VIDEOLABS

Hisense

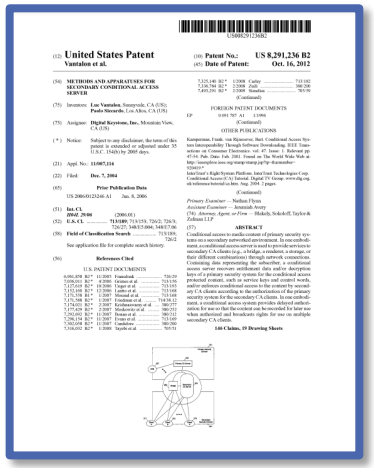
VideoLabs – Hisense Licensing Discussion

Claim Charts for US-8291236 & US-8667304

Confidential and Subject to FRE408

June 7, 2023

Exemplary Hardware Patents (US) cont.



(12) **United States Patent**
Vantalon et al.

(10) **Patent No.: US 8,291,236 B2**
(45) **Date of Patent: Oct. 16, 2012**

(54) **METHODS AND APPARATUSES FOR SECONDARY CONDITIONAL ACCESS SERVER**

(75) Inventors: **Luc Vantalon**, Sunnyvale, CA (US); **Paolo Sicuranza**, Los Altos, CA (US)

(73) Assignee: **Digital Keystone, Inc.**, Mountain View, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 2005 days.

(21) Appl. No.: **11/007,114**

(22) Filed: **Dec. 7, 2004**

Prior Publication Data

US 2006/0123246 A1 Jun. 8, 2006

(51) **Int. Cl.**
H04L 29/06 (2006.01)

(52) **U.S. Cl.** **713/189**; 713/153; 726/2; 726/3; 726/26; 340/5.64; 340/12.066; 340/12.06

(58) **Field of Classification Search** 713/189, 713/153; 726/2
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

ABSTRACT

146 Claims, 19 Drawing Sheets

US8,291,236

(12) **United States Patent**
Vantalon et al.

(10) **Patent No.: US 8,667,304 B2**
(45) **Date of Patent: *Mar. 4, 2014**

(54) **METHODS AND APPARATUSES FOR SECONDARY CONDITIONAL ACCESS SERVER**

(75) Inventors: **Luc Vantalon**, Sunnyvale, CA (US); **Paolo Sicuranza**, Los Altos, CA (US)

(73) Assignee: **Digital Keystone, Inc.**, Mountain View, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **13/612,643**

(22) Filed: **Sep. 12, 2012**

Prior Publication Data

US 2013/0007471 A1 Jan. 3, 2013

Related U.S. Application Data

(63) Continuation of application No. 11/007,114, filed on Dec. 7, 2004, now Pat. No. 8,291,236.

(51) **Int. Cl.**
H04L 29/06 (2006.01)

(52) **U.S. Cl.**
USPC **713/189**; 713/153; 713/168; 726/2; 726/3; 340/5.64; 340/12.066; 340/12.06

(58) **Field of Classification Search**
None
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

ABSTRACT

22 Claims, 19 Drawing Sheets

US8,667,304

Secured transmission of digital content between different Digital Rights Management domains (DRM bridging)

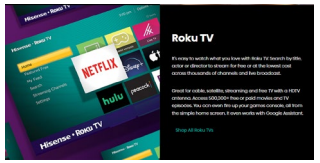
Relevant to video headend/server and Smart TV/media streamer/STB

Acquired from Digital Keystone April 2023

Exemplary VL Patents Confirmed Relevant to Hisense**

Hisense Smart TV

Hisense Android STB



Hisense Smart TV Content Streaming & App Mgmt

7,769,238 CAVLC decode	★	★	
7,970,059 CABAC decode	★	★	
9,066,124 Video/audio power mgmt	●		
8,291,236 DRM bridging	●		'236 & '304 claim charts vs Hisense Smart TVs with HDCP provided herein on June 7, 2023 U.S. *
8,667,304 DRM bridging	●		
8,605,794* DASH/HLS Streaming			★ S
7,440,559* Channel Mgmt			★

● = Rule 11 claim chart
★ = patent previously litigated
S = DASH SEP

* = **Foreign EP counterpart**
** = VideoLabs analysis ongoing

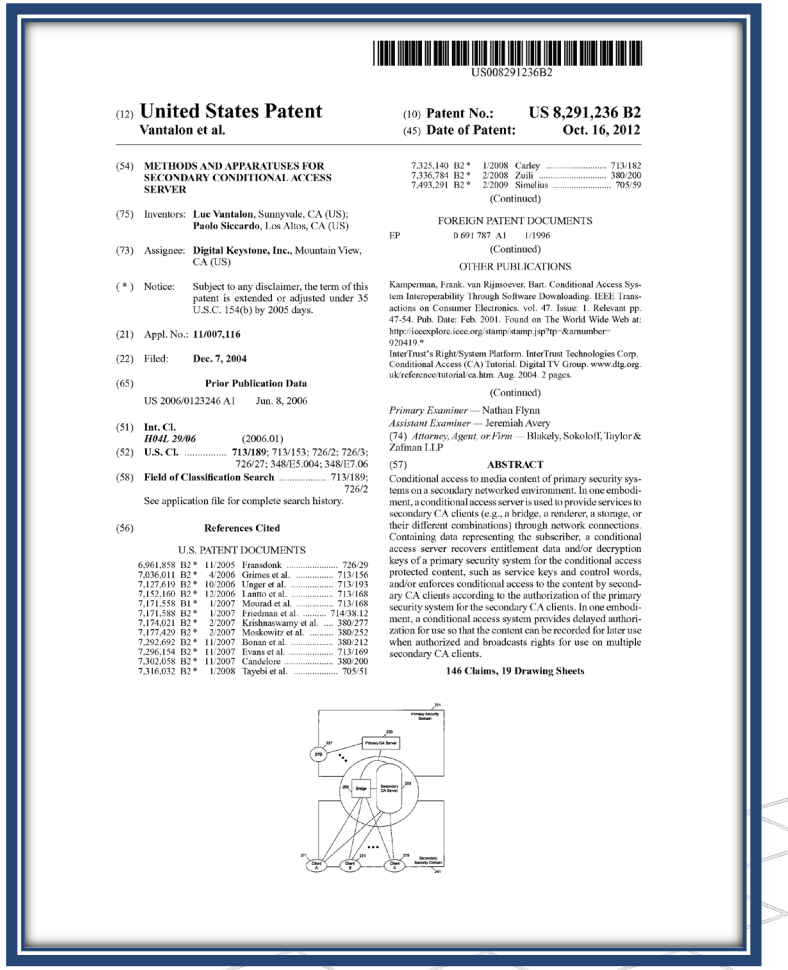
** All other noted claim charts were provided to Hisense on April 18, 2023 U.S.*

VIDEOLABS

US Patent No. 8,291,236 Against Hisense Smart TVs With HDCP

EX. 2006

U.S. Patent No. 8,291,236



US008291236B2

(12) **United States Patent**
Vantalon et al.

(10) **Patent No.: US 8,291,236 B2**
(45) **Date of Patent: Oct. 16, 2012**

(54) **METHODS AND APPARATUSES FOR SECONDARY CONDITIONAL ACCESS SERVER**

(75) Inventors: **Luc Vantalon**, Sunnyvale, CA (US); **Paolo Siccardo**, Los Altos, CA (US)

(73) Assignee: **Digital Keystone, Inc.**, Mountain View, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 2005 days.

(21) Appl. No.: **11/007,116**

(22) Filed: **Dec. 7, 2004**

(65) **Prior Publication Data**

US 2006/0123246 A1 Jun. 8, 2006

(51) **Int. Cl.**
H04L 29/06 (2006.01)

(52) **U.S. Cl.** **713/189**; 713/153; 726/2; 726/3; 726/27; 348/E5.004; 348/E7.06

(58) **Field of Classification Search** 713/189; 726/2

See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

6,961,858	B2 *	11/2005	Fransdonk	726/29
7,036,011	B2 *	4/2006	Grimes et al.	713/156
7,127,619	B2 *	10/2006	Unger et al.	713/193
7,152,160	B2 *	12/2006	Lantto et al.	713/168
7,171,558	B1 *	1/2007	Mourad et al.	713/168
7,171,588	B2 *	1/2007	Friedman et al.	714/38.12
7,174,021	B2 *	2/2007	Krishnaswamy et al.	380/277
7,177,429	B2 *	2/2007	Moskowitz et al.	380/252
7,292,692	B2 *	11/2007	Bonan et al.	380/212
7,296,154	B2 *	11/2007	Evans et al.	713/169
7,302,058	B2 *	11/2007	Candelore	380/200
7,316,032	B2 *	1/2008	Tayebi et al.	705/51
7,325,140	B2 *	1/2008	Carley	713/182
7,336,784	B2 *	2/2008	Zuili	380/200
7,493,291	B2 *	2/2009	Simelius	705/59

(Continued)

FOREIGN PATENT DOCUMENTS

EP	0 691 787	A1	1/1996

(Continued)

OTHER PUBLICATIONS

Kamperman, Frank. van Rijnsoever, Bart. Conditional Access System Interoperability Through Software Downloading. IEEE Transactions on Consumer Electronics. vol. 47. Issue: 1. Relevant pp. 47-54. Pub. Date: Feb. 2001. Found on The World Wide Web at: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=920419.*
InterTrust's Right/System Platform. InterTrust Technologies Corp. Conditional Access (CA) Tutorial. Digital TV Group. www.dtg.org.uk/reference/tutorial/ca.htm. Aug. 2004. 2 pages.

(Continued)

Primary Examiner — Nathan Flynn
Assistant Examiner — Jeremiah Avery
(74) *Attorney, Agent, or Firm* — Blakely, Sokoloff, Taylor & Zafman LLP

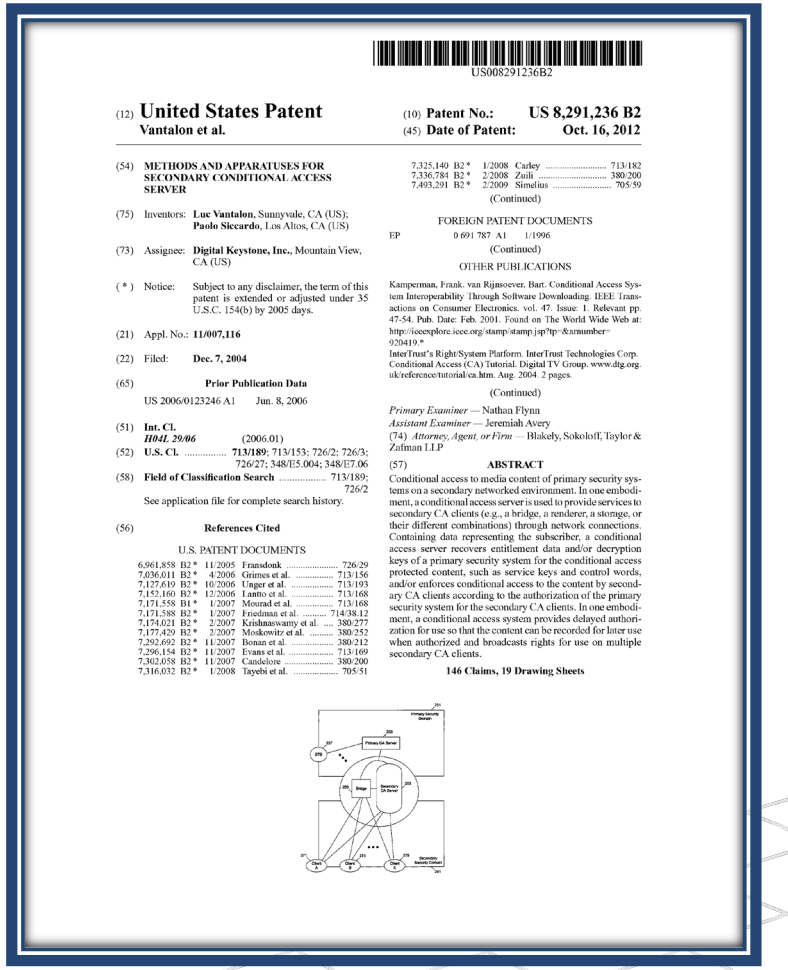
(57) **ABSTRACT**

Conditional access to media content of primary security systems on a secondary networked environment. In one embodiment, a conditional access server is used to provide services to secondary CA clients (e.g., a bridge, a renderer, a storage, or their different combinations) through network connections. Containing data representing the subscriber, a conditional access server recovers entitlement data and/or decryption keys of a primary security system for the conditional access protected content, such as service keys and control words, and/or enforces conditional access to the content by secondary CA clients according to the authorization of the primary security system for the secondary CA clients. In one embodiment, a conditional access system provides delayed authorization for use so that the content can be recorded for later use when authorized and broadcasts rights for use on multiple secondary CA clients.

