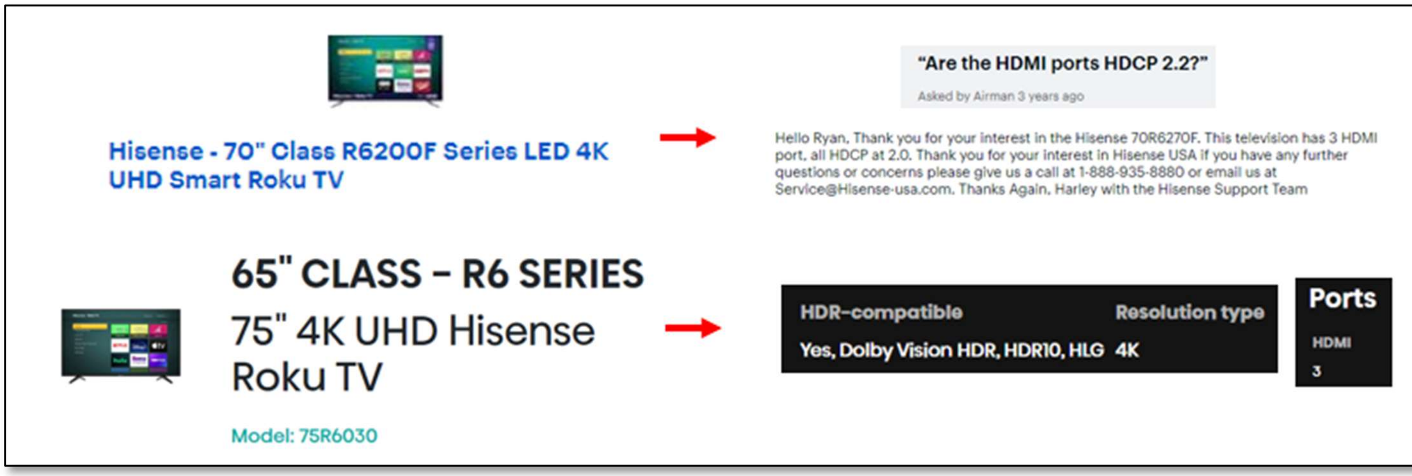
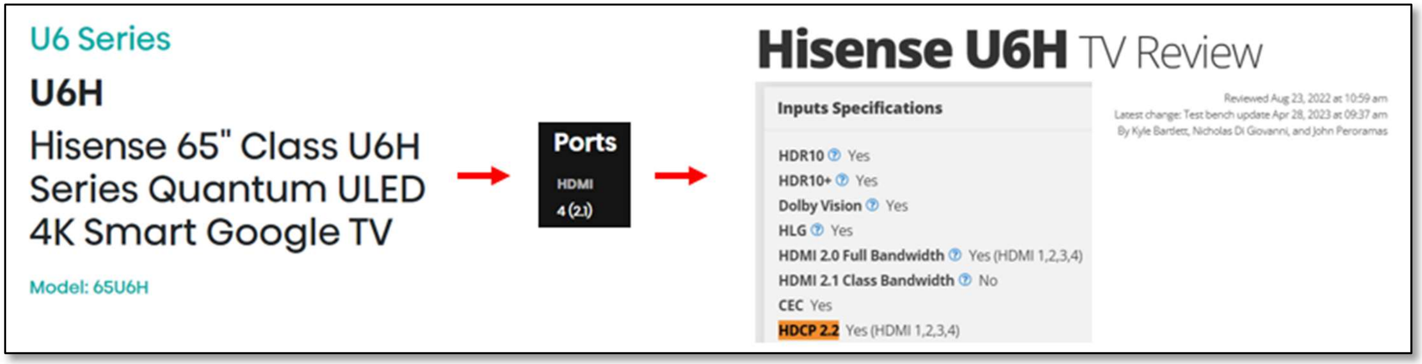
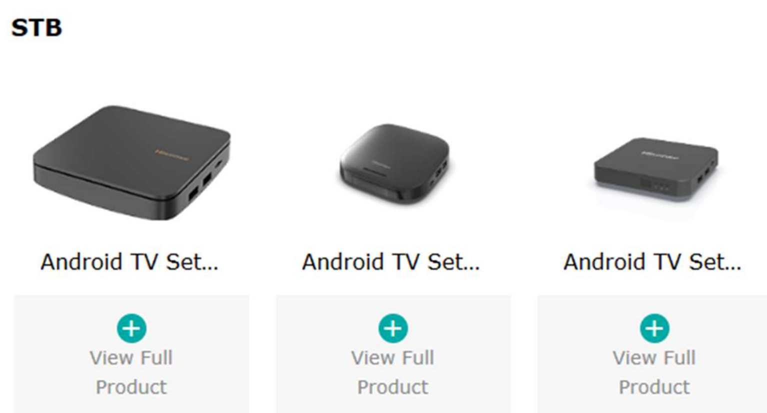
EXHIBIT F

