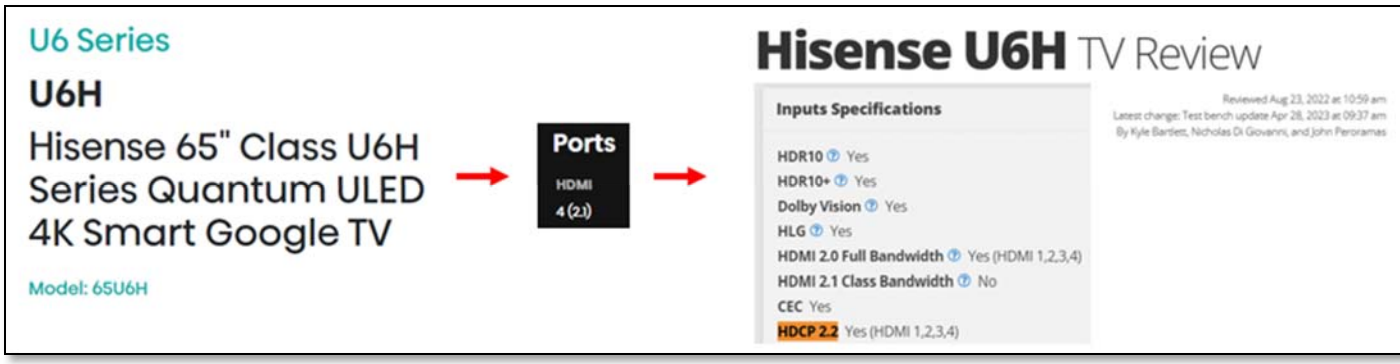
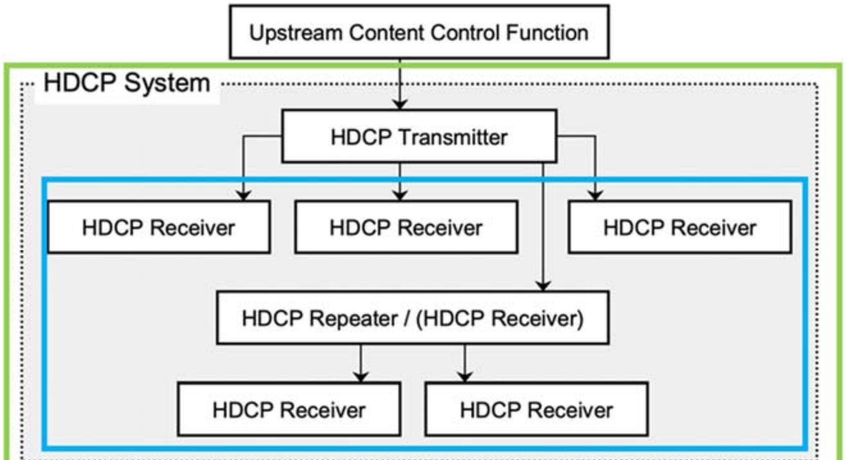
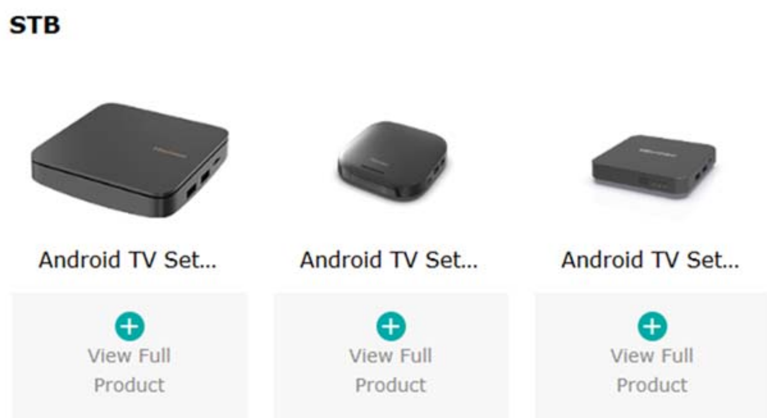
EXHIBIT F