146 Claims, 19 Drawing Sheets

- **Inventor**: Luc Vantalon, Paolo Siccardo
- **Priority Date**: December 7, 2004
  Expiration Date: June 4, 2030
- **Summary of Technology**: DRM bridge between two independent security domains
- **Claim Mapping**: Hisense TVs with HDCP

U.S. Patent No. 8,291,236, Claim 140



US008291236B2

(12) **United States Patent**
Vantalon et al.

(10) **Patent No.: US 8,291,236 B2**
(45) **Date of Patent: Oct. 16, 2012**

(54) **METHODS AND APPARATUSES FOR SECONDARY CONDITIONAL ACCESS SERVER**

(75) Inventors: **Luc Vantalon**, Sunnyvale, CA (US); **Paolo Siccardo**, Los Altos, CA (US)

(73) Assignee: **Digital Keystone, Inc.**, Mountain View, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 2005 days.

(21) Appl. No.: **11/007,116**

(22) Filed: **Dec. 7, 2004**

(65) **Prior Publication Data**

US 2006/0123246 A1 Jun. 8, 2006

(51) **Int. Cl.**
H04L 29/06 (2006.01)

(52) **U.S. Cl.** **713/189**; 713/153; 726/2; 726/3; 726/27; 348/E5.004; 348/E7.06

(58) **Field of Classification Search** 713/189; 726/2

See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

6,961,858 B2 * 11/2005 Fransdonk 726/29
7,036,011 B2 * 4/2006 Grimes et al. 713/156
7,127,619 B2 * 10/2006 Unger et al. 713/193
7,152,160 B2 * 12/2006 Lantto et al. 713/168
7,171,558 B1 * 1/2007 Mourad et al. 713/168
7,171,588 B2 * 1/2007 Friedman et al. 714/38.12
7,174,021 B2 * 2/2007 Krishnaswamy et al. 380/277
7,177,429 B2 * 2/2007 Moskowitz et al. 380/252
7,292,692 B2 * 11/2007 Bonan et al. 380/212
7,296,154 B2 * 11/2007 Evans et al. 713/169
7,302,058 B2 * 11/2007 Candelore 380/200
7,316,032 B2 * 1/2008 Tayebi et al. 705/51
7,325,140 B2 * 1/2008 Carley 713/182
7,336,784 B2 * 2/2008 Zuili 380/200
7,493,291 B2 * 2/2009 Simelius 705/59
(Continued)

FOREIGN PATENT DOCUMENTS

EP 0 691 787 A1 1/1996
(Continued)

OTHER PUBLICATIONS

Kamperman, Frank. van Rijnsoever, Bart. Conditional Access System Interoperability Through Software Downloading. IEEE Transactions on Consumer Electronics. vol. 47. Issue. 1. Relevant pp. 47-54. Pub. Date: Feb. 2001. Found on The World Wide Web at: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=920419.*
InterTrust's Right/System Platform. InterTrust Technologies Corp. Conditional Access (CA) Tutorial. Digital TV Group. www.dtg.org.uk/reference/tutorial/ca.htm. Aug. 2004. 2 pages.
(Continued)

Primary Examiner — Nathan Flynn
Assistant Examiner — Jeremiah Avery
(74) *Attorney, Agent, or Firm* — Blakely, Sokoloff, Taylor & Zafman LLP

(57) **ABSTRACT**

Conditional access to media content of primary security systems on a secondary networked environment. In one embodiment, a conditional access server is used to provide services to secondary CA clients (e.g., a bridge, a renderer, a storage, or their different combinations) through network connections. Containing data representing the subscriber, a conditional access server recovers entitlement data and/or decryption keys of a primary security system for the conditional access protected content, such as service keys and control words, and/or enforces conditional access to the content by secondary CA clients according to the authorization of the primary security system for the secondary CA clients. In one embodiment, a conditional access system provides delayed authorization for use so that the content can be recorded for later use when authorized and broadcasts rights for use on multiple secondary CA clients.

146 Claims, 19 Drawing Sheets

Claim 140. A secondary conditional access client, comprising:

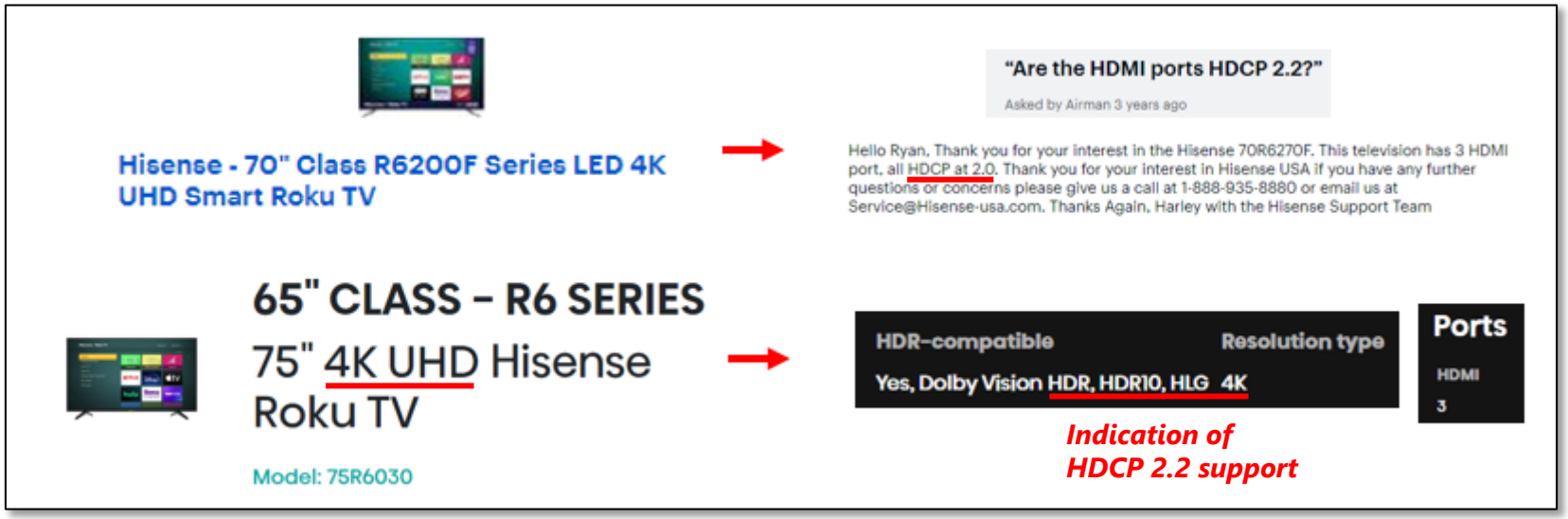
a communication interface to receive, from a conditional access server through a network connection, access controlled data that is in an access controlled format and that is at least partially derived from a security message of a primary security system in a first security domain, the secondary conditional access client being in a second security domain; and

a processor coupled to the communication interface, the processor to process the access controlled data,

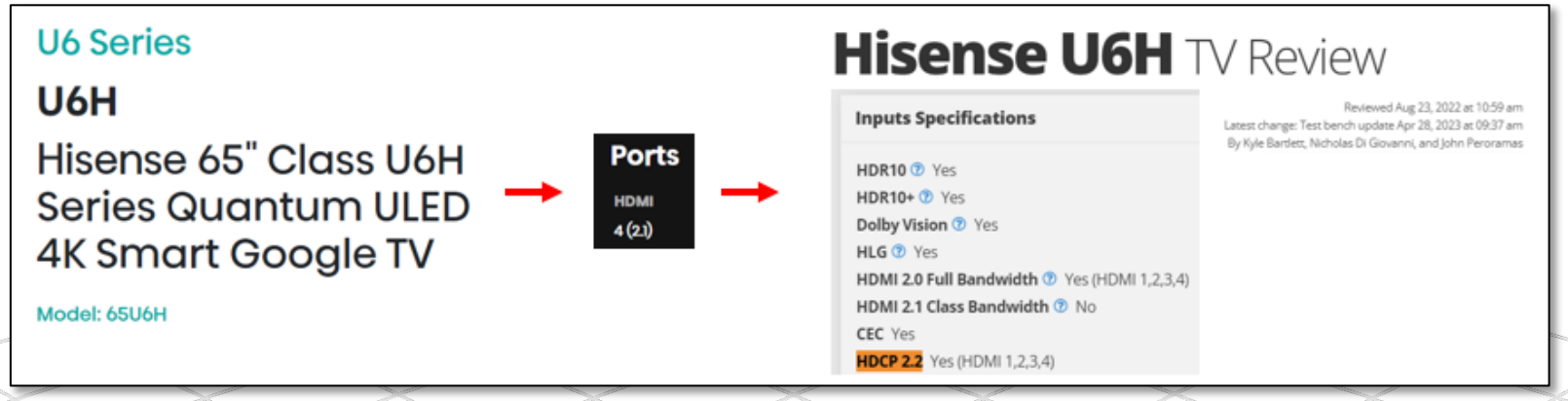
wherein the primary security system authenticates the conditional access server as one of clients of the primary security system through a first authentication process using a first root of trust and the conditional access server authenticates clients of the conditional access server through a second authentication process which is independent of the first authentication process and wherein the second authentication process uses a second root of trust which is independent of and different than the first root of trust,

and wherein the conditional access server is configured to substitute the first security domain with the second security domain for the clients under the second root of trust.

Hisense's Smart TV Platform Devices All Support HDCP



Exemplary Hisense Roku TVs support HDCP 2.x security over HDMI



Exemplary Hisense Google/Android TVs support HDCP 2.2 security over HDMI

Sources:

- https://www.bestbuy.com/site/questions/hisense-70-class-r6200f-series-led-4k-uhd-smart-roku-tv/6378023/question/27db90b1-3884-3c16-aba2-321e1249578a
- https://www.hisense-usa.com/televisions/75r6030-75-4k-uhd-hisense-roku-tv-with-hdr-2020#ProductDetailsBox7
- https://www.hisense-usa.com/televisions/65u6h-hisense-65-inch-u6h-series-quantum-uled-4k-smart-google-tv-2022#ProductDetailsBox17
- https://www.rtings.com/tv/reviews/hisense/u6h

U.S. Patent No. 8,291,236 Against Hisense Smart TVs

Claim 140. A secondary conditional access client [A], comprising:
a communication interface [B] to receive, from a conditional access server [C] through a network connection [D], access controlled data [E] that is in an access controlled format and that is at least partially derived from a security message [F] of a primary security system [G] in a first security domain [H], the secondary conditional access client [A] being in a second security domain [I]; and

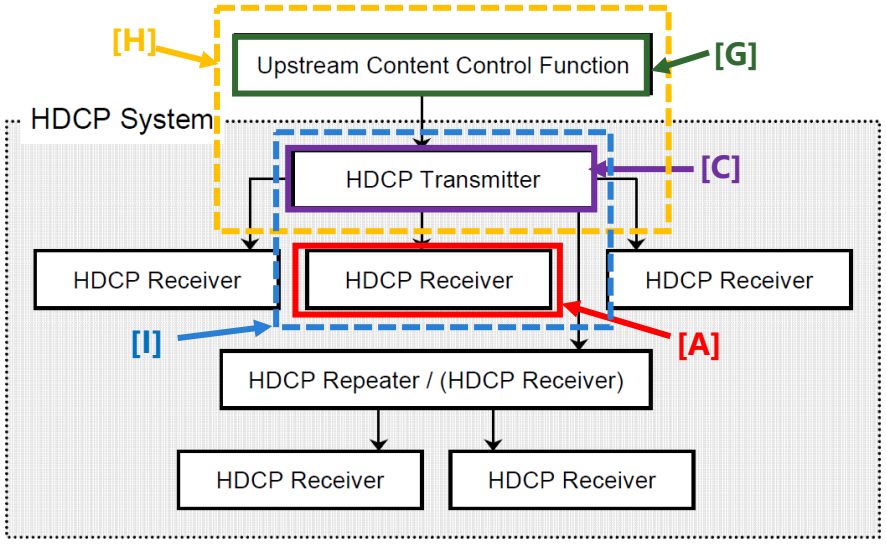


Figure 1.1. Sample Connection Topology of an HDCP System

HDCP on HDMI Specification, Rev. 2.2

For the purpose of this specification, it is assumed that the Audiovisual content is transmitted over a HDMI based wired display link. In an HDCP System, two or more HDCP Devices are interconnected through an HDCP-protected Interface. The Audiovisual Content flows from the Upstream Content Control Function into the HDCP System at the most upstream HDCP Transmitter. From there the Audiovisual Content encrypted by the HDCP System, referred to as HDCP Content, flows through a tree-shaped topology of HDCP Receivers over HDCP-protected Interfaces. This specification describes a content protection mechanism for: (1) authentication of HDCP Receivers to their immediate upstream connection (i.e., an HDCP Transmitter), (2) revocation of HDCP Receivers that are determined by the Digital Content Protection, LLC, to be invalid, and (3) HDCP Encryption of Audiovisual Content over the HDCP-protected Interfaces between HDCP Transmitters and their downstream HDCP Receivers. HDCP Receivers may render the HDCP Content in audio and visual form for human consumption. HDCP Receivers may be HDCP Repeaters that serve as downstream HDCP Transmitters emitting the HDCP Content further downstream to one or more additional HDCP Receivers.