Exhibit F – U.S. Patent No. 8,291,236 ("'236 Patent")

Claim 130	**Accused Instrumentalities**
130[pre] A conditional access server, comprising:	The Hisense Accused Instrumentalities include Hisense devices compatible with HDCP, including Hisense devices configured to stream 4K and/or HDR content, such as, e.g., Hisense streaming players, including Hisense Smart TVs (e.g., Hisense 75R6030 Roku TV), Hisense Set-top boxes (e.g., Hisense Android TV Set-top Box IP960N), and Hisense TV Dongles (e.g., Hisense Android TV Dongle IP151D). 

Claim 130	Accused Instrumentalities
	 *See, e.g.*, 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.  *See, e.g.*, https://www.hisensebroadband.com/html/products/broadcast%20stb/

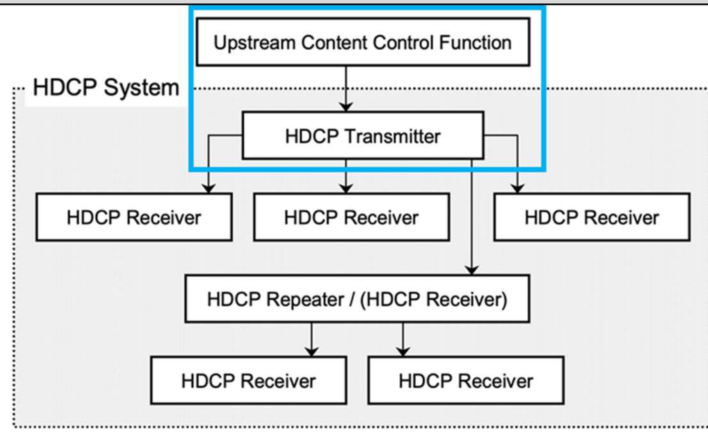
Claim 130	**Accused Instrumentalities**
	Features • Highest efficiency ARMv8 64-bit CPU, Quad core ARM Cortex-A55 CPU • High Performance GPU, ARM G31 MP2 GPU • Support AI video upscaling • Supports AV1 Video Decoding MP-10@L5.1 up to 4Kx2K@60fps • Supports VP9 Profile-2 Video Decoding up to 4Kx2K@60fps • Supports H.265 HEVC Video Decoding MP-10@L5.1 up to 4Kx2K@60fps • Supports H.264 AVC HP@L5.1 up to 4Kx2K@30fps • Supports HDMI 2.1 with HDCP2.2/HDCP2.3 • Supports Dolby Vision, HDR10, HDR10+, HLG HDR processing • Supports Wi-Fi 5 (802.11b/g/n/ac) 2x2 MU-MIMO and Bluetooth 5.0 • Base on Android TV platform • Supports Widevine L1 and Playready 3.0 • Supports TR069 network management • Supports Google Play Store, Youtube, Google Cast, Google Assistant • Support Netflix • Support customized Lanucher • Designed based on open technology, supports third-party applications effectively *See, e.g.*, https://www.hisensebroadband.com/html/products/broadcast%20stb/20240809_466.html

Claim 130	Accused Instrumentalities
	Dongle  Android TV Do... View Full Product *See, e.g.*, https://www.hisensebroadband.com/html/products/broadcast%20stb/

Claim 130	Accused Instrumentalities
	Features • High efficiency ARMv8 64-bit CPU, Quad core ARM Cortex-A35 CPU • High Performance GPU, ARM G31 MP2 GPU • Supports AV1 Video Decoding MP-10@L5.1 up to 4Kx2K@60fps • Supports VP9 Profile-2 Video Decoding up to 4Kx2K@60fps • Supports H.265 HEVC Video Decoding MP-10@L5.1 up to 4Kx2K@60fps • Supports H.264 AVC HP@L5.1 up to 4Kx2K@30fps • Supports HDMI 2.1 with HDCP2.2/HDCP2.3 • Supports Dolby Vision, HDR10, HDR10+, HLG HDR processing • Supports Wi-Fi 5 (802.11b/g/n/ac) 2x2 MU-MIMO and Bluetooth 5.0 • Base on Android TV platform • Supports Widevine L1 and Playready 3.0 • Supports TR069 network management • Supports Google Play Store, Youtube, Google Cast, Google Assistant • Support customized Lanucher • Designed based on open technology, supports third-party applications effectively • Support power from TV USB *See, e.g.*, https://www.hisensebroadband.com/html/products/dongle/20240809_467.html To the extent the preamble is limiting, each Accused Instrumentality is a conditional access server. For example, the Accused Instrumentalities are HDCP-compliant devices that incorporate respective applications resident in the memory thereon (e.g., streaming applications). The Accused Instrumentalities further include HDCP

