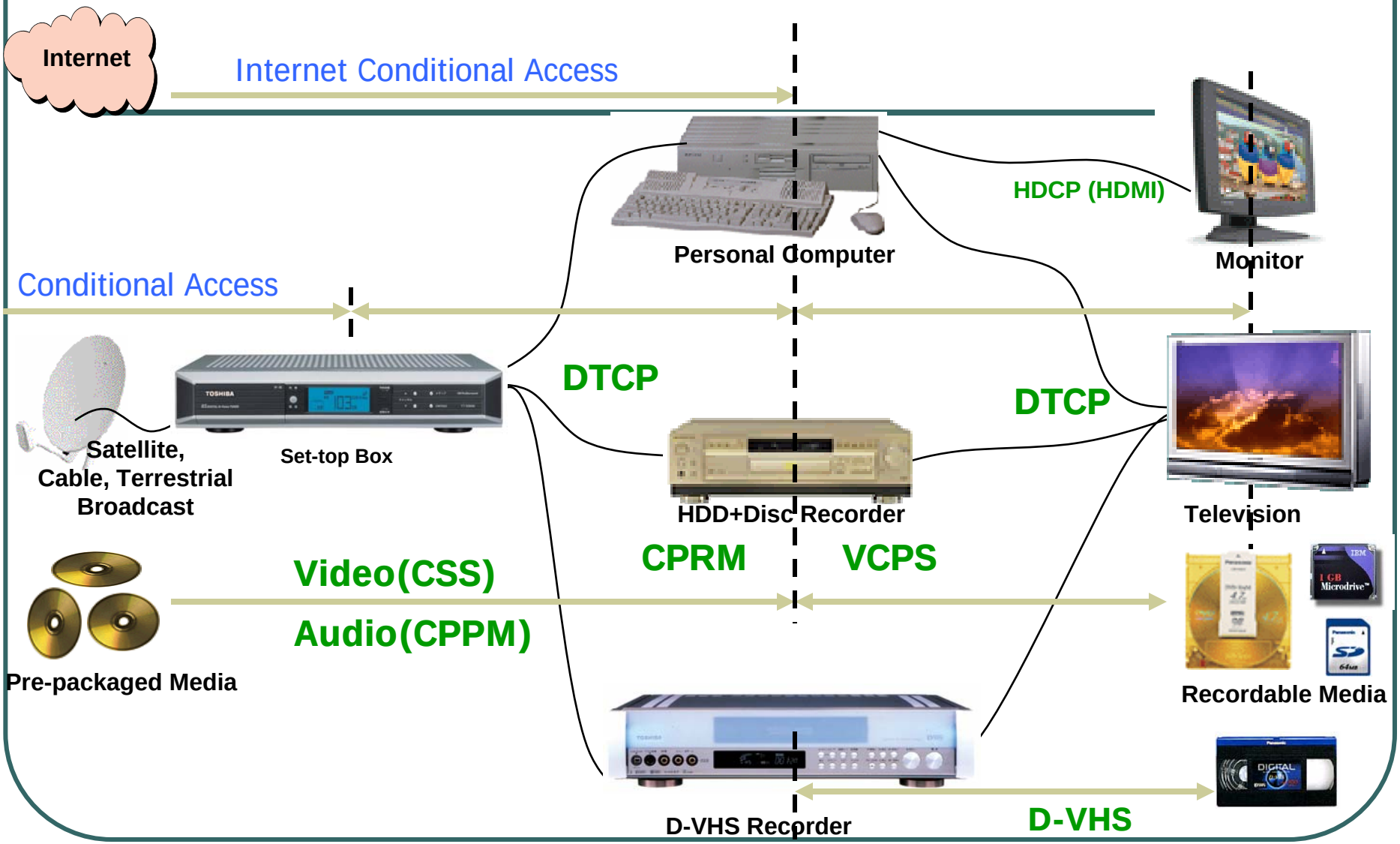
** Provisional approval for Windows Media DRM versions 10 and higher*

Chain of Licensing and Technology

- Permits a variety of marketplace technologies that support current and future content delivery business models.

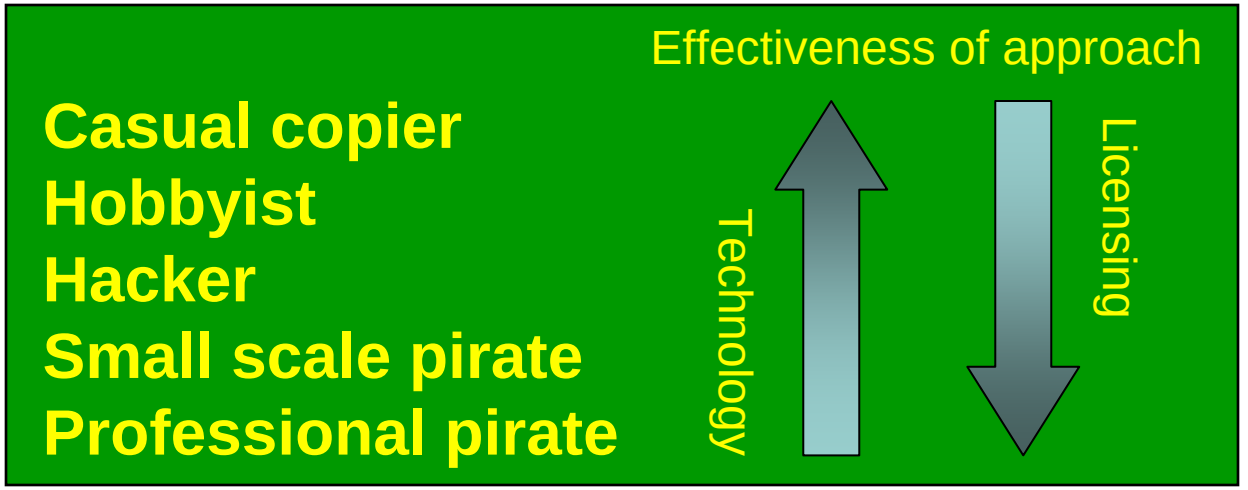


Result: End-To-End Content Protection



DTCP Protection Framework

- DTCP combines technical mechanisms for content protection with an effective licensing structure for enforcement.