HDCP on HDMI Specification, Rev. 2.2

Hisense's Smart TVs are HDCP-compliant devices and incorporate an HDCP receiver component to receive HDCP encrypted content securely over an HDMI interface

U.S. Patent No. 8,291,236 Against Hisense Smart TVs

Claim 140. A secondary conditional access client [A], comprising:
a communication interface [B] to receive, from a conditional access server [C] through a network connection [D], access controlled data [E] that is in an access controlled format and that is at least partially derived from a security message [F] of a primary security system [G] in a first security domain [H], the secondary conditional access client [A] being in a second security domain [I]; and

Exemplary Roku TV

HDMI interface

Exemplary Google TV

Sources:

- *https://www.hisense-usa.com/televisions/75r6030-75-4k-uhd-hisense-roku-tv-with-hdr-2020#ProductDetailsBox7*
- *https://www.hisense-usa.com/televisions/65u6h-hisense-65-inch-u6h-series-quantum-uled-4k-smart-google-tv-2022#ProductDetailsBox17*

[H]

Set-top boxes & casting	PlayReady	Widevine MODULAR	FairPlay Streaming	WisePlay	Widevine CLASSIC
Chromecast	✓	✓	✗	✗	✗
Android TV	✓	✓	✗	✗	✗
Roku	✓	✓	✗	✗	✗
Apple TV					
Amazon Fire TV					
Google TV (2010-2014)					

[H]

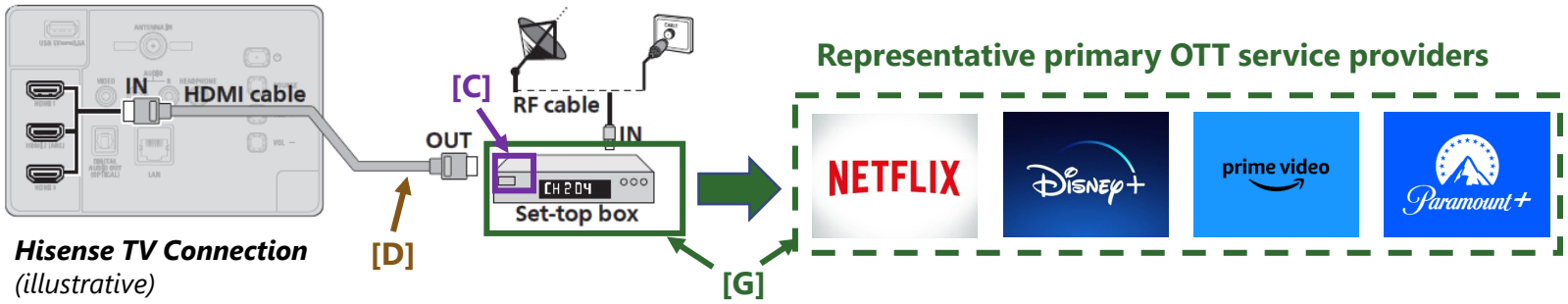
Smart TVs	PlayReady	Widevine MODULAR	FairPlay Streaming	WisePlay	Widevine CLASSIC
Samsung (Tizen) 2018+ MODELS	✓	✓	✗	✗	✗
Samsung (Tizen) 2016-2017 MODELS	✓	✓	✗	✗	✓
Samsung (Tizen & Orsay) 2010-2015 MODELS	✓	✗	✗	✗	✓
LG (webOS 3.0+)	✓	✓	✗	✗	✓
LG (webOS 1-2 & Netcast)	✓	✗	✗	✗	✓
Huawei (HarmonyOS)	✗	✓	✗	✓	✗
Android TV	✓	✓	✗	✗	✗
Smart TV Alliance LG, PHILIPS, TOSHIBA, PANASONIC	✓	✓	✗	✗	✗

Source: https://castlabs.com/resources/drm-comparison/

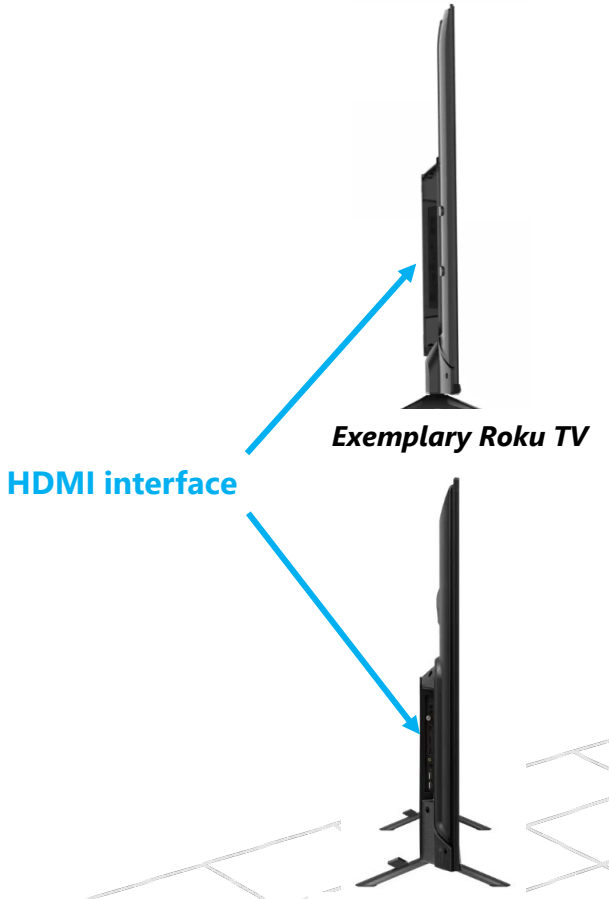
DRM-protected content from the primary OTT streaming provider is received securely by the Hisense Smart TV over the HDMI connection as HDCP encrypted content in accordance with the requirements of HDCP security messages specified by the primary OTT streaming provider

U.S. Patent No. 8,291,236 Against Hisense Smart TVs

Claim 140. A secondary conditional access client [A], comprising:
a communication interface [B] to receive, from a conditional access server [C] through a network connection [D], access controlled data [E] that is in an access controlled format and that is at least partially derived from a security message [F] of a primary security system [G] in a first security domain [H], the secondary conditional access client [A] being in a second security domain [I]; and



Hisense TV Connection
(illustrative)



Exemplary Roku TV

Exemplary Google TV

[H]

Microsoft PlayReady

3.6.5 **Output Control for Uncompressed Digital Video Content**

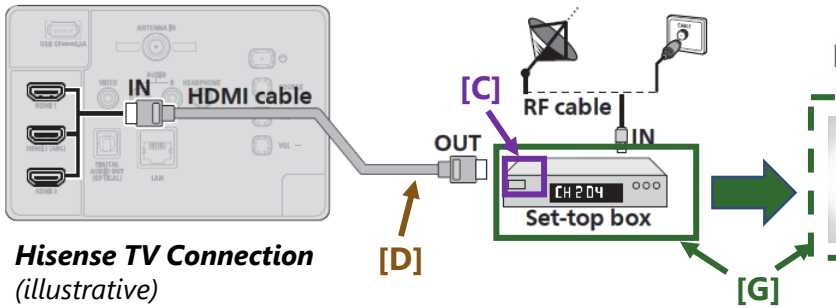
If a PlayReady Product Passes the video portion of uncompressed decrypted A/V Content, the PlayReady Product must follow restrictions as specified in the License and this Section 3.6.5 (Output Control for Uncompressed Digital Video Content). In PlayReady Licenses and WMDRM-ND Licenses, the Output Protection Level is specified in the *Minimum Uncompressed Digital Video Output Protection Level* field of the *Output Protection Level Restriction Object*. In WMDRM-PD Licenses, this Output Protection Level is specified in the ***RESTRICTIONS\UNCOMPRESSEDDIGITALVIDEO*** node.

Compliance Rule for PlayReady Products

DRM-protected content from the primary OTT streaming provider is received securely by the Hisense Smart TV over the HDMI connection as HDCP encrypted content in accordance with the requirements of HDCP security messages specified by the primary OTT streaming provider

U.S. Patent No. 8,291,236 Against Hisense Smart TVs

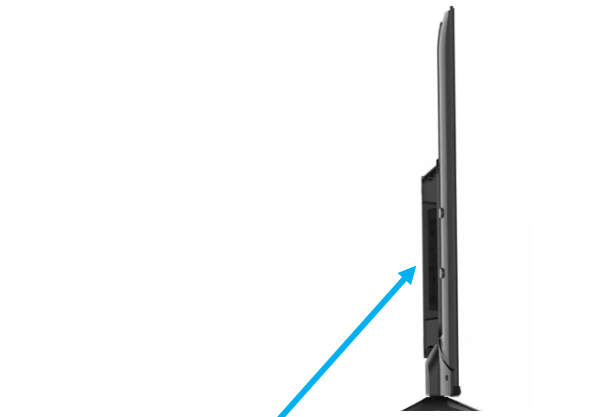
Claim 140. A secondary conditional access client [A], comprising:
a communication interface [B] to receive, from a conditional access server [C] through a network connection [D], access controlled data [E] that is in an access controlled format and that is at least partially derived from a security message [F] of a primary security system [G] in a first security domain [H], the secondary conditional access client [A] being in a second security domain [I]; and



Hisense TV Connection
(illustrative)

Representative primary OTT service providers

NETFLIX | Disney+ | prime video | Paramount+



Exemplary Roku TV

HDMI interface

Exemplary Google TV

[H] WIDEVINE

[F]

content_key_specs. required_output_protection. hdcp	string - one of: HDCP_NONE, HDCP_V1, HDCP_V2	Indicates whether HDCP is required. *Default = HDCP_NONE.* *Note: These must be capitalized, lowercase will result in a malformed request.* See Appendix.