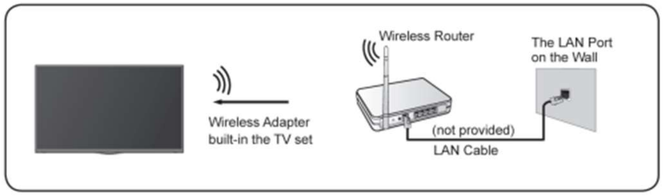
Claim 130	Accused Instrumentalities
	transmitter hardware, I/O circuitry and respective firmware to communicate using HDCP-based encryption and/or otherwise support HDCP functionality to serve HDCP-related content, as shown above. The Accused Instrumentalities integrate a content DRM system such as PlayReady and/or Widevine with its HDCP transmitter (e.g., as shown in the blue box of the second image, below). Features • High efficiency ARMv8 64-bit CPU, Quad core ARM Cortex-A35 CPU • High Performance GPU, ARM G31 MP2 GPU • Supports AV1 Video Decoding MP-10@L5.1 up to 4Kx2K@60fps • Supports VP9 Profile-2 Video Decoding up to 4Kx2K@60fps • Supports H.265 HEVC Video Decoding MP-10@L5.1 up to 4Kx2K@60fps • Supports H.264 AVC HP@L5.1 up to 4Kx2K@30fps • Supports HDMI 2.1 with HDCP2.2/HDCP2.3 • Supports Dolby Vision, HDR10, HDR10+, HLG HDR processing • Supports Wi-Fi 5 (802.11b/g/n/ac) 2x2 MU-MIMO and Bluetooth 5.0 • Base on Android TV platform • Supports Widevine L1 and Playready 3.0 • Supports TR069 network management • Supports Google Play Store, Youtube, Google Cast, Google Assistant • Support customized Lanucher • Designed based on open technology, supports third-party applications effectively • Support power from TV USB

Claim 130	Accused Instrumentalities
	See, e.g., https://www.hisensebroadband.com/html/products/dongle/20240809_467.html Features • Highest efficiency ARMv8 64-bit CPU, Quad core ARM Cortex-A55 CPU • High Performance GPU, ARM G31 MP2 GPU • Support AI video upscaling • Supports AV1 Video Decoding MP-10@L5.1 up to 4Kx2K@60fps • Supports VP9 Profile-2 Video Decoding up to 4Kx2K@60fps • Supports H.265 HEVC Video Decoding MP-10@L5.1 up to 4Kx2K@60fps • Supports H.264 AVC HP@L5.1 up to 4Kx2K@30fps • Supports HDMI 2.1 with HDCP2.2/HDCP2.3 • Supports Dolby Vision, HDR10, HDR10+, HLG HDR processing • Supports Wi-Fi 5 (802.11b/g/n/ac) 2x2 MU-MIMO and Bluetooth 5.0 • Base on Android TV platform • Supports Widevine L1 and Playready 3.0 • Supports TR069 network management • Supports Google Play Store, Youtube, Google Cast, Google Assistant • Support Netflix • Support customized Lanucher • Designed based on open technology, supports third-party applications effectively *See, e.g.*, https://www.hisensebroadband.com/html/products/broadcast%20stb/20240809_466.html

Claim 130	Accused Instrumentalities
	 **Figure 1.1. Sample Connection Topology of an HDCP System** *See, e.g.*, HDCP on HDMI Specification, Rev. 2.2
130[a] one or more communication interfaces, the one or more communication interfaces to receive security messages of a primary security system in a first security domain;	The Accused Instrumentalities include one or more communication interfaces, the one or more communication interfaces to receive security messages of a primary security system in a first security domain. For example, the Accused Instrumentalities receive streaming content, including security messages, via their respective wired or wireless Internet communication interfaces.

