

EXHIBIT 24

Exhibit 24: Claim Chart Showing Infringement for U.S. Patent No. 9,313,178

The Lenovo Mobile Phone Products (“Lenovo Mobile Phones”) are listed in Exhibit 12, including exemplary product Motorola Edge (2022), and infringe at least one claim of the ’178 Patent. No part of this exemplary chart construes, or is intended to construe, the specification, file history, or claims of the ’178 Patent. Moreover, this exemplary chart does not limit, and is not intended to limit, Ericsson’s infringement or domestic industry positions or contentions.

Claims	Motorola Edge (2022) (“Accused Device”)
1. A method for handling secure distribution of content comprising:	When a user operates a Motorola Edge (2022), which implements the Google Widevine DRM system, the user is causing the device to implement “a method for handling secure distribution of content.” The Motorola Edge (2022) includes a Widevine Content Decryption Module (CDM), with a Security level L1, which is used to decrypt content for playback. A Widevine CDM with Security level L1 is incorporated into the Motorola Edge (2022) by the manufacturer. The “secure distribution of live video content” corresponds to live streaming content secured with encryption keys. The Motorola Edge (2022) is representative of the other Lenovo Mobile Phone Products for purposes of practice of the asserted claims because these products all implement the Google Widevine DRM system. Ex. 76 (https://www.gsmarena.com/motorola_edge_(2022)-11777.php) at 1:

INFRINGEMENT CLAIM CHART FOR
LENOVO MOBILE PHONES – U.S. PATENT NO. 9,313,178



The DRM Info app was installed to reveal the DRM software already loaded on the Accused Device, as follows. Ex. 77 (Screenshots from Motorola Edge (2022)) at 1-3:

INFRINGEMENT CLAIM CHART FOR
LENOVO MOBILE PHONES – U.S. PATENT NO. 9,313,178

4:52

DRM Info

motorola motorola edge (2022)

Brand
motorola

Hardware
mt6879

SoC Manufacturer
Mediatek

SoC Model
MT6879V/ZA

Build
S2ST532.71-53-3-1-4

Build Type
user

Build Fingerprint
motorola/tesla_g_sys/tesla:12/S2ST532.71-53-3-1-4/
aab5af:user/release-keys

SDK Level
31

Release or Codename
12

Supported ABI
arm64-v8a, armeabi-v7a, armeabi

Supported Hardware Decoder
audio/gsm, image/vnd.android.heic, video/3gpp, video/avc, video/hevc, video/mp4v-es, video/mpeg2, video/x-vnd.on2.vp8, video/x-vnd.on2.vp9