Exhibit F – U.S. Patent No. 8,667,304 ("'304 Patent")

Claim 5	**Accused Instrumentalities**
5[pre.1] 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	The Hisense Accused Instrumentalities include Hisense devices compatible with HDCP, including, e.g., 4K TVs (e.g., Hisense 4K Smart Google TVs, including the Hisense U6H). By way of example, the Accused Instrumentalities are configured to play HDCP-protected content (including, e.g., 4K Ultra HD and High Dynamic Range Content) via the HDMI interface of the Accused Instrumentalities, including e.g., streamed content from a streamed media device (e.g., a cable box, or other external streaming equipment).  *See, e.g.*, 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. To the extent the preamble is limiting, the Accused Instrumentalities incorporate 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.

Claim 5	Accused Instrumentalities
	For example, the Accused Instrumentalities are client systems in a second security domain (e.g., a security domain associated with HDCP). The Accused Instrumentalities employ memory, such as RAM memory, to store executable program instructions (e.g., the OS operating system and/or other firmware for the operation of the Accused Instrumentalities). Each Accused Instrumentality includes a data processing system (e.g., a processor). Executing the computer program instructions by the data processing system causes content in a second security domain (e.g., HDCP security domain, shown in the light green box in the below figure) to be presented (e.g., played or provided for playing) by the Accused Instrumentalities. The content originally is provided by a first conditional access server (e.g., a streaming content server).  **Figure 1.1. Sample Connection Topology of an HDCP System** *See, e.g.*, HDCP on HDMI Specification, Rev. 2.2
5[pre.2] wherein the first conditional	The Accused Instrumentalities are configured to be connected to streaming media devices (e.g., streaming media devices, cable boxes, or other external streaming equipment) via an HDMI interface for streaming 4K Ultra HD and High Dynamic Range Content. The Accused Instrumentalities are configured to receive high-bandwidth data. The Accused Instrumentalities are configured to receive data by the streaming device for use in

Claim 5	**Accused Instrumentalities**
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	the Accused Instrumentalities that is protected with DRM functionality such as PlayReady and/or Widevine. For example, the Accused Instrumentalities are configured to receive data from a Hisense STB or other external device that was protected with PlayReady and/or Widevine:  *See, e.g.*, https://www.hisensebroadband.com/html/products/broadcast%20stb/

Claim 5	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 To the extent the preamble is limiting, 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. For example, the first conditional access server (e.g., the streaming content server) authenticated a streaming media device using a PlayReady root of trust in a first security domain (e.g., PlayReady DRM, in the example shown below). As another example, the first conditional access server authenticates a streaming media device using a Widevine root of trust in the Widevine DRM security domain.

Claim 5	Accused Instrumentalities

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.

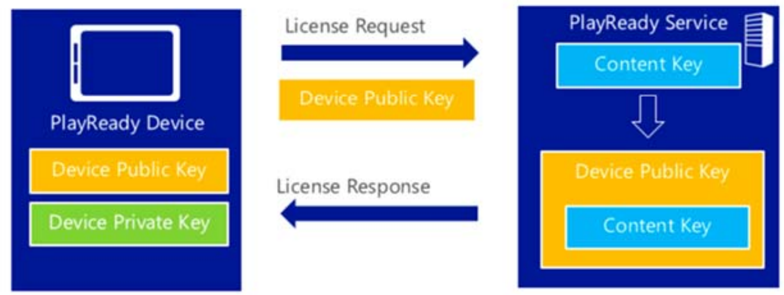
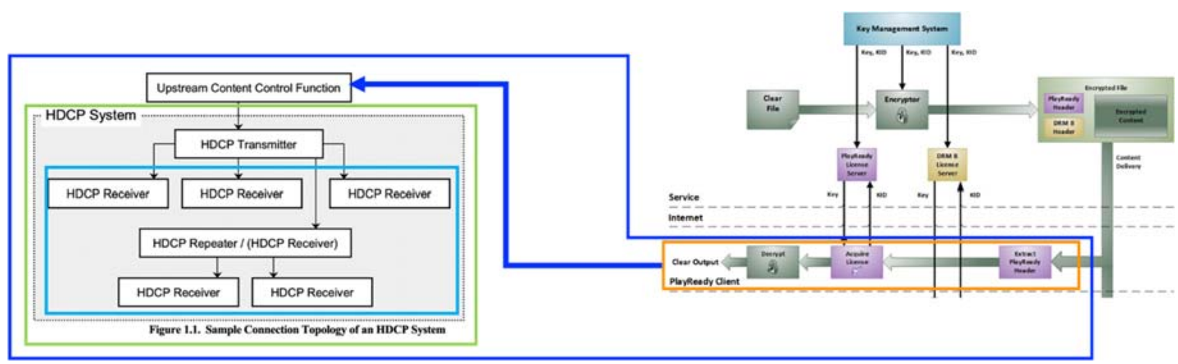