Widevine DRM Proxy Integration

DRM-protected content from the primary OTT streaming provider is received securely by the Hisense Smart TV over the HDMI connection as HDCP encrypted content in accordance with the requirements of HDCP security messages specified by the primary OTT streaming provider

U.S. Patent No. 8,291,236 Against Hisense Smart TVs

Claim 140. A secondary conditional access client [A], comprising:
a communication interface [B] to receive, from a conditional access server [C] through a network connection [D], access controlled data [E] that is in an access controlled format and that is at least partially derived from a security message [F] of a primary security system [G] in a first security domain [H], the secondary conditional access client [A] being in a second security domain [I]; and

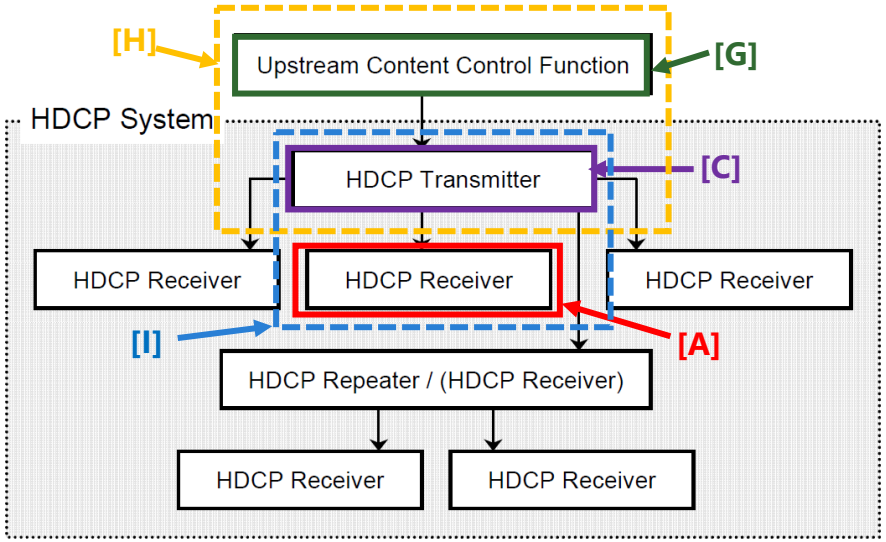


Figure 1.1. Sample Connection Topology of an HDCP System

HDCP on HDMI Specification, Rev. 2.2

Hisense Smart TVs are HDCP-compliant devices and incorporate an HDCP receiver component to receive HDCP encrypted content securely over an HDMI interface

OPL	Compressed Digital Video	Uncompressed Digital Vi		
	Any	HDMI, DVI, DisplayPort,		
0-100	Block	Passes content		
101-150				
151-200				Passes content when CGMS-A CopyNever is engaged.
201-250		Attempts to engage HDCP, but passes content regardless of result.		Does NOT pass content
251-270		**SWDRM:** Attempts to engage HDCP. If HDCP fails to engage, the PC will constrain the effective resolution to 520,000 pixels per frame and pass the content.	**HWDRM:** Passes content with HDCP. If HDCP fails to engage, playback to HDMI/DVI ports is blocked.	
271-300		When HDCP type restriction is NOT defined:Passes content with HDCP. If HDCP fails to engage, playback to HDMI/DVI ports is blocked. When HDCP type restriction IS defined: Passes content with HDCP 2.2 and content stream type set to 1. If HDCP fails to engage or content stream type can't be set to 1, playback to HDMI/DVI ports is blocked.		
>300		Does NOT pass content		

Microsoft PlayReady [H]

WIDEVINE

content_key_specs. required_output_protection. hdcp	string - one of: HDCP_NONE, HDCP_V1, HDCP_V2	Indicates whether HDCP is required. *Default = HDCP_NONE.* *Note: These must be capitalized, lowercase will result in a malformed request.* See Appendix.

Widevine DRM Proxy Integration

[F]

Source: *https://learn.microsoft.com/en-us/playready/overview/output-protection-levels*

Content is received by the connected TV over the HDMI connection as HDCP encrypted content in accordance with the requirements of the HDCP security messages specified by the primary OTT service provider

U.S. Patent No. 8,291,236 Against Hisense Smart TVs

Claim 140. A secondary conditional access client [A], comprising:
a processor [J] coupled to the communication interface [B], the processor [J] to process the access controlled data [E],

For the purpose of this specification, it is assumed that the Audiovisual content is transmitted over a HDMI based wired display link. In an HDCP System, two or more HDCP Devices are interconnected through an HDCP-protected Interface. The Audiovisual Content flows from the Upstream Content Control Function into the HDCP System at the most upstream HDCP Transmitter. From there the Audiovisual Content encrypted by the HDCP System, referred to as HDCP Content, flows through a tree-shaped topology of HDCP Receivers over HDCP-protected Interfaces. This specification describes a content protection mechanism for: (1) authentication of HDCP Receivers to their immediate upstream connection (i.e., an HDCP Transmitter), (2) revocation of HDCP Receivers that are determined by the Digital Content Protection, LLC, to be invalid, and (3) HDCP Encryption of Audiovisual Content over the HDCP-protected Interfaces between HDCP Transmitters and their downstream HDCP Receivers. HDCP Receivers may render the HDCP Content in audio and visual form for human consumption. HDCP Receivers may be HDCP Repeaters that serve as downstream HDCP Transmitters emitting the HDCP Content further downstream to one or more additional HDCP Receivers.

HDCP on HDMI Specification, Rev. 2.2

Hisense Smart TVs incorporate an onboard processor to process the HDCP encrypted content for display

U.S. Patent No. 8,291,236 Against Hisense Smart TVs

Claim 140. A secondary conditional access client [A], comprising:
wherein the primary security system [G] authenticates the conditional access server [C] as one of clients of the primary security system [G] through a first authentication process [K1] using a first root of trust [K2] and the conditional access server [C] authenticates clients [A] of the conditional access server [C] through a second authentication process [L1] which is independent of the first authentication process [K1] and wherein the second authentication process [L1] uses a second root of trust [L2] which is independent of and different than the first root of trust [K2],

Client Authentication

In the context of content protection, client authentication may occur at two levels, the client device and the user. PlayReady handles device authentication automatically through its use of *device keys* when issuing licenses to PlayReady clients, as illustrated in the following diagram.

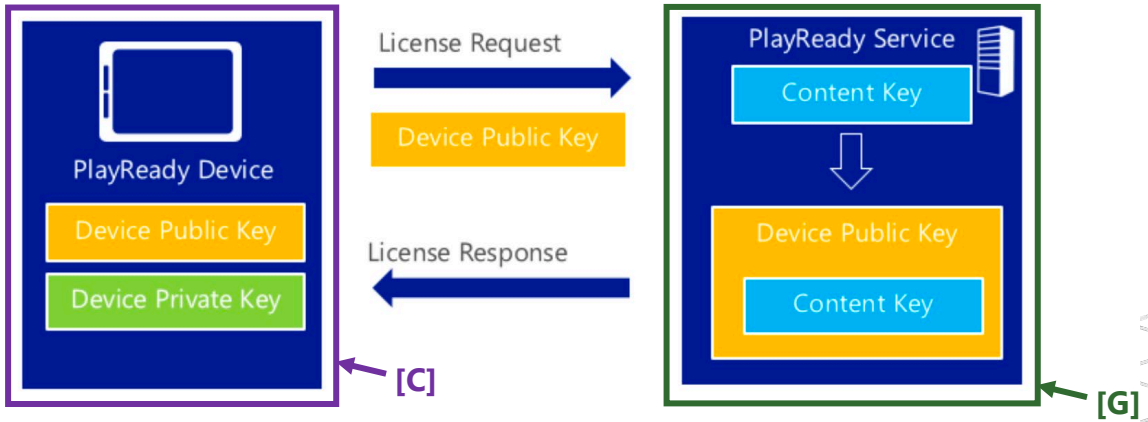


Figure 4 – Role of Device Keys in the Licensing Process

Source: *https://download.microsoft.com/download/B/D/4/BD42A75B-5B3E-49C0-B70D-DD49FA9592F9/DevelopingMicrosoftPlayReadyClients_March2015.pdf, p12*

Each PlayReady client device has a unique public-private key pair. When a client sends a license request to a license service, it includes its device public key. The license service uses that public key to verify that the client device is a valid PlayReady client before it issues the license. If the device is a valid PlayReady client, the license service uses the device's public key to encrypt the content key for the media file and then sends the resulting license to the client. The client must then use its device private key to decrypt and play back the content. This authentication model ensures that the issued license is valid and usable only on that device (in the case of the device binding).

Source: *https://download.microsoft.com/download/B/D/4/BD42A75B-5B3E-49C0-B70D-DD49FA9592F9/DevelopingMicrosoftPlayReadyClients_March2015.pdf, p12*

PlayReady Certificate Authority

Microsoft owns the PlayReady Certificate Authority (PlayReady CA) including the PlayReady top level CA certificates, which gives Microsoft the authority to deliver PlayReady certificates to its customers, and revoke them whenever it is required to keep the ecosystem functional and secure.

Source: *https://learn.microsoft.com/en-us/playready/overview/certificates*

The primary security system authenticates the conditional access server using a root of trust

U.S. Patent No. 8,291,236 Against Hisense Smart TVs

Claim 140. A secondary conditional access client [A], comprising:
wherein the primary security system [G] authenticates the conditional access server [C] as one of clients of the primary security system [G] through a first authentication process [K1] using a first root of trust [K2] and the conditional access server [C] authenticates clients [A] of the conditional access server [C] through a second authentication process [L1] which is independent of the first authentication process [K1] and wherein the second authentication process [L1] uses a second root of trust [L2] which is independent of and different than the first root of trust [K2],

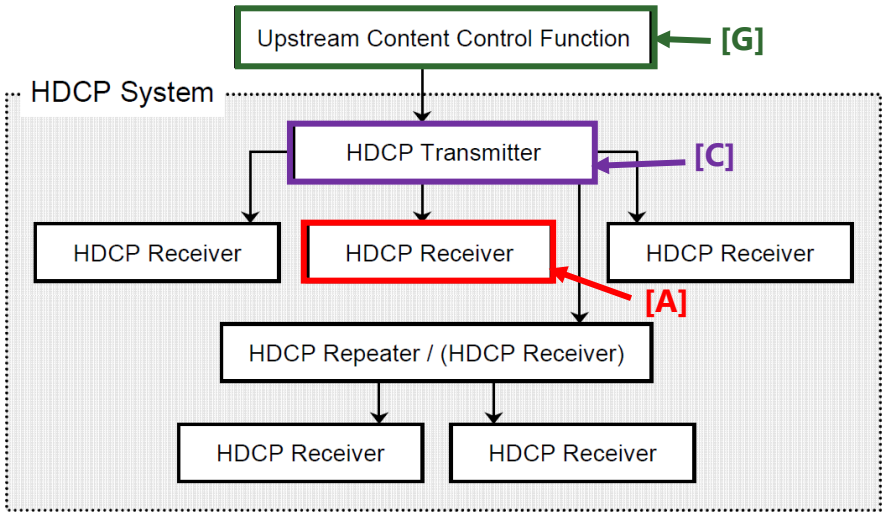


Figure 1.1. Sample Connection Topology of an HDCP System

HDCP on HDMI Specification, Rev. 2.2

[L1]

2 Authentication Protocol

2.1 Overview

The HDCP authentication protocol is an exchange between an HDCP Transmitter and an HDCP Receiver that affirms to the HDCP Transmitter that the HDCP Receiver is authorized to receive HDCP Content. It is comprised of the following stages

Root of trust

- Authentication and Key Exchange (AKE) – The HDCP Receiver's public key certificate is verified by the HDCP Transmitter. A Master Key k_m is exchanged.
- Locality Check – The HDCP Transmitter enforces locality on the content by requiring that the Round Trip Time (RTT) between a pair of messages is not more than 20 ms.
- Session Key Exchange (SKE) – The HDCP Transmitter exchanges Session Key k_s with the HDCP Receiver.
- Authentication with Repeaters – The step is performed by the HDCP Transmitter only with HDCP Repeaters. In this step, the repeater assembles downstream topology information and forwards it to the upstream HDCP Transmitter.

Successful completion of AKE and locality check stages affirms to the HDCP Transmitter that the HDCP Receiver is authorized to receive HDCP Content. At the end of the authentication protocol, a communication path is established between the HDCP Transmitter and HDCP Receiver that only Authorized Devices can access.

HDCP on HDMI Specification, Rev. 2.2

The HDCP transmitter component in the streaming media devices authenticates to the HDCP receiver component in the Hisense Smart TV using a root of trust established by an HDCP authentication protocol which is independent of and different from the first root of trust

U.S. Patent No. 8,291,236 Against Hisense Smart TVs

Claim 140. A secondary conditional access client [A], comprising:
and wherein the conditional access server [C] is configured to substitute [M] the first security domain [H] with the second security domain [I] for the clients [A] under the second root of trust [L2].