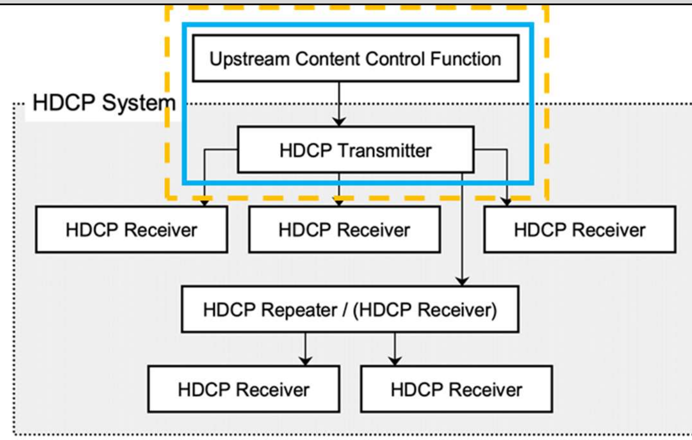
Claim 130	**Accused Instrumentalities**
	Features • High efficiency ARMv8 64-bit CPU, Quad core ARM Cortex-A35 CPU • High Performance GPU, ARM G31 MP2 GPU • Supports AV1 Video Decoding MP-10@L5.1 up to 4Kx2K@60fps • Supports VP9 Profile-2 Video Decoding up to 4Kx2K@60fps • Supports H.265 HEVC Video Decoding MP-10@L5.1 up to 4Kx2K@60fps • Supports H.264 AVC HP@L5.1 up to 4Kx2K@30fps • Supports HDMI 2.1 with HDCP2.2/HDCP2.3 • Supports Dolby Vision, HDR10, HDR10+, HLG HDR processing • Supports Wi-Fi 5 (802.11b/g/n/ac) 2x2 MU-MIMO and Bluetooth 5.0 • Base on Android TV platform • Supports Widevine L1 and Playready 3.0 • Supports TR069 network management • Supports Google Play Store, Youtube, Google Cast, Google Assistant • Support customized Lanucher • Designed based on open technology, supports third-party applications effectively • Support power from TV USB *See, e.g.*, https://www.hisensebroadband.com/html/products/dongle/20240809_467.html

Claim 130	Accused Instrumentalities
	Features • Highest efficiency ARMv8 64-bit CPU, Quad core ARM Cortex-A55 CPU • High Performance GPU, ARM G31 MP2 GPU • Support AI video upscaling • Supports AV1 Video Decoding MP-10@L5.1 up to 4Kx2K@60fps • Supports VP9 Profile-2 Video Decoding up to 4Kx2K@60fps • Supports H.265 HEVC Video Decoding MP-10@L5.1 up to 4Kx2K@60fps • Supports H.264 AVC HP@L5.1 up to 4Kx2K@30fps • Supports HDMI 2.1 with HDCP2.2/HDCP2.3 • Supports Dolby Vision, HDR10, HDR10+, HLG HDR processing • Supports Wi-Fi 5 (802.11b/g/n/ac) 2x2 MU-MIMO and Bluetooth 5.0 • Base on Android TV platform • Supports Widevine L1 and Playready 3.0 • Supports TR069 network management • Supports Google Play Store, Youtube, Google Cast, Google Assistant • Support Netflix • Support customized Lanucher • Designed based on open technology, supports third-party applications effectively *See, e.g.*, https://www.hisensebroadband.com/html/products/broadcast%20stb/20240809_466.html **Connecting to the Internet** To get access to the Internet using a wired connection or connecting to an available wireless network. **Connect to a Wired (Ethernet) Network**

Claim 130	Accused Instrumentalities
	Connect to a Wireless Network To connect to an available wireless network, make sure that you turn on your wireless router and have the wireless router's SSID and password before attempting to connect.  *See, e.g.*, https://assets.hisense-usa.com/assets/ProductDownloads/443/79afa2684c/65U6H-User-manual.pdf The Accused Instrumentalities receive security messages of a primary security system in a first security domain (e.g., security messages associated with a PlayReady and/or Widevine license and content distribution system).

Claim 130	**Accused Instrumentalities**
	Features • High efficiency ARMv8 64-bit CPU, Quad core ARM Cortex-A35 CPU • High Performance GPU, ARM G31 MP2 GPU • Supports AV1 Video Decoding MP-10@L5.1 up to 4Kx2K@60fps • Supports VP9 Profile-2 Video Decoding up to 4Kx2K@60fps • Supports H.265 HEVC Video Decoding MP-10@L5.1 up to 4Kx2K@60fps • Supports H.264 AVC HP@L5.1 up to 4Kx2K@30fps • Supports HDMI 2.1 with HDCP2.2/HDCP2.3 • Supports Dolby Vision, HDR10, HDR10+, HLG HDR processing • Supports Wi-Fi 5 (802.11b/g/n/ac) 2x2 MU-MIMO and Bluetooth 5.0 • Base on Android TV platform • Supports Widevine L1 and Playready 3.0 • Supports TR069 network management • Supports Google Play Store, Youtube, Google Cast, Google Assistant • Support customized Lanucher • Designed based on open technology, supports third-party applications effectively • Support power from TV USB *See, e.g.*, https://www.hisensebroadband.com/html/products/dongle/20240809_467.html