Supported HDR Types
HDR10, HDR10+, HLG

Supported Refresh Rate (Hz)
48, 60, 90, 120, 144

ClearKey CDM

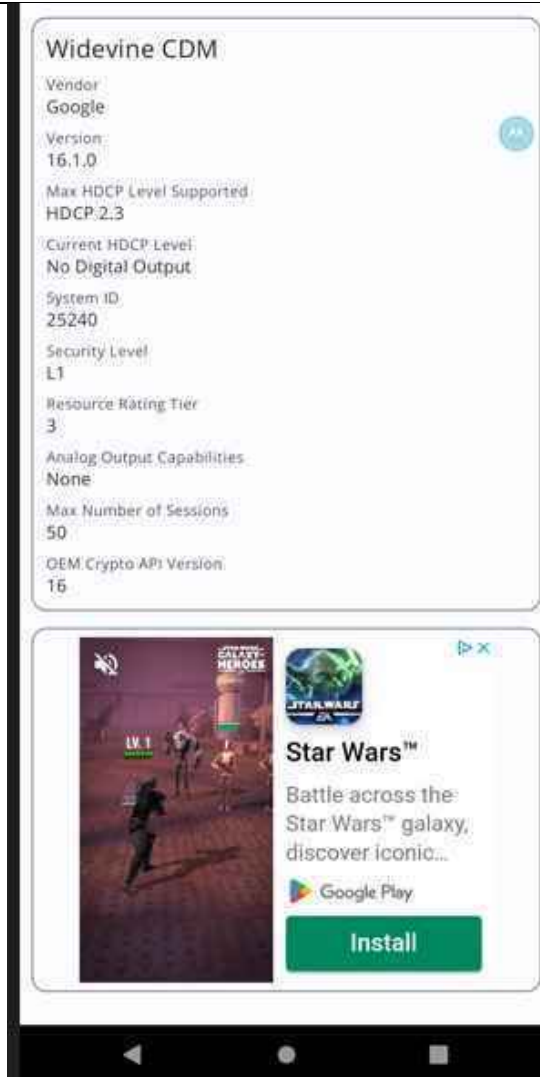
Vendor
Google

Version
1.2

Max HDCP Level Supported
No Digital Output

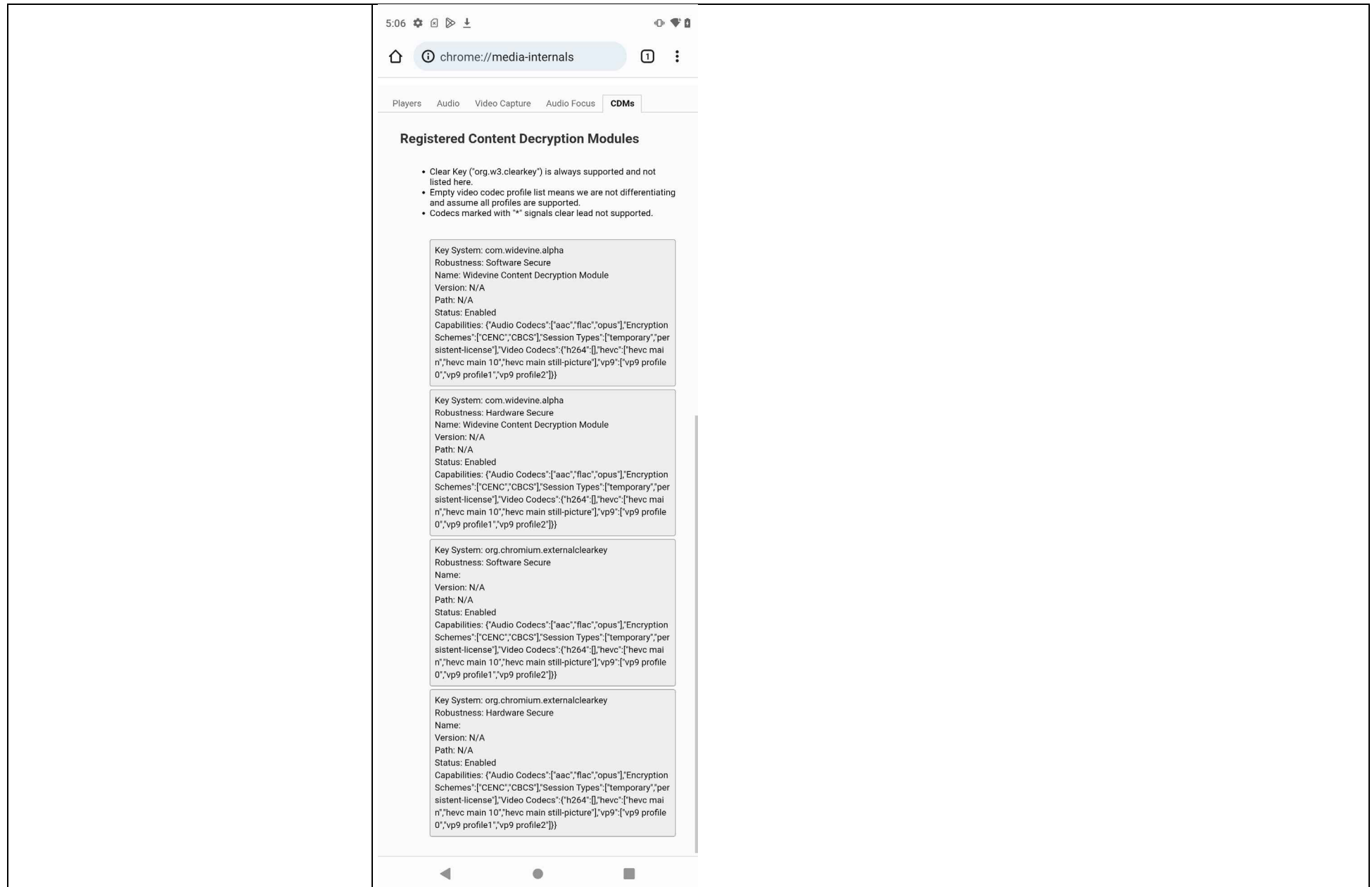
Current HDCP Level
None

INFRINGEMENT CLAIM CHART FOR
LENOVO MOBILE PHONES – U.S. PATENT NO. 9,313,178



The following screenshot from the pre-installed Google Chrome browser pointing to the internal <chrome://media-internals> URL reveals the DRM software loaded on the Accused Device. Ex. 77 at 4:

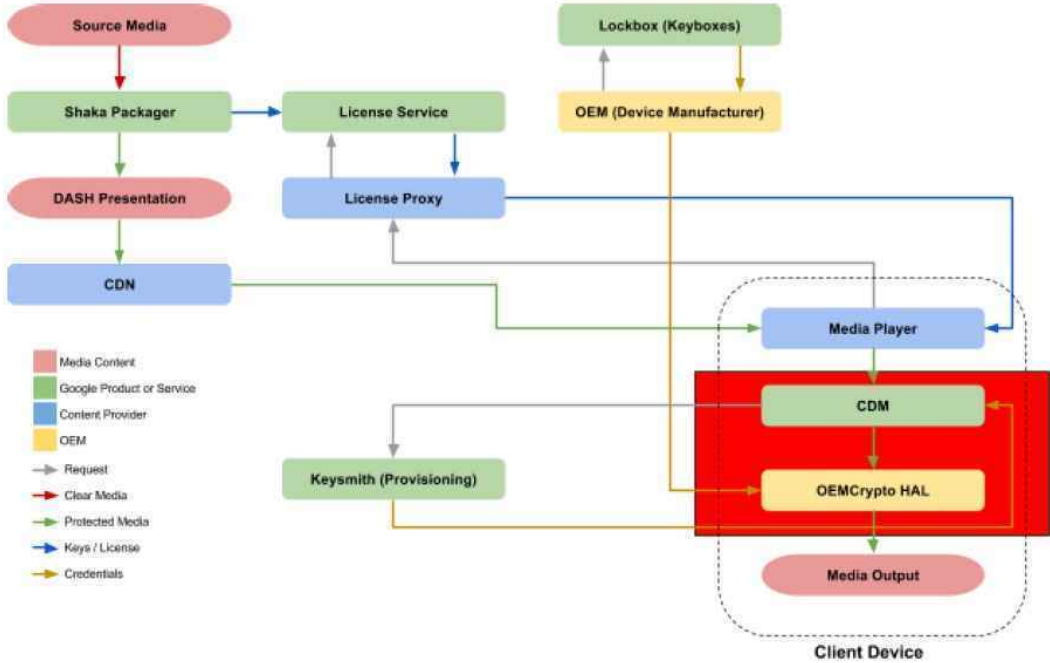
INFRINGEMENT CLAIM CHART FOR LENOVO MOBILE PHONES – U.S. PATENT NO. 9,313,178



INFRINGEMENT CLAIM CHART FOR
LENOVO MOBILE PHONES – U.S. PATENT NO. 9,313,178

	Ex. 79 (WIDEVINE Getting Started Widevine DRM on Devices Version 1.5 (2018)) at 6, 12: Widevine Client Security Levels The following security level definitions are used by Widevine: Security Level 1 (L1) Widevine DRM keys and decrypted content are never exposed to the host CPU. Only security hardware or a protected security co-processor uses clear key values and the media content is decrypted by the secure hardware. Key requirements of this security level: • Device manufacturers must provide a secure bootloader. The chain of trust from the bootloader must extend through any software or firmware components involved in the security implementation, such as the ARM TrustZone protected application and any components involved in the enforcement of the secure video path. • The Widevine keybox must be encrypted with a device-unique secret key that is not visible to software or probing methods outside of the TrustZone. The Widevine key-box must be installed in the factory or delivered to the device using an approved secure delivery mechanism. • Device manufacturers must provide an implementation of the Widevine Level 1 OEMCrypto API that performs all key processing and decryption in a trusted environment. All content processing, cryptography, and control is performed within the Trusted Execution Environment (TEE). In some implementation models, security processing may be performed in different chips. This level of security requires factory provisioning of the Widevine keybox or requires the Widevine keybox to be protected by a device