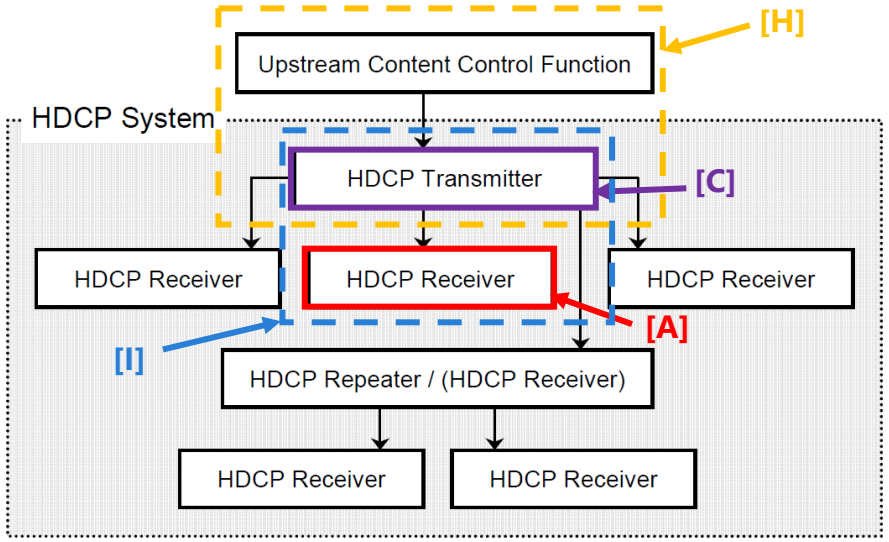
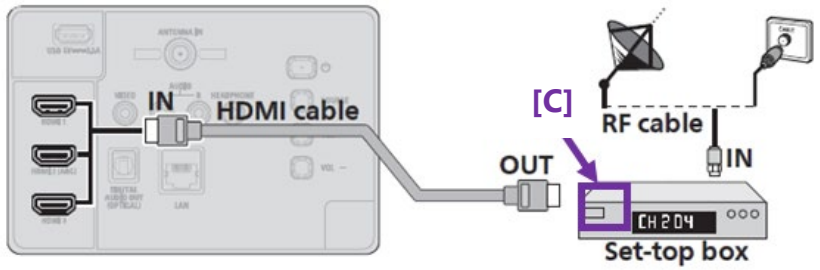
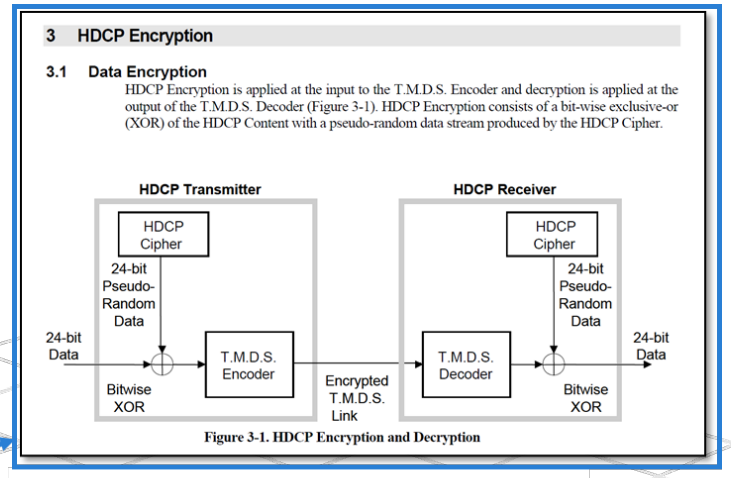


Figure 1.1. Sample Connection Topology of an HDCP System

HDCP on HDMI Specification, Rev. 2.2



Hisense TV Connection *(illustrative)*



3 HDCP Encryption

3.1 Data Encryption

HDCP Encryption is applied at the input to the T.M.D.S. Encoder and decryption is applied at the output of the T.M.D.S. Decoder (Figure 3-1). HDCP Encryption consists of a bit-wise exclusive-or (XOR) of the HDCP Content with a pseudo-random data stream produced by the HDCP Cipher.

Figure 3-1. HDCP Encryption and Decryption

HDCP on HDMI Specification, Rev. 2.2

[H]

[I]

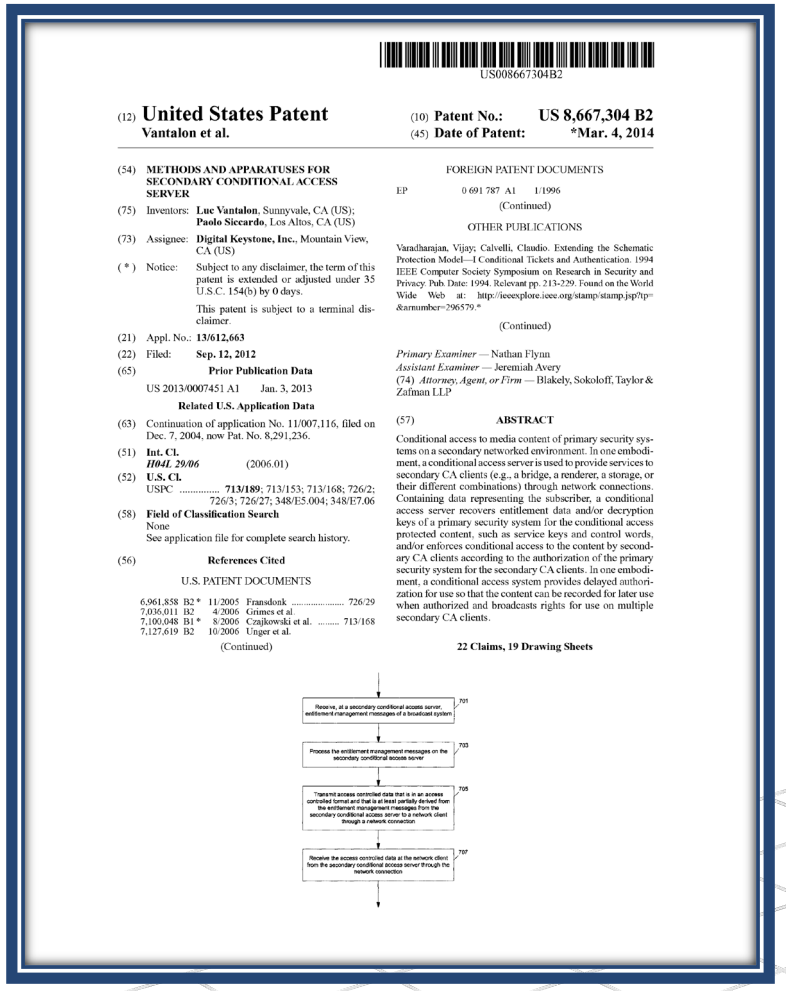
The HDCP transmitter component in the streaming media device is configured to apply HDCP encryption to the locally-decoded DRM-protected content and transmit the HDCP-encrypted content securely to the HDCP receiver component in the Hisense Smart TV in accordance with the established HDCP root of trust for subsequent display

VIDEOLABS

US Patent No. 8,667,304 Against Hisense Smart TVs With HDCP

EX. 2006

U.S. Patent No. 8,667,304



US008667304B2

(12) **United States Patent**
Vantalon et al.

(10) **Patent No.: US 8,667,304 B2**
(45) **Date of Patent: *Mar. 4, 2014**

(54) **METHODS AND APPARATUSES FOR SECONDARY CONDITIONAL ACCESS SERVER**

(75) Inventors: **Luc Vantalon**, Sunnyvale, CA (US); **Paolo Siccardo**, Los Altos, CA (US)

(73) Assignee: **Digital Keystone, Inc.**, Mountain View, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **13/612,663**

(22) Filed: **Sep. 12, 2012**

(65) **Prior Publication Data**

US 2013/0007451 A1 Jan. 3, 2013

Related U.S. Application Data

(63) Continuation of application No. 11/007,116, filed on Dec. 7, 2004, now Pat. No. 8,291,236.

(51) **Int. Cl.**
H04L 29/06 (2006.01)

(52) **U.S. Cl.**
USPC **713/189**; 713/153; 713/168; 726/2; 726/3; 726/27; 348/E5.004; 348/E7.06

(58) **Field of Classification Search**
None
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

6,961,858 B2 * 11/2005 Fransdonk 726/29
7,036,011 B2 4/2006 Grimes et al.
7,100,048 B1 * 8/2006 Czajkowski et al. 713/168
7,127,619 B2 10/2006 Unger et al.
(Continued)

FOREIGN PATENT DOCUMENTS

EP 0 691 787 A1 1/1996
(Continued)

OTHER PUBLICATIONS

Varadharajan, Vijay; Calvelli, Claudio. Extending the Schematic Protection Model—I Conditional Tickets and Authentication. 1994 IEEE Computer Society Symposium on Research in Security and Privacy. Pub. Date: 1994. Relevant pp. 213-229. Found on the World Wide Web at: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=296579.*
(Continued)

Primary Examiner — Nathan Flynn
Assistant Examiner — Jeremiah Avery
(74) *Attorney, Agent, or Firm* — Blakely, Sokoloff, Taylor & Zafman LLP

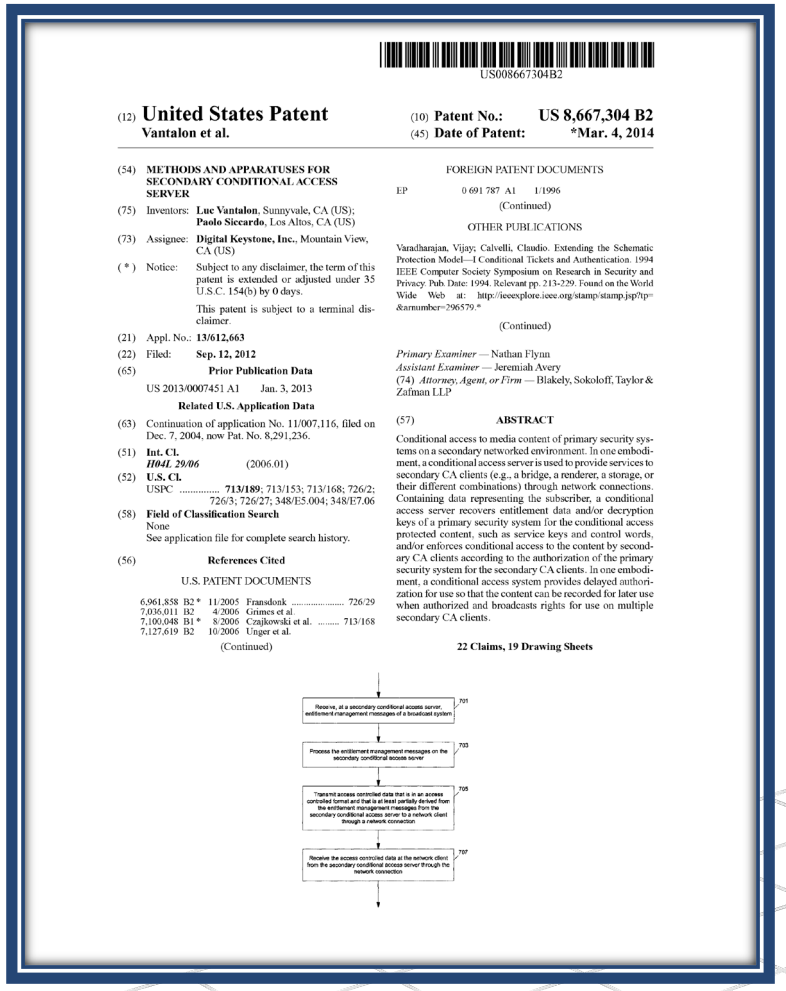
(57) **ABSTRACT**

Conditional access to media content of primary security systems on a secondary networked environment. In one embodiment, a conditional access server is used to provide services to secondary CA clients (e.g., a bridge, a renderer, a storage, or their different combinations) through network connections. Containing data representing the subscriber, a conditional access server recovers entitlement data and/or decryption keys of a primary security system for the conditional access protected content, such as service keys and control words, and/or enforces conditional access to the content by secondary CA clients according to the authorization of the primary security system for the secondary CA clients. In one embodiment, a conditional access system provides delayed authorization for use so that the content can be recorded for later use when authorized and broadcasts rights for use on multiple secondary CA clients.

22 Claims, 19 Drawing Sheets

- **Inventor**: Luc Vantalon, Paolo Siccardo
- **Priority Date**: December 7, 2004
  Expiration Date: December 7, 2024
- **Summary of Technology**: DRM bridge between two independent security domains
- **Claim Mapping**: Hisense TVs with HDCP

U.S. Patent No. 8,667,304, Claim 5



US008667304B2

(12) **United States Patent**
Vantalon et al.

(10) **Patent No.: US 8,667,304 B2**
(45) **Date of Patent: *Mar. 4, 2014**

(54) **METHODS AND APPARATUSES FOR SECONDARY CONDITIONAL ACCESS SERVER**

(75) Inventors: **Luc Vantalon**, Sunnyvale, CA (US); **Paolo Siccardo**, Los Altos, CA (US)

(73) Assignee: **Digital Keystone, Inc.**, Mountain View, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **13/612,663**

(22) Filed: **Sep. 12, 2012**

(65) **Prior Publication Data**

US 2013/0007451 A1 Jan. 3, 2013

Related U.S. Application Data

(63) Continuation of application No. 11/007,116, filed on Dec. 7, 2004, now Pat. No. 8,291,236.