Claim 130	**Accused Instrumentalities**
	Features • Highest efficiency ARMv8 64-bit CPU, Quad core ARM Cortex-A55 CPU • High Performance GPU, ARM G31 MP2 GPU • Support AI video upscaling • Supports AV1 Video Decoding MP-10@L5.1 up to 4Kx2K@60fps • Supports VP9 Profile-2 Video Decoding up to 4Kx2K@60fps • Supports H.265 HEVC Video Decoding MP-10@L5.1 up to 4Kx2K@60fps • Supports H.264 AVC HP@L5.1 up to 4Kx2K@30fps • Supports HDMI 2.1 with HDCP2.2/HDCP2.3 • Supports Dolby Vision, HDR10, HDR10+, HLG HDR processing • Supports Wi-Fi 5 (802.11b/g/n/ac) 2x2 MU-MIMO and Bluetooth 5.0 • Base on Android TV platform • Supports Widevine L1 and Playready 3.0 • Supports TR069 network management • Supports Google Play Store, Youtube, Google Cast, Google Assistant • Support Netflix • Support customized Lanucher • Designed based on open technology, supports third-party applications effectively *See, e.g.*, https://www.hisensebroadband.com/html/products/broadcast%20stb/20240809_466.html

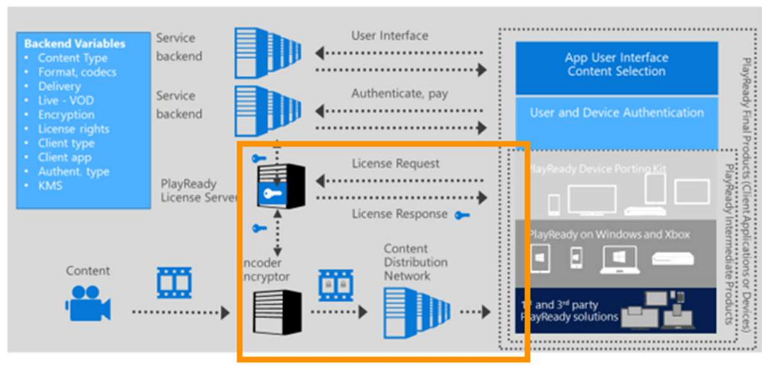
Claim 130	Accused Instrumentalities
	 **Figure 1.1. Sample Connection Topology of an HDCP System** *See, e.g.*, HDCP on HDMI Specification, Rev. 2.2 As an example, a license received by a DRM (e.g., PlayReady and/or Widevine) license server is a security message. **Deliver a license for the content** When a client makes a license request, it sends the content's PlayReady Header to the license issuer. The license issuer extracts the KID and determines the corresponding key value, using one of the methods described above—if it uses the key seed mechanism, it just regenerates the key based on the KID and key seed. Then it generates a license including this key, which it sends back to the client in a *license response*. *See, e.g.*, https://learn.microsoft.com/en-us/playready/overview/key-and-key-ids-kids

<table>
<tr><th>Claim 130</th><th>Accused Instrumentalities</th></tr>
<tr><td></td><td>

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.

See, e.g., https://learn.microsoft.com/en-us/playready/overview/certificates



On the left side of the illustration you can see the service has some Servers to stream the video (content distribution network). There are also some Servers that let the users browse the content and choose the content they want to play (user interface). In addition, there are some Servers that allow the users to log in and be authenticated, as well as pay for content (authenticate, pay). And, there is also a PlayReady License Server.

See, e.g., https://learn.microsoft.com/en-us/playready/overview/simple-end-to-end-system

HDCP enforcement requirements of the primary security system are contained within the license response.

</td></tr>
</table>

<table>
<tr><th>Claim 130</th><th>Accused Instrumentalities</th></tr>
<tr><td></td><td>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.

See, e.g., Compliance Rules for PlayReady Products

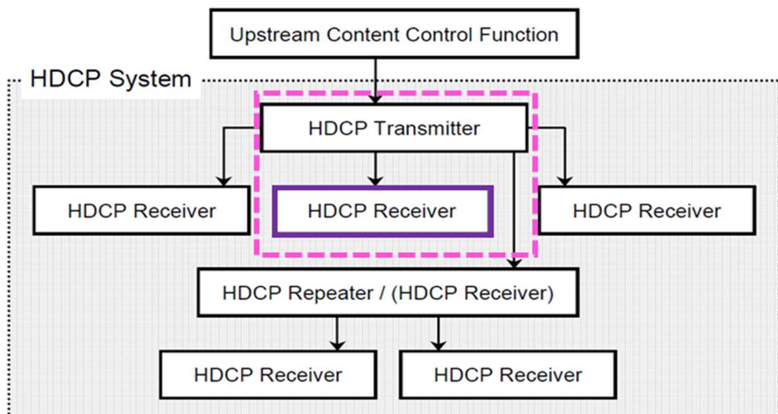
<table>
<tr><td>content_key_specs.
required_output_protection.
hdcp</td><td>string - one of:
HDCP_NONE,
HDCP_V1,
HDCP_V2</td><td>Indicates whether HDCP is required.