DTCP Specifications

- First issued in 1998
- Latest Specification v. 1.5 (June 2007)
- Supplements map DTCP to interconnects
  - Currently, DTCP protocol mapped to IP, IEEE1394 (included related transports such as IDB 1394 and OP i.Link), USB, MOST and Bluetooth.
- Informational versions can be downloaded for review

Technical Elements

- Authentication and Key Exchange (AKE)
- Content Encryption
- Copy Control Information (Usage Rules)
  - Encryption Mode Indicator
  - Embedded CCI
- System Renewability

Authentication

- Two authentication levels are offered to satisfy scalability and provide efficient content protection implementations.
  - **Full authentication** can be used with all content and is required for content marked as Copy Never.
  - **Restricted authentication** enables protection of content marked as copy-one-generation and no-more-copies.

Key Exchange

- Three cryptographic keys:
  - **Authentication key** which is formed as a result of authentication and used to protect the exchange keys.
  - **Exchange key** which is used to set up and protect content streams.
  - **Content key** which is used to encrypt the content being exchanged.

Content Encryption

- Balance robustness and implementation efficiency.
- Baseline Cipher
  - M6 for 1394, USB, and MOST.
  - AES-128 for DTCP-IP.
- Can support additional optional ciphers, the use of which is negotiated during authentication.

Embedded CCI

- Carried as part of the content stream and identifies rules associated with content.
- Integrity of embedded CCI is ensured since tampering with content stream results in erroneous decryption of content.
- Only devices capable of processing the content can process this form of CCI.

Embedded CCI		Meaning
Copy-never		Content is not to be copied.
Copy-one-generation		Permission to make one generation of copies.
No-more-copies		When copy of content marked Copy-one-generation is made it is remarked as No-more-copies.
Copy-freely	EPN Asserted	Unlimited protected copies are permitted.
	EPN Unasserted	Not protected by DTCP.

Additional DTCP-IP Attributes

- DTCP over Internet Protocol
- Over all interfaces
- Wired or Wireless
- Localization (redistribution control)
  - Time To Live packet/”hops” <= 3
  - WEP, WAP/equivalents or successors
  - Round Trip Time <= 7 milliseconds

System Renewability

- Device with full authentication capabilities can receive and process System Renewability Messages (SRM).
- SRMs are exchanged between DTCP licensed products after authentication is completed.
- SRMs are generated by DTLA and delivered via content.

Licensing Elements

- Adopter Agreement
- Content Participant Agreement
  - IP Statement

Adopter Agreement

- **License Grant**
  - License to all “necessary” patent claims, trade secrets, and copyrights is granted only to implement the technology in a manner consistent with the Specification and license terms, including the robustness and compliance rules.
- **Specification changes**
  - DTLA will not make mandatory material changes to the specification but may make limited changes to enable DTCP to be used with additional interconnects.

Adopter Agreement

- **Compliance Rules**
  - Technical requirements included in the Adopter Agreement that specify the treatment and processing of protected content transported using DTCP. For example:
    - Rules for storing protected content
    - Rules for “pausing” protected content (e.g., PVRs)
    - Rules for output of protected content
    - Rules for “moving” content from temporary storage to permanent storage

Adopter Agreement

- **Robustness Rules**
  - Technical description of how licensed products must be designed and manufactured in order to frustrate attempts to defeat the content protections of DTCP.

Adopter Agreement

- **Revocation**
  - Individual device certificates will be revoked if a device's private key has been lost, stolen, intercepted, misdirected or publicly disclosed, or has been cloned into another device, or if revocation is required by a government authority.

Adopter Fees

- Based on Cost Recovery
- Annual administration fee
  - Evaluation only -- $10,000
  - Small Adopter -- $14,000
  - Large Adopter -- $18,000
- Device Key/Certificate Generation Fee
  - Small Adopter -- $.06-.07
  - Large Adopter -- $.05-.06

  - Note: “Small” vs. “Large” enables Adopter to choose the less expensive alternative

Content Participant Agreement

- Content owners can sign agreements with DTLA
- Right to approve changes to DTCP that could have a material and adverse impact on their rights.
- Injunction against material breaches of the compliance rules or robustness rules.

Content Participant Agreement

- Encoding Rules limit application of CCI to particular types of content.
  - Prerecorded media, Pay Per View, Video on Demand can be encoded “Copy Never”
  - Premium cable or satellite TV can be encoded “Copy One Generation”
    - Copies are marked “Copy No More”
  - Copy Never and Copy One Generation content also can be transmitted as Encrypted Copy Freely (EPN)
  - Broadcast TV and basic subscription TV can be encoded as “Copy Freely”

IP Statement

- Content owners can use DTCP without a license if they follow the Encoding Rules.

Summary

- DTCP protects against unauthorized redistribution and copying.
- Security protocols are same for all transports.
- Promotes home and personal network interoperability and transport of protected commercial content.
- Inexpensive, low technical overhead.

Further Information

- http://www.dtcp.com to download
  - Informational versions of Specification and all Supplements
  - Adopter Agreement
  - Content Participant Agreement
  - IP Statement