(51) **Int. Cl.**
H04L 29/06 (2006.01)

(52) **U.S. Cl.**
USPC **713/189**; 713/153; 713/168; 726/2; 726/3; 726/27; 348/E5.004; 348/E7.06

(58) **Field of Classification Search**
None
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

6,961,858 B2 * 11/2005 Fransdonk 726/29
7,036,011 B2 4/2006 Grimes et al.
7,100,048 B1 * 8/2006 Czajkowski et al. 713/168
7,127,619 B2 10/2006 Unger et al.
(Continued)

FOREIGN PATENT DOCUMENTS

EP 0 691 787 A1 1/1996
(Continued)

OTHER PUBLICATIONS

Varadharajan, Vijay; Calvelli, Claudio. Extending the Schematic Protection Model—I Conditional Tickets and Authentication. 1994 IEEE Computer Society Symposium on Research in Security and Privacy. Pub. Date: 1994. Relevant pp. 213-229. Found on the World Wide Web at: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=296579.*
(Continued)

Primary Examiner — Nathan Flynn
Assistant Examiner — Jeremiah Avery
(74) *Attorney, Agent, or Firm* — Blakely, Sokoloff, Taylor & Zafman LLP

(57) **ABSTRACT**

Conditional access to media content of primary security systems on a secondary networked environment. In one embodiment, a conditional access server is used to provide services to secondary CA clients (e.g., a bridge, a renderer, a storage, or their different combinations) through network connections. Containing data representing the subscriber, a conditional access server recovers entitlement data and/or decryption keys of a primary security system for the conditional access protected content, such as service keys and control words, and/or enforces conditional access to the content by secondary CA clients according to the authorization of the primary security system for the secondary CA clients. In one embodiment, a conditional access system provides delayed authorization for use so that the content can be recorded for later use when authorized and broadcasts rights for use on multiple secondary CA clients.

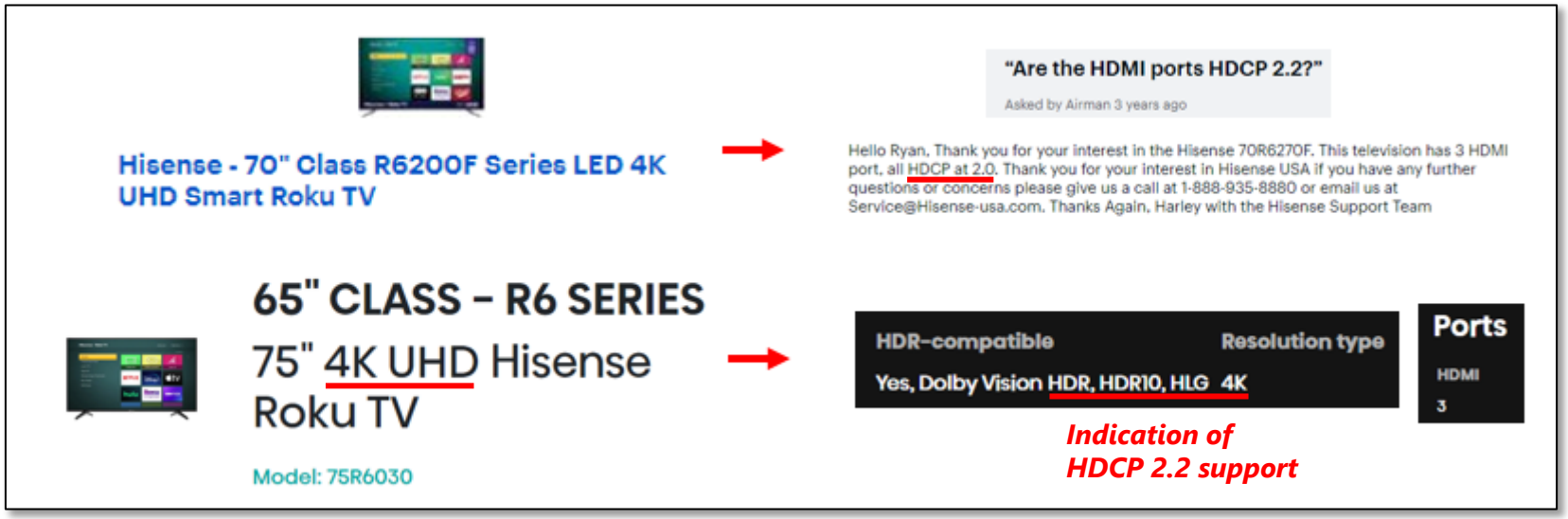
22 Claims, 19 Drawing Sheets

Claim 5. A non-transitory machine readable medium containing executable computer program instructions which when executed by a data processing system cause a client system in a second security domain to present content provided by a first conditional access server wherein the first conditional access server has authenticated a client device of the first conditional access server through a first authentication process using a first root of trust for a first security domain and wherein a second conditional access server is configured to substitute the first security domain with the second security domain for client devices under a second root of trust, the method comprising:

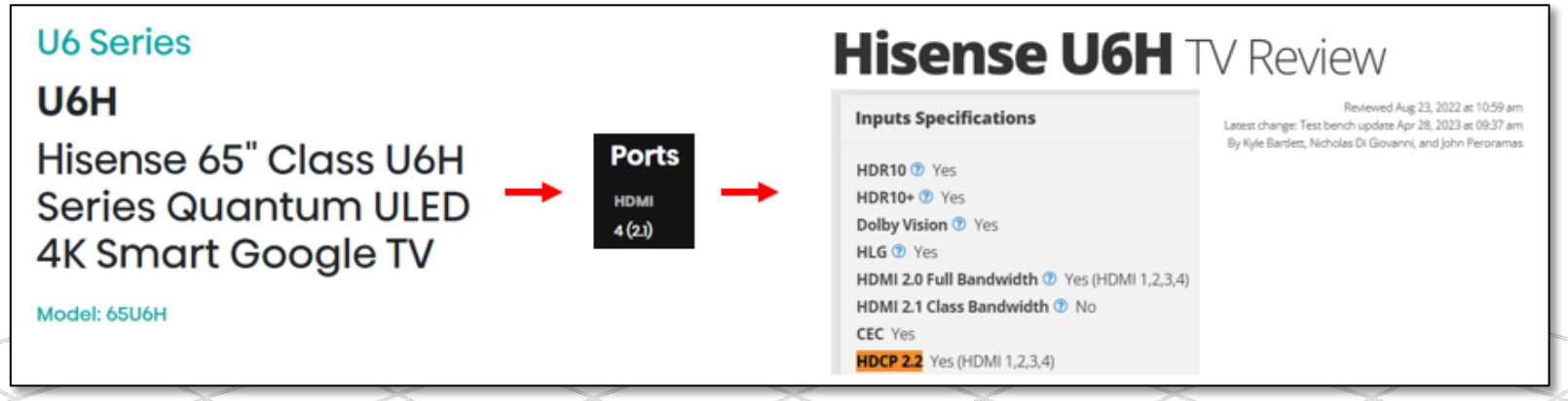
receiving, at a second conditional access client of the second conditional access server, an authentication through a second authentication process which is independent of the first authentication process and wherein the second authentication process uses the second root of trust for the second security domain which is independent of and different than the first root of trust; and

receiving, at the second conditional access client, content that is in an access controlled format specified by the second conditional access server in the second security domain, the second conditional access client being in the second security domain.

Hisense's Smart TV Platform Devices All Support HDCP



Exemplary Hisense Roku TVs support HDCP 2.x security over HDMI



Exemplary Hisense Google/Android TVs support HDCP 2.2 security over HDMI

Sources:

- https://www.bestbuy.com/site/questions/hisense-70-class-r6200f-series-led-4k-uhd-smart-roku-tv/6378023/question/27db90b1-3884-3c16-aba2-321e1249578a
- https://www.hisense-usa.com/televisions/75r6030-75-4k-uhd-hisense-roku-tv-with-hdr-2020#ProductDetailsBox7
- https://www.hisense-usa.com/televisions/65u6h-hisense-65-inch-u6h-series-quantum-uled-4k-smart-google-tv-2022#ProductDetailsBox17
- https://www.rtings.com/tv/reviews/hisense/u6h

U.S. Patent No. 8,667,304 Against Hisense Smart TVs

Claim 5. A non-transitory machine readable medium containing executable computer program instructions [A] which when executed by a data processing system cause a client system [B] in a second security domain [C] to present content provided by a first conditional access server [D] wherein the first conditional access server [D] has authenticated [E] a client device [F] of the first conditional access server [D] through a first authentication process using a first root of trust [G] for a first security domain [H] and wherein a second conditional access server [I] is configured to substitute [J] the first security domain [H] with the second security domain [C] for client devices [B] under a second root of trust [K], the method comprising:

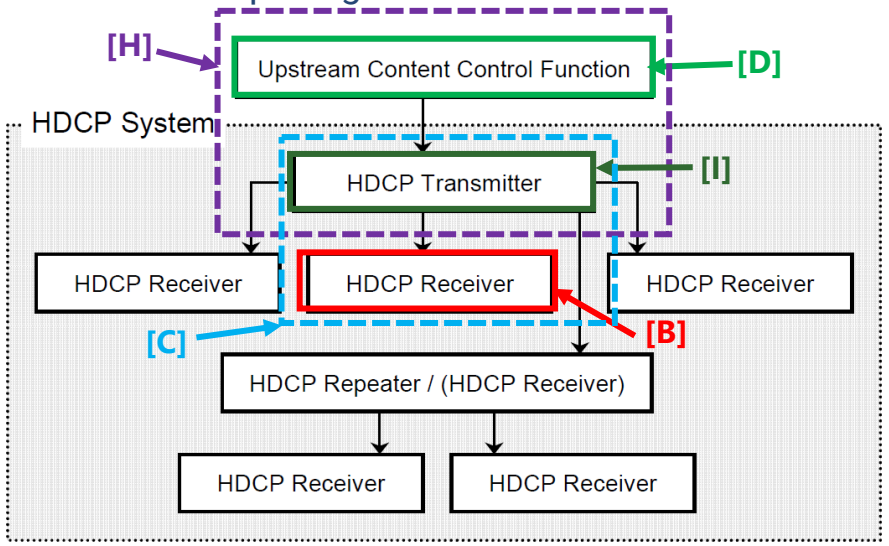


Figure 1.1. Sample Connection Topology of an HDCP System

HDCP on HDMI Specification, Rev. 2.2

For the purpose of this specification, it is assumed that the Audiovisual content is transmitted over a HDMI based wired display link. In an HDCP System, two or more HDCP Devices are interconnected through an HDCP-protected Interface. The Audiovisual Content flows from the Upstream Content Control Function into the HDCP System at the most upstream HDCP Transmitter. From there the Audiovisual Content encrypted by the HDCP System, referred to as HDCP Content, flows through a tree-shaped topology of HDCP Receivers over HDCP-protected Interfaces. This specification describes a content protection mechanism for: (1) authentication of HDCP Receivers to their immediate upstream connection (i.e., an HDCP Transmitter), (2) revocation of HDCP Receivers that are determined by the Digital Content Protection, LLC, to be invalid, and (3) HDCP Encryption of Audiovisual Content over the HDCP-protected Interfaces between HDCP Transmitters and their downstream HDCP Receivers. HDCP Receivers may render the HDCP Content in audio and visual form for human consumption. HDCP Receivers may be HDCP Repeaters that serve as downstream HDCP Transmitters emitting the HDCP Content further downstream to one or more additional HDCP Receivers.

HDCP on HDMI Specification, Rev. 2.2

Hisense Smart TVs are HDCP-compliant devices and incorporate respective Roku or Google TV platform applications and an HDCP transmitter component to communicate DRM-protected streaming content originating from a primary OTT service provider with other HDCP-complaint devices securely over an HDMI interface

U.S. Patent No. 8,667,304 Against Hisense Smart TVs

Claim 5. A non-transitory machine readable medium containing executable computer program instructions [A] which when executed by a data processing system cause a client system [B] in a second security domain [C] to present content provided by a first conditional access server [D] wherein the first conditional access server [D] has authenticated [E] a client device [F] of the first conditional access server [D] through a first authentication process using a first root of trust [G] for a first security domain [H] and wherein a second conditional access server [I] is configured to substitute [J] the first security domain [H] with the second security domain [C] for client devices [B] under a second root of trust [K], the method comprising:

Client Authentication

In the context of content protection, client authentication may occur at two levels, the client device and the user. PlayReady handles device authentication automatically through its use of *device keys* when issuing licenses to PlayReady clients, as illustrated in the following diagram.