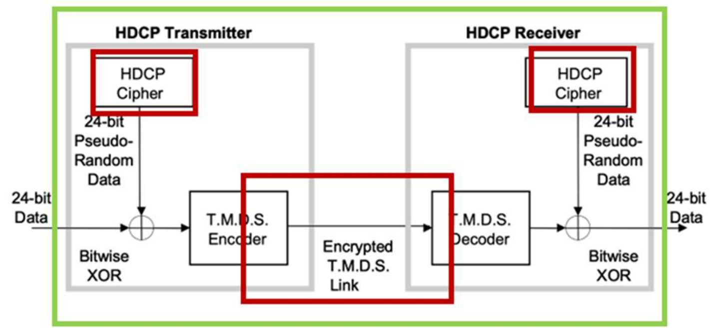
Default = HDCP_NONE.

Note: These must be capitalized, lowercase will result in a malformed request.

See Appendix.</td></tr>
</table>
See, e.g., Widevine DRM Proxy Integration</td></tr>
<tr><td>130[b] a processor coupled to the one or more communication interfaces, the processor to process the security messages, and the one or more communication interfaces to</td><td>The Accused Instrumentalities include a processor coupled to the one or more communication interfaces, the processor to process the security messages, and the one or more communication interfaces to transmit, to a secondary conditional access client through a network connection in a second security domain, access controlled data that is in an access controlled format and that is at least partially derived from the security messages.

For example, the Accused Instrumentalities incorporate a processor for providing functionality discussed herein coupled to the one or more communication interfaces (e.g., WiFi and/or Ethernet network interfaces), to process security messages (e.g., the license responses containing HDCP enforcement requirements and decryption keys described above). As an additional example of a communication interface, the Accused Instrumentalities include an HDMI interface.</td></tr>
</table>

Claim 130	**Accused Instrumentalities**
transmit, to a secondary conditional access client through a network connection in a second security domain, access controlled data that is in an access controlled format and that is at least partially derived from the security messages,	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. *See, e.g.*, HDCP on HDMI Specification, Rev. 2.2 The Accused Instrumentalities transmit to a secondary conditional access client (e.g., as shown in purple box below), such as an HDMI-connected display/audio device , via a HDMI network connection, in a second security domain (shown in pink box below), such as a HDCP encrypted security domain, access controlled data that is in an access controlled format (i.e., HDCP-encrypted content).  **Figure 1.1. Sample Connection Topology of an HDCP System**

Claim 130	Accused Instrumentalities
	See, e.g., HDCP on HDMI Specification, Rev. 2.2 **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** *See, e.g.*, HDCP on HDMI Specification, Rev. 2.2 The access controlled data that is in an access controlled format (i.e., the HDCP encrypted content) is at least partially derived from the security messages. For example, the Accused Instrumentalities derive HDCP control information from the licensing information discussed above, including for 4K and UHD content.

Claim 130	Accused Instrumentalities
	Each license contains the following information: • The content encryption key. • The rights of the license. • The right restrictions and right modifiers, also known as the conditions of the license. Before a client can decrypt the content associated with a license, it must retrieve the policy from the license. The content protection information within the license is encrypted using a client's public key or a client's domain's public key encryption information. The license is considered "bound" to the client or domain that has the private key for decrypting the content protection information. Clients acquire licenses either directly from License Servers or through a Proxy Server. *See, e.g.*, https://learn.microsoft.com/en-us/playready/overview/license-acquisition **Rights Restrictions and other Policies** The PlayReady Compliance Rules contain a full list of right modifiers (extensions and restrictions) that may apply to the license. Each of these modifiers has multiple properties: • **Action**—specifies the action of the policy (for example, engage HDCP encryption on the HDMI output). • **Optional**—specifies if the client must engage the action or must try to engage the action (for example, Output Control for Uncompressed Digital Video Content 250, see CR 3.6.5). *See, e.g.*, https://learn.microsoft.com/en-us/playready/overview/license-and-policies Content is transmitted to the connected device, over the HDMI interface as HDCP encrypted content in accordance with the requirements of the HDCP enforcement security messages specified by the primary security system platform.