Figure 4 – Role of Device Keys in the Licensing Process

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

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

Claim 5	Accused Instrumentalities
	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
5[pre.3] 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:	To the extent the preamble is limiting, 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. For example, a second conditional access server (e.g., the streaming media device that serves content to the Accused Instrumentalities) decrypts 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-encrypts the content in 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., that support HDCP as shown in the light blue box in the below figure). 

<table>
<tr><th>Claim 5</th><th>Accused Instrumentalities</th></tr>
<tr><td></td><td>

See, *e.g.*, HDCP on HDMI Specification, Rev. 2.2; https://learn.microsoft.com/en-us/playready/overview/playready-and-other-protection-technologies

HDCP employs an established authentication process and root of trust for HDCP client devices.

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

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

Claim 5	Accused Instrumentalities
	See, e.g., HDCP on HDMI Specification, Rev. 2.2, pp. 11-12
5[a] 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	The Accused Instrumentalities receive an authentication through a second authentication process which is independent of the first authentication process. For example, the Accused Instrumentalities receive an authentication using the HDCP authentication process (shown in the blue boxes in the below figures), which is independent of the first authentication process (e.g., DRM). **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.

<table>
<tr><th>Claim 5</th><th>Accused Instrumentalities</th></tr>
<tr><td></td><td>
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>5[b] 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</td><td>
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.

For example, the HDCP authentication process (shown in the blue boxes in the below figures) uses a different root of trust than the PlayReady root of trust (or the Widevine root of trust) (shown in the yellow boxes and highlighting in the below figures).

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).
</td></tr>
</table>

Claim 5	Accused Instrumentalities
	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 **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.

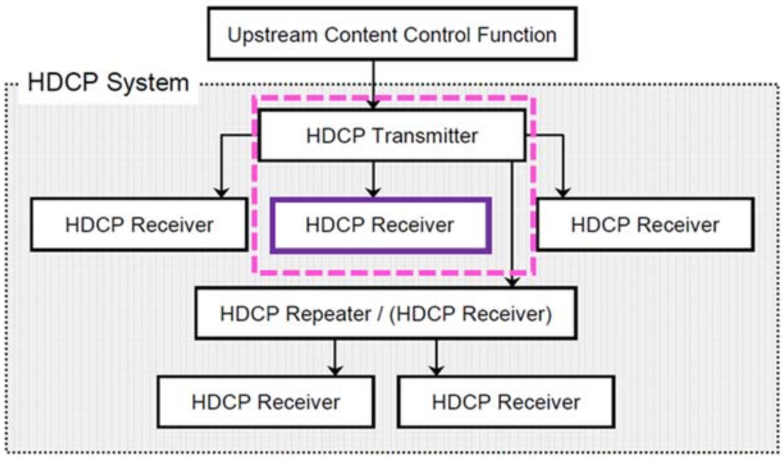
<table>
<tr><th>Claim 5</th><th>Accused Instrumentalities</th></tr>
<tr><td></td><td>
The HDCP Transmitter contains the 3072-bit RSA public key of DCP LLC denoted by $kpub_{dcp}$.