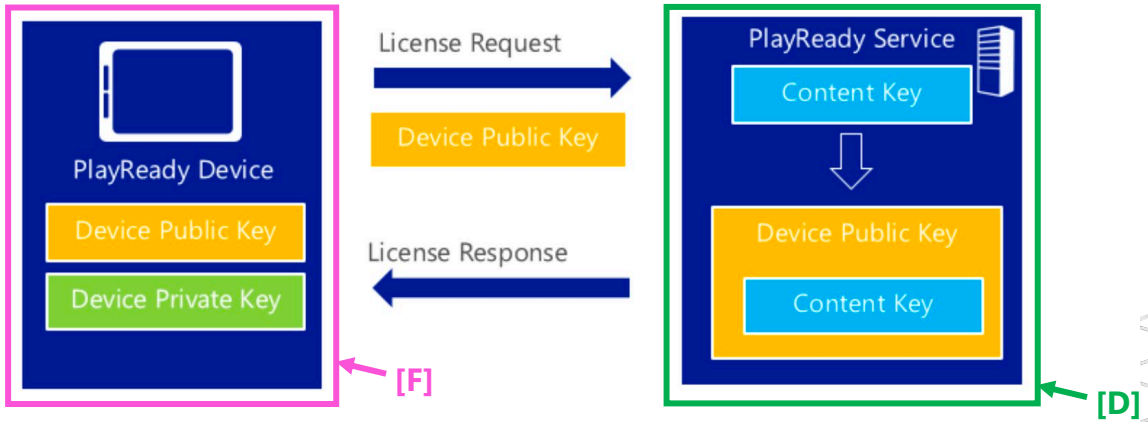


Figure 4 – Role of Device Keys in the Licensing Process

Source: *https://download.microsoft.com/download/B/D/4/BD42A75B-5B3E-49C0-B70D-DD49FA9592F9/DevelopingMicrosoftPlayReadyClients_March2015.pdf, p12*

Each PlayReady client device has a unique public-private key pair. When a client sends a license request to a license service, it includes its device public key. The license service uses that public key to verify that the client device is a valid PlayReady client before it issues the license. If the device is a valid PlayReady client, the license service uses the device's public key to encrypt the content key for the media file and then sends the resulting license to the client. The client must then use its device private key to decrypt and play back the content. This authentication model ensures that the issued license is valid and usable only on that device (in the case of the device binding).

Source: *https://download.microsoft.com/download/B/D/4/BD42A75B-5B3E-49C0-B70D-DD49FA9592F9/DevelopingMicrosoftPlayReadyClients_March2015.pdf, p12*

PlayReady Certificate Authority

Microsoft owns the PlayReady Certificate Authority (PlayReady CA) including the PlayReady top level CA certificates, which gives Microsoft the authority to deliver PlayReady certificates to its customers, and revoke them whenever it is required to keep the ecosystem functional and secure.

Source: *https://learn.microsoft.com/en-us/playready/overview/certificates*

U.S. Patent No. 8,667,304 Against Hisense Smart TVs

Claim 5. A non-transitory machine readable medium containing executable computer program instructions [A] which when executed by a data processing system cause a client system [B] in a second security domain [C] to present content provided by a first conditional access server [D] wherein the first conditional access server [D] has authenticated [E] a client device [F] of the first conditional access server [D] through a first authentication process using a first root of trust [G] for a first security domain [H] and wherein a second conditional access server [I] is configured to substitute [J] the first security domain [H] with the second security domain [C] for client devices [B] under a second root of trust [K], the method comprising:

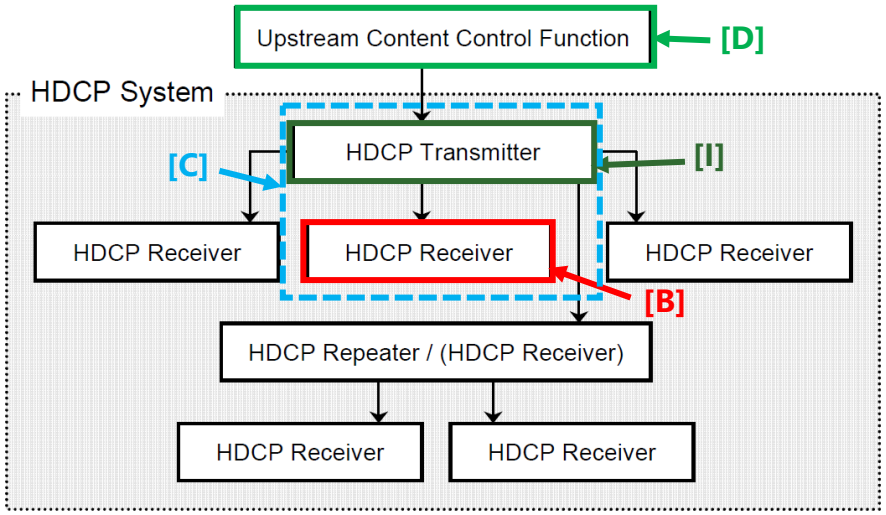


Figure 1.1. Sample Connection Topology of an HDCP System

HDCP on HDMI Specification, Rev. 2.2

2 Authentication Protocol

2.1 Overview

The HDCP authentication protocol is an exchange between an HDCP Transmitter and an HDCP Receiver that affirms to the HDCP Transmitter that the HDCP Receiver is authorized to receive HDCP Content. It is comprised of the following stages

Root of trust

- Authentication and Key Exchange (AKE) – The HDCP Receiver's public key certificate is verified by the HDCP Transmitter. A Master Key k_m is exchanged.
- Locality Check – The HDCP Transmitter enforces locality on the content by requiring that the Round Trip Time (RTT) between a pair of messages is not more than 20 ms.
- Session Key Exchange (SKE) – The HDCP Transmitter exchanges Session Key k_s with the HDCP Receiver.
- Authentication with Repeaters – The step is performed by the HDCP Transmitter only with HDCP Repeaters. In this step, the repeater assembles downstream topology information and forwards it to the upstream HDCP Transmitter.

Successful completion of AKE and locality check stages affirms to the HDCP Transmitter that the HDCP Receiver is authorized to receive HDCP Content. At the end of the authentication protocol, a communication path is established between the HDCP Transmitter and HDCP Receiver that only Authorized Devices can access.

HDCP on HDMI Specification, Rev. 2.2

The HDCP transmitter component in the streaming media device is configured to apply HDCP encryption to the locally-decoded DRM-protected content and transmit the HDCP-encrypted content securely to the HDCP receiver component in the connected Hisense Smart TVs in accordance with the established HDCP root of trust for subsequent display

U.S. Patent No. 8,667,304 Against Hisense Smart TVs

Claim 5. A non-transitory machine readable medium containing executable computer program instructions [A] which when executed by a data processing system cause a client system [B] in a second security domain [C] to present content provided by a first conditional access server [D] wherein the first conditional access server [D] has authenticated [E] a client device [F] of the first conditional access server [D] through a first authentication process using a first root of trust [G] for a first security domain [H] and wherein a second conditional access server [I] is configured to substitute [J] the first security domain [H] with the second security domain [C] for client devices [B] under a second root of trust [K], the method comprising:

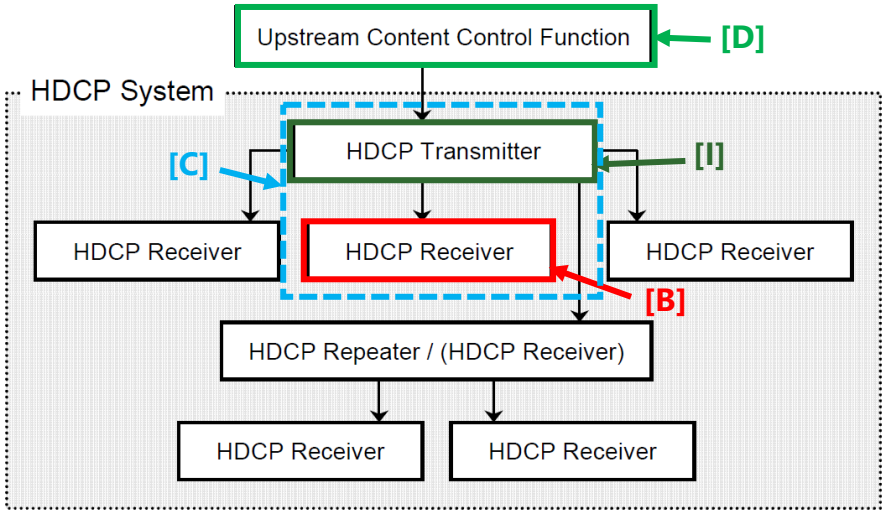
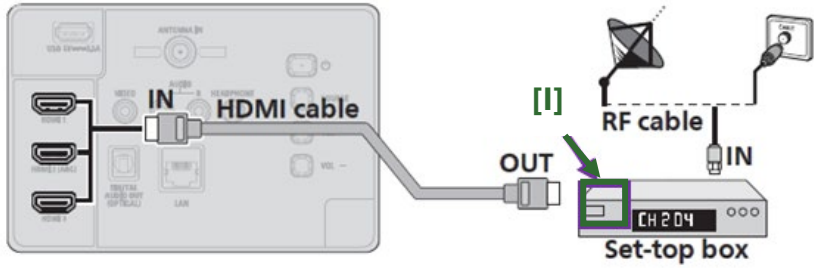
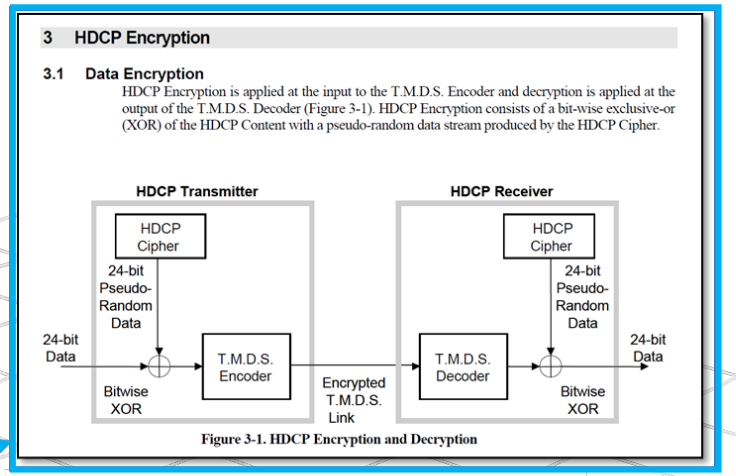


Figure 1.1. Sample Connection Topology of an HDCP System

HDCP on HDMI Specification, Rev. 2.2



Hisense TV Connection *(illustrative)*



[C]

HDCP on HDMI Specification, Rev. 2.2

[G]

The HDCP transmitter component in the streaming media device is configured to apply HDCP encryption to the locally-decoded DRM-protected content and transmit the HDCP-encrypted content securely to the HDCP receiver component in the connected Hisense Smart TV in accordance with the established HDCP root of trust for subsequent display

U.S. Patent No. 8,667,304 Against Hisense Smart TVs

Claim 5. A non-transitory machine readable medium containing executable computer program instructions [A]..., the method comprising:
receiving, at a second conditional access client [B] of the second conditional access server [I], an authentication through a second authentication process [L] which is independent of the first authentication process [E] and wherein the second authentication process [L] uses the second root of trust [K] for the second security domain [C] which is independent of and different than the first root of trust [G]; and

Exemplary Roku TV ***Exemplary Google TV***

[B]

The HDCP receiver component in the Hisense connected TV authenticates to the HDCP transmitter component in the streaming media device using a root of trust established by an HDCP authentication protocol which is independent of and different from the first root of trust

Client Authentication

In the context of content protection, client authentication may occur at two levels, the client device and the user. PlayReady handles device authentication automatically through its use of *device keys* when issuing licenses to PlayReady clients, as illustrated in the following diagram.