Claim 130	Accused Instrumentalities

OPL	Compressed Digital Video	Uncompressed Digital Video		Analog TV
	Any	HDMI, DVI, DisplayPort, MHL		Component, Composite
0-100	Block	Passes content		Passes content
101-150				Passes content when CGMS-A CopyNever is engaged or if CGMS-A can't be engaged.
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		

See, e.g., https://learn.microsoft.com/en-us/playready/overview/output-protection-levels

<table>
<tr><th>Claim 130</th><th>Accused Instrumentalities</th></tr>
<tr><td></td><td>
<table>
<tr><td>content_key_specs.
required_output_protection.
hdcp</td><td>string - one of:
HDCP_NONE,
HDCP_V1,
HDCP_V2</td><td>Indicates whether HDCP is required.

Default = HDCP_NONE.

Note: These must be capitalized, lowercase will result in a malformed request.

See Appendix.</td></tr>
</table>

See, e.g., Widevine DRM Proxy Integration
</td></tr>
<tr><td>130[c] wherein the primary security system authenticates the conditional access server 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</td><td>
The primary security system authenticates the conditional access server clients of the primary security system through a first authentication process using a first root of trust. For example, the DRM (e.g., PlayReady and/or Widevine DRM) authenticates the Accused Instrumentality using a PlayReady and/or Widevine root of trust (PlayReady root of trust shown below).

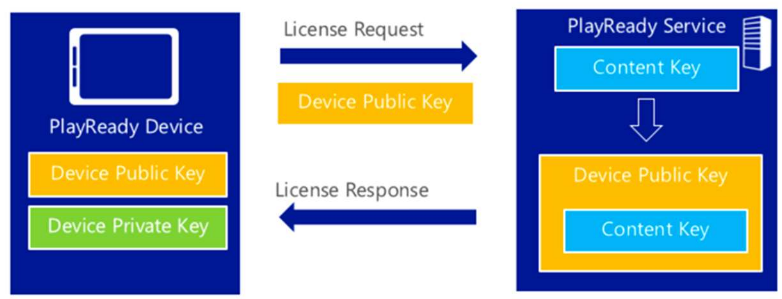
Client Authentication
In the context of content protection, client authentication may occur at two levels, the client device and the user. PlayReady handles device authentication automatically through its use of device keys when issuing licenses to PlayReady clients, as illustrated in the following diagram.


Figure 4 – Role of Device Keys in the Licensing Process

See, e.g., https://download.microsoft.com/download/B/D/4/BD42A75B-5B3E-49C0-B70D-DD49FA9592F9/DevelopingMicrosoftPlayReadyClients_March2015.pdf, p12
</td></tr>
</table>

<table>
<tr><th>Claim 130</th><th>Accused Instrumentalities</th></tr>
<tr><td>authentication process which is independent of the first authentication process and</td><td>
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).

See, e.g., 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.

See, e.g., https://learn.microsoft.com/en-us/playready/overview/certificates

The conditional access server authenticates clients of the conditional access server through a second authentication process which is independent of the first authentication process. For example, HDCP clients are authenticated using the HDCP authentication process (shown in the blue boxes in the below figures), which is independent of the first authentication processes described above.
</td></tr>
</table>

<table>
<tr><th>Claim 130</th><th>Accused Instrumentalities</th></tr>
<tr><td></td><td>

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

- 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.

The HDCP Transmitter contains the 3072-bit RSA public key of DCP LLC denoted by $kpub_{dcp}$.

The HDCP Receiver is issued 1024-bit RSA public and private keys. The public key is stored in a Public Key Certificate issued by DCP LLC, denoted by $cert_{rx}$. Table 2.1 gives the fields contained in the certificate. All values are stored in big-endian format.

<table>
<tr><th>Name</th><th>Size (bits)</th><th>Bit position</th><th>Function</th></tr>
<tr><td>Receiver ID</td><td>40</td><td>4175:4136</td><td>Unique receiver identifier. It has the same format as an HDCP 1.x KSV i.e. it contains 20 ones and 20 zeroes</td></tr>
<tr><td>Receiver Public Key</td><td>1048</td><td>4135:3088</td><td>Unique RSA public key of HDCP Receiver denoted by $kpub_{rx}$. The first 1024 bits is the big-endian representation of the modulus n and the trailing 24 bits is the big-endian representation of the public exponent e</td></tr>
<tr><td>Reserved2</td><td>4</td><td>3087:3084</td><td>Reserved for future definition. Must be 0x0 or 0x1.</td></tr>
<tr><td>Reserved1</td><td>12</td><td>3083:3072</td><td>Reserved for future definition. Must be 0x000</td></tr>
<tr><td>DCP LLC Signature</td><td>3072</td><td>3071:0</td><td>A cryptographic signature calculated over all preceding fields of the certificate. RSASSA-PKCS1-v1_5 is the signature scheme used as defined by PKCS #1 V2.1: RSA Cryptography Standard. SHA-256 is the underlying hash function</td></tr>
</table>