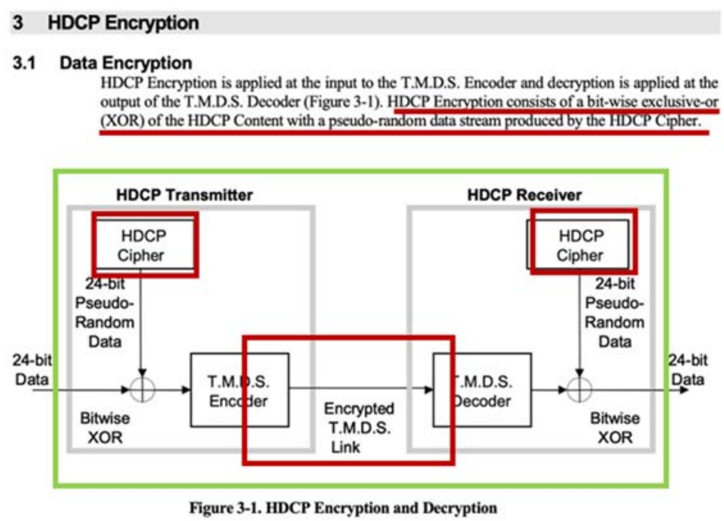
The HDCP Receiver is issued 1024-bit RSA public and private keys. The public key is stored in a Public Key Certificate issued by DCP LLC, denoted by $cert_{rx}$. Table 2.1 gives the fields contained in the certificate. All values are stored in big-endian format.

<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>**5[c]** 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</td><td>
The Accused Instrumentalities receive 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.

For example, the Accused Instrumentalities receive (e.g., using an HDCP Receiver) content in an access controlled format (e.g., HDCP encrypted content) in a second security domain (e.g., as shown in the pink box below), such as a HDCP encrypted security domain.
</td></tr>
</table>

Claim 5	Accused Instrumentalities
conditional access client being in the second security domain.	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  **Figure 1.1. Sample Connection Topology of an HDCP System** *See, e.g.*, HDCP on HDMI Specification, Rev. 2.2

Claim 5	Accused Instrumentalities
	 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 format is specified by the second conditional access server. For example, streaming media devices derive HDCP control information from PlayReady (or Widevine) licensing information, including for 4K and UHD content.

Claim 5	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 The Accused Instrumentalities receive content over the HDMI interface as HDCP encrypted content in accordance with engaging the HDCP requirements of the PlayReady (or Widevine) HDCP enforcement requirements as specified by the streaming media device during engagement of HDCP over HDMI.

<table>
<tr><th>Claim 5</th><th>Accused Instrumentalities</th></tr>
<tr><td></td><td>
<table>
<tr><th rowspan="2">OPL</th><th>Compressed Digital Video</th><th colspan="2">Uncompressed Digital Video</th><th>Analog TV</th></tr>
<tr><th>Any</th><th colspan="2">HDMI, DVI, DisplayPort, MHL</th><th>Component, Composite</th></tr>
<tr><td>0-100</td><td rowspan="6">Block</td><td colspan="2" rowspan="3">Passes content</td><td>Passes content</td></tr>
<tr><td>101-150</td><td>Passes content when CGMS-A CopyNever is engaged or if CGMS-A can't be engaged.</td></tr>
<tr><td>151-200</td><td>Passes content when CGMS-A CopyNever is engaged.</td></tr>
<tr><td>201-250</td><td colspan="2">Attempts to engage HDCP, but passes content regardless of result.</td><td rowspan="4">Does NOT pass content</td></tr>
<tr><td>251-270</td><td>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.</td><td>HWDRM: Passes content with HDCP. If HDCP fails to engage, playback to HDMI/DVI ports is blocked.</td></tr>
<tr><td>271-300</td><td colspan="2">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.</td></tr>
<tr><td>>300</td><td></td><td colspan="2">Does NOT pass content</td></tr>
</table>
See, e.g., https://learn.microsoft.com/en-us/playready/overview/output-protection-levels
</td></tr>
</table>

Claim 5	**Accused Instrumentalities**
	<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