key installed at the time of manufacturing. The Device Provisioning Models document provides additional information about Widevine device provisioning models. This is the recommended path for any device integration as it provides the highest level of security. [...]
--	---

INFRINGEMENT CLAIM CHART FOR
LENOVO MOBILE PHONES – U.S. PATENT NO. 9,313,178

	Ecosystem  Ex. 80 (WIDEVINE Modular DRM Key Rotation Version 1 (2014)) at 2: Introduction This document describes changes to the Widevine common encryption API to support key rotation. Key rotation allows the key used to encrypt the content to change midstream, typically for use in live streaming.
initiating a media playback request and receiving a playback request response.	When a user operates an Accused Device, which implements the Google Widevine DRM system, the user is causing the device to perform the steps of “initiating a media playback request and receiving a playback request response.” The Motorola Edge (2022) includes a media player, which receives media in response to a request to a Content Delivery Network (“CDN”) and, when the media is encrypted, issues a license request

INFRINGEMENT CLAIM CHART FOR
LENOVO MOBILE PHONES – U.S. PATENT NO. 9,313,178

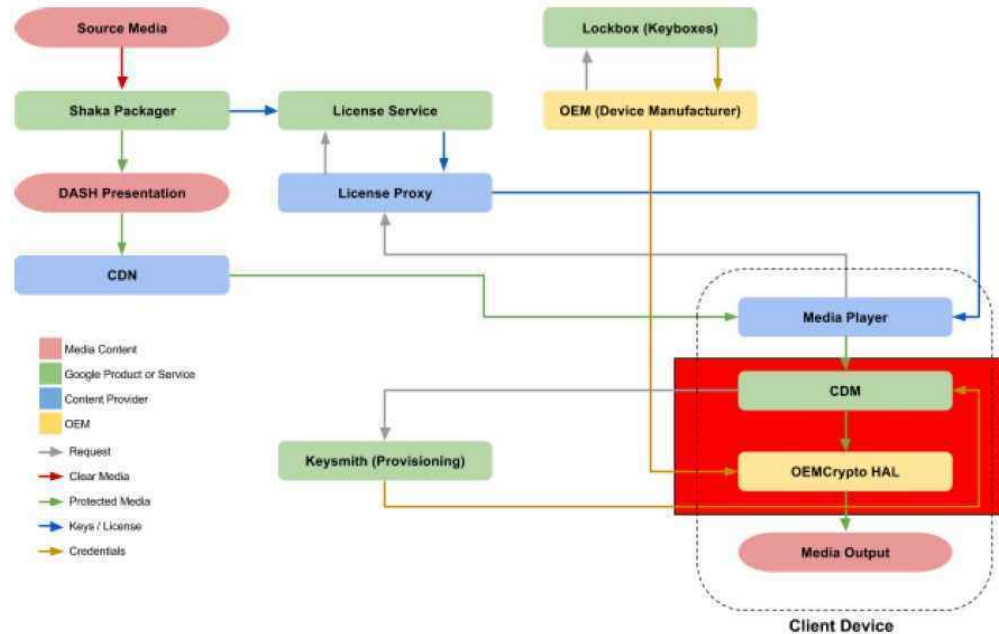
	to the license server. The Motorola Edge (2022) media player receives the media from the CDN and a license from the license server. The “media playback request” corresponds to a request for media sent to the CDN and/or the license request. The “playback request response” corresponds to the media and related content received from the CDN and/or receipt of the license from the license server. Ex. 81 (WIDEVINE DRM Architecture Overview Version 1.2 (March 6, 2017)) at 11:
--	--