Table 2.1. Public Key Certificate of HDCP Receiver

See, e.g., HDCP on HDMI Specification, Rev. 2.2, pp. 11-12
</td></tr>
<tr><td>**130[d]** wherein the second authentication</td><td>The second authentication process uses a second root of trust which is independent of and different than the first root of trust.</td></tr>
</table>

Claim 130	**Accused Instrumentalities**
process uses a second root of trust which is independent of and different than the first root of trust, and	For example, the HDCP authentication process (shown in the blue boxes in the below figures) uses a different and independent root of trust than the DRM (e.g., PlayReady and/or Widevine) root of trust (shown in the yellow boxes and highlighting in the below figures) (PlayReady example shown below). 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). *See, e.g.*, 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. *See, e.g.*, https://learn.microsoft.com/en-us/playready/overview/certificates

<table>
<tr><th>Claim 130</th><th>Accused Instrumentalities</th></tr>
<tr><td></td><td>

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

- 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.

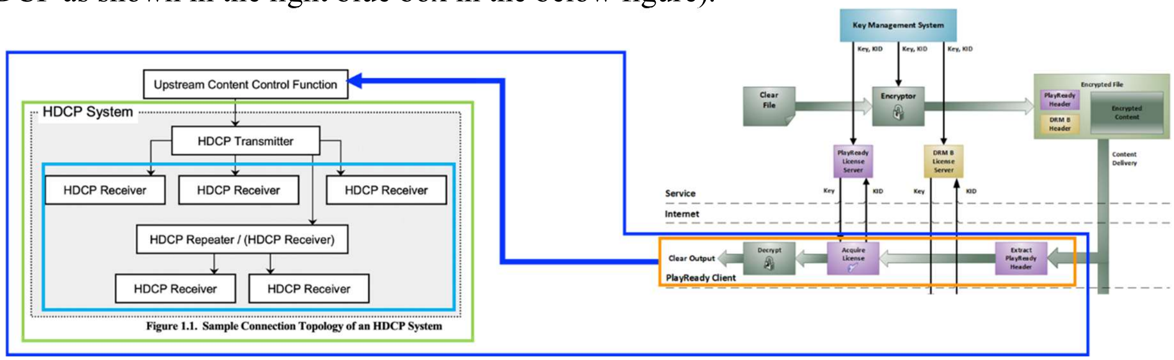
The HDCP Transmitter contains the 3072-bit RSA public key of DCP LLC denoted by $kpub_{dcp}$.

The HDCP Receiver is issued 1024-bit RSA public and private keys. The public key is stored in a Public Key Certificate issued by DCP LLC, denoted by $cert_{rx}$. Table 2.1 gives the fields contained in the certificate. All values are stored in big-endian format.

Name	Size (bits)	Bit position	Function
Receiver ID	40	4175:4136	Unique receiver identifier. It has the same format as an HDCP 1.x KSV i.e. it contains 20 ones and 20 zeroes
Receiver Public Key	1048	4135:3088	Unique RSA public key of HDCP Receiver denoted by $kpub_{rx}$. The first 1024 bits is the big-endian representation of the modulus n and the trailing 24 bits is the big-endian representation of the public exponent e
Reserved2	4	3087:3084	Reserved for future definition. Must be 0x0 or 0x1.
Reserved1	12	3083:3072	Reserved for future definition. Must be 0x000
DCP LLC Signature	3072	3071:0	A cryptographic signature calculated over all preceding fields of the certificate. RSASSA-PKCS1-v1_5 is the signature scheme used as defined by PKCS #1 V2.1: RSA Cryptography Standard. SHA-256 is the underlying hash function

Table 2.1. Public Key Certificate of HDCP Receiver

See, e.g., HDCP on HDMI Specification, Rev. 2.2, pp. 11-12
</td></tr>
<tr><td>130[e] wherein the conditional access server is</td><td>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.</td></tr>
</table>

Claim 130	Accused Instrumentalities
configured to substitute the first security domain with the second security domain for the clients under the second root of trust.	For example, the Accused Instrumentalities are configured to decrypt the content in the first security domain (e.g., the PlayReady DRM-protected content (or Widevine DRM-protected content), shown in the orange box in the below figure) and re-encrypt the content with the second security domain (e.g., using HDCP encryption, shown in the light green box in the below figure) for client devices under a second root of trust (e.g., devices that support HDCP as shown in the light blue box in the below figure).  *See, e.g.*, HDCP on HDMI Specification, Rev. 2.2*;* https://learn.microsoft.com/en-us/playready/overview/playready-and-other-protection-technologies