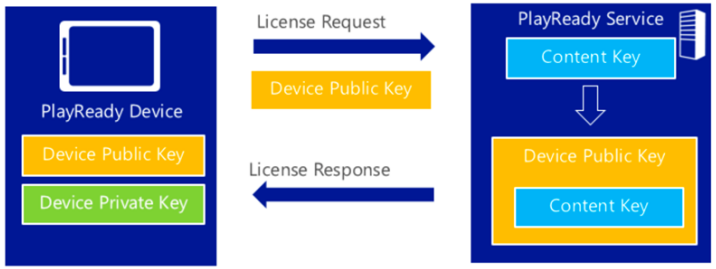


Figure 4 – Role of Device Keys in the Licensing Process

Source: *https://download.microsoft.com/download/B/D/4/BD42A75B-5B3E-49C0-B70D-DD49FA9592F9/DevelopingMicrosoftPlayReadyClients_March2015.pdf, p12*

Each PlayReady client device has a unique public-private key pair. When a client sends a license request to a license service, it includes its device public key. The license service uses that public key to verify that the client device is a valid PlayReady client before it issues the license. If the device is a valid PlayReady client, the license service uses the device's public key to encrypt the content key for the media file and then sends the resulting license to the client. The client must then use its device private key to decrypt and play back the content. This authentication model ensures that the issued license is valid and usable only on that device (in the case of the device binding).

Source: *https://download.microsoft.com/download/B/D/4/BD42A75B-5B3E-49C0-B70D-DD49FA9592F9/DevelopingMicrosoftPlayReadyClients_March2015.pdf, p12*

PlayReady Certificate Authority

Microsoft owns the PlayReady Certificate Authority (PlayReady CA) including the PlayReady top level CA certificates, which gives Microsoft the authority to deliver PlayReady certificates to its customers, and revoke them whenever it is required to keep the ecosystem functional and secure.

Source: *https://learn.microsoft.com/en-us/playready/overview/certificates*

2 Authentication Protocol

2.1 Overview

The HDCP authentication protocol is an exchange between an HDCP Transmitter and an HDCP Receiver that affirms to the HDCP Transmitter that the HDCP Receiver is authorized to receive HDCP Content. It is comprised of the following stages

Root of trust

- Authentication and Key Exchange (AKE) – The HDCP Receiver's public key certificate is verified by the HDCP Transmitter. A Master Key k_m is exchanged.
- Locality Check – The HDCP Transmitter enforces locality on the content by requiring that the Round Trip Time (RTT) between a pair of messages is not more than 20 ms.
- Session Key Exchange (SKE) – The HDCP Transmitter exchanges Session Key k_s with the HDCP Receiver.
- Authentication with Repeaters – The step is performed by the HDCP Transmitter only with HDCP Repeaters. In this step, the repeater assembles downstream topology information and forwards it to the upstream HDCP Transmitter.

Successful completion of AKE and locality check stages affirms to the HDCP Transmitter that the HDCP Receiver is authorized to receive HDCP Content. At the end of the authentication protocol, a communication path is established between the HDCP Transmitter and HDCP Receiver that only Authorized Devices can access.

HDCP on HDMI Specification, Rev. 2.2

U.S. Patent No. 8,667,304 Against Hisense Smart TVs

Claim 5. A non-transitory machine readable medium containing executable computer program instructions [A]..., the method comprising: receiving, at the second conditional access client [B], content that is in an access controlled format [M] specified by the second conditional access server [I] in the second security domain [C], the second conditional access client [B] being in the second security domain [C].

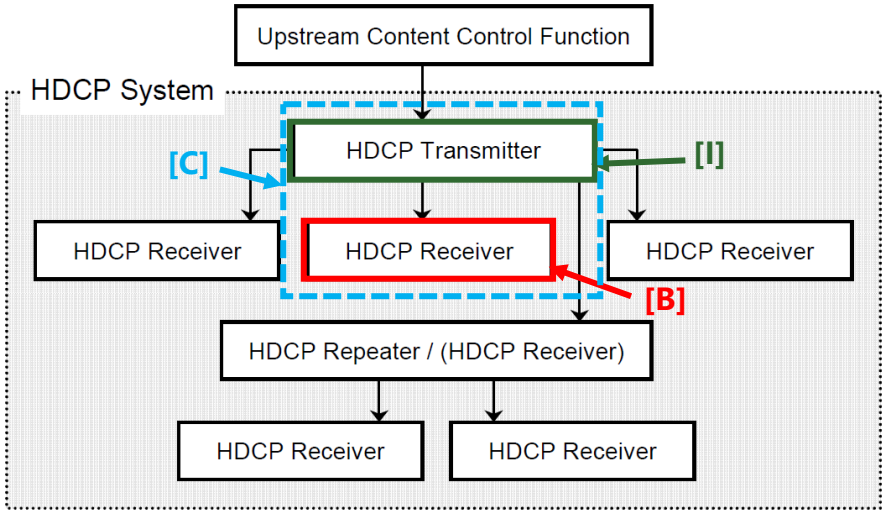


Figure 1.1. Sample Connection Topology of an HDCP System

HDCP on HDMI Specification, Rev. 2.2

For the purpose of this specification, it is assumed that the Audiovisual content is transmitted over a HDMI based wired display link. In an HDCP System, two or more HDCP Devices are interconnected through an HDCP-protected Interface. The Audiovisual Content flows from the Upstream Content Control Function into the HDCP System at the most upstream HDCP Transmitter. From there the Audiovisual Content encrypted by the HDCP System, referred to as HDCP Content, flows through a tree-shaped topology of HDCP Receivers over HDCP-protected Interfaces. This specification describes a content protection mechanism for: (1) authentication of HDCP Receivers to their immediate upstream connection (i.e., an HDCP Transmitter), (2) revocation of HDCP Receivers that are determined by the Digital Content Protection, LLC, to be invalid, and (3) HDCP Encryption of Audiovisual Content over the HDCP-protected Interfaces between HDCP Transmitters and their downstream HDCP Receivers. HDCP Receivers may render the HDCP Content in audio and visual form for human consumption. HDCP Receivers may be HDCP Repeaters that serve as downstream HDCP Transmitters emitting the HDCP Content further downstream to one or more additional HDCP Receivers.

HDCP on HDMI Specification, Rev. 2.2

The HDCP receiver component in the connected Hisense TV receives HDCP encrypted content securely over the HDMI interface

U.S. Patent No. 8,667,304 Against Roku Platform Devices

Claim 5. A non-transitory machine readable medium containing executable computer program instructions [A]..., the method comprising: receiving, at the second conditional access client [B], content that is in an access controlled format [M] specified by the second conditional access server [I] in the second security domain [C], the second conditional access client [B] being in the second security domain [C].

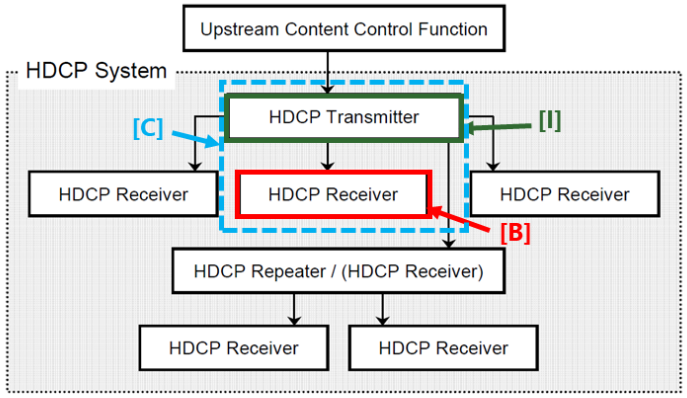
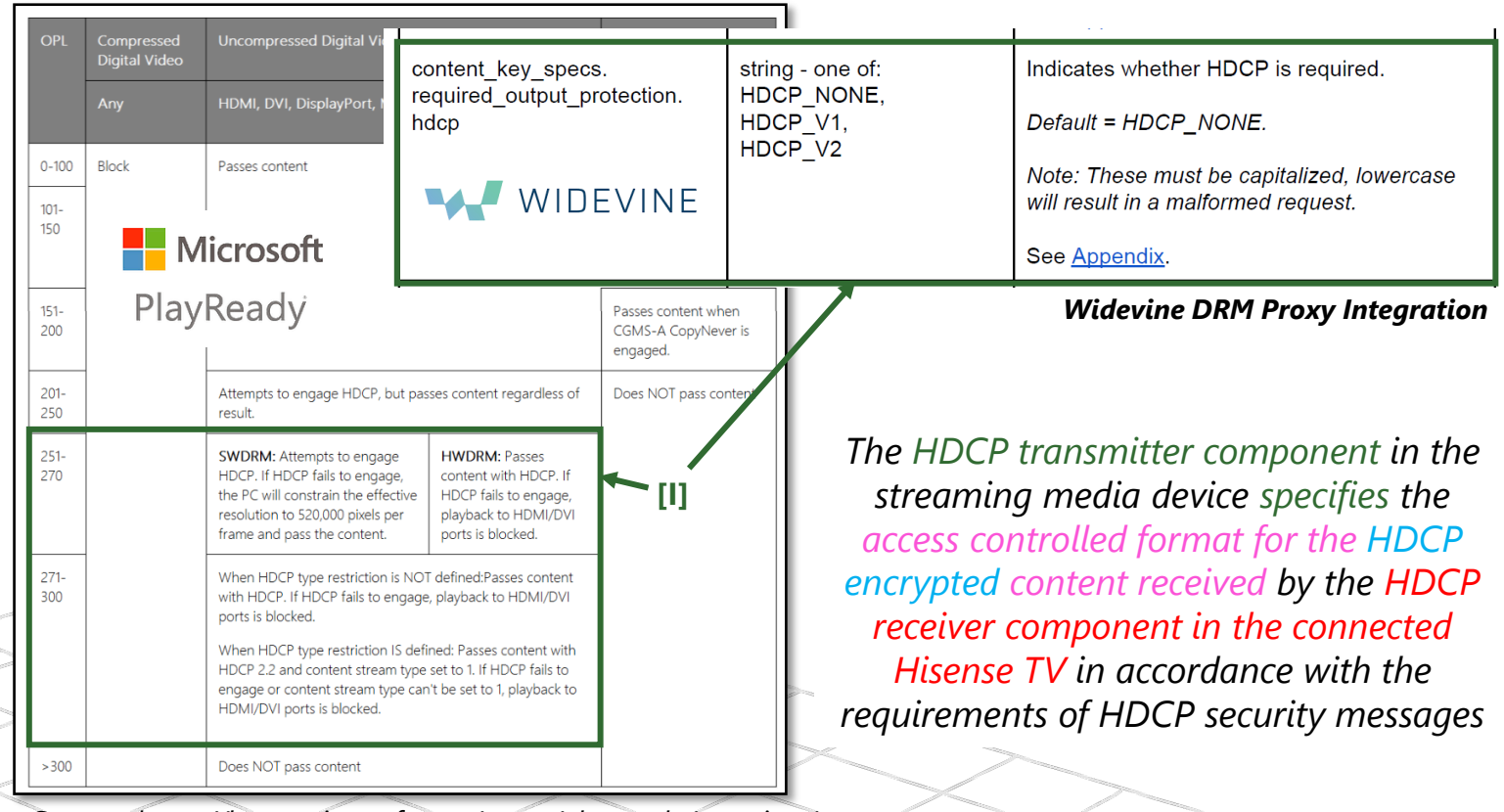


Figure 1.1. Sample Connection Topology of an HDCP System

HDCP on HDMI Specification, Rev. 2.2

For the purpose of this specification, it is assumed that the Audiovisual content is transmitted over a HDMI based wired display link. In an HDCP System, two or more HDCP Devices are interconnected through an HDCP-protected Interface. The Audiovisual Content flows from the Upstream Content Control Function into the HDCP System at the most upstream HDCP Transmitter. From there the Audiovisual Content encrypted by the HDCP System, referred to as HDCP Content, flows through a tree-shaped topology of HDCP Receivers over HDCP-protected Interfaces. This specification describes a content protection mechanism for: (1) authentication of HDCP Receivers to their immediate upstream connection (i.e., an HDCP Transmitter), (2) revocation of HDCP Receivers that are determined by the Digital Content Protection, LLC, to be invalid, and (3) HDCP Encryption of Audiovisual Content over the HDCP-protected Interfaces between HDCP Transmitters and their downstream HDCP Receivers. HDCP Receivers may render the HDCP Content in audio and visual form for human consumption. HDCP Receivers may be HDCP Repeaters that serve as downstream HDCP Transmitters emitting the HDCP Content further downstream to one or more additional HDCP Receivers.

HDCP on HDMI Specification, Rev. 2.2



Widevine DRM Proxy Integration

Source: *https://learn.microsoft.com/en-us/playready/overview/output-protection-levels*

The HDCP transmitter component in the streaming media device specifies the access controlled format for the HDCP encrypted content received by the HDCP receiver component in the connected Hisense TV in accordance with the requirements of HDCP security messages