INFRINGEMENT CLAIM CHART FOR
LENOVO MOBILE PHONES – U.S. PATENT NO. 9,313,178

	The following eight steps explain the sequence of security exchanges for decryption: 1. Receive Media from Content Delivery Network (CDN) The browser's media engine determines that the media is encrypted. The initialization data (InitData) is extracted from the content by the browser and sent to the Player as an event. User authorization is up to the client, not Widevine. 2. Pass Data to the Content Decryption Module (CDM) The Player passes the initData to the Content Decryption Module. The Player is not able to decrypt anything. 3. CDM Passes License Request to the Player Having received data from the Player, the CDM creates a license request and passes the request information back to the Player. 4. Player Passes License Request to License Server (via proxy) Once the Player has the License Request, it can now pass that request to the Widevine License Server (via proxy). But the Player cannot read the request itself or take any action except to pass it on. 5. License Server Passes License to Player When the License Server receives the request, it responds to the request by sending the license back to the Player. The license is an encrypted message that includes license information data. 6. The Player Passes the License to the Content Decryption Module The Player passes the encrypted license to the Content Decryption Module. 7. The CDM Passes Data to the OEMCrypto Module Because the CDM is not in the Trusted Layer of the device, it must pass the information to the OEMCrypto Module, which does reside in the Trusted layer of the device. The actual decryption takes place in the OEMCrypto Module. In some implementations, the decoding takes place there also. The Browser does the actual parsing of the container. 8. OEMCrypto Sends Video Chunks to the Screen Ex. 79 at 6:
--	---

INFRINGEMENT CLAIM CHART FOR
LENOVO MOBILE PHONES – U.S. PATENT NO. 9,313,178

Ecosystem



Ex. 80 at 3:

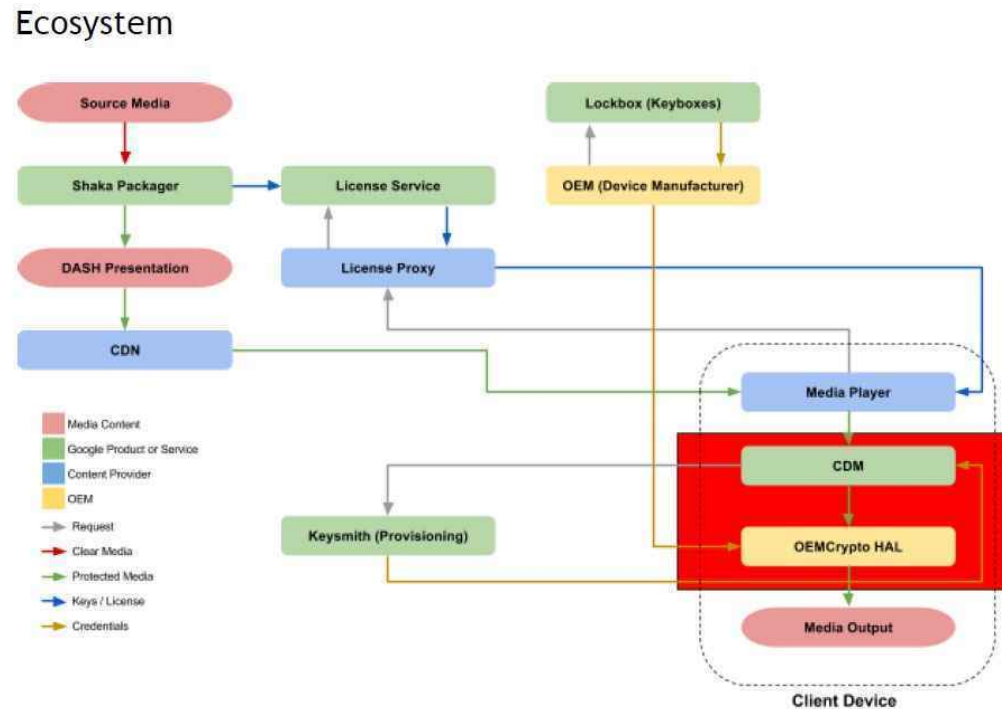
Generate License

The license exchange protocol requires no changes. If the user tunes into the live stream described above, the client will issue a license request containing the 'pssh' box from the media segment at the playback starting point. The license server will then issue a license containing the keys for that media segment, as well as the keys for the previous key rotation period, and the following key rotation period. Fewer keys may be provided if playing the media near the start (previous period key omitted), or near the end (following period key omitted). This allows content for the following key rotation period to be decrypted while the license request for it is being processed, and for reverse trick-play.

INFRINGEMENT CLAIM CHART FOR
LENOVO MOBILE PHONES – U.S. PATENT NO. 9,313,178

parsing content from the playback request response, the content information including content encryption keys, content encryption key identifiers, and content encryption key expiration times;	When a user operates an Accused Device, which implements the Google Widevine DRM system, the user is causing the device to perform the step of “parsing content from the playback request response, the content information including content encryption keys, content encryption key identifiers, and content encryption key expiration times.” The Motorola Edge (2022) media player retrieves information from the CDN and from the license received from the license server. The information includes: keys for the media segment, keys for the previous key rotation period, and keys for the following rotation period; key_ids, which identify the keys; and the crypto periods, which identify the key rotation periods. The “content encryption keys” correspond to the keys for the current, previous, and following key rotation periods. The “content encryption key identifiers” correspond to the key_ids. The “content encryption key expiration times” correspond to the key rotation periods. Ex. 79 at 6:
---	---

INFRINGEMENT CLAIM CHART FOR
LENOVO MOBILE PHONES – U.S. PATENT NO. 9,313,178



Ex. 80 at 3:

Generate License

The license exchange protocol requires no changes. If the user tunes into the live stream described above, the client will issue a license request containing the 'pssh' box from the media segment at the playback starting point. The license server will then issue a license containing the keys for that media segment, as well as the keys for the previous key rotation period, and the following key rotation period. Fewer keys may be provided if playing the media near the start (previous period key omitted), or near the end (following period key omitted). This allows content for the following key rotation period to be decrypted while the license request for it is being processed, and for reverse trick-play.

INFRINGEMENT CLAIM CHART FOR
LENOVO MOBILE PHONES – U.S. PATENT NO. 9,313,178

	[...] In addition to the 100 KIDs, 100 'pssh' data blobs are returned. Each 'pssh' data blob contains key Id, content Id, and track type. For key rotation, the 'pssh' will also contain the crypto period, which for the example above would be as follows: <i>'pssh' (1) : crypto_period_index = 383517</i> <i>'pssh' (2) : crypto_period_index = 383518</i> ... <i>'pssh' (100) : crypto_period_index = 383616</i> Note that even without key_period, the pssh is sufficient to locate a key by key_id. Including key_period enables us to also prefetch adjacent keys in the same stream.
retrieving content and manifest files from a content delivery server;	When a user operates an Accused Device, which implements the Google Widevine DRM system, the user is causing the device to perform the step of “retrieving content and manifest files from a content delivery server.” The Motorola Edge (2022) media player retrieves premium video content, distributed in files, and manifest files (MPDs) from a Content Delivery Network. The “content” corresponds to the premium video content. The “manifest files” correspond to the manifest (MPD), which describe the different resolutions and bandwidth for each media file. Ex. 81 at 5-6, 10-11: Architecture Component Relationships The Widevine DRM components work together to create an end-to-end platform for protecting premium video content, and provides all the tools you need to go from the content preparation stage to the final delivery on any device. The flow process begins by preparing your media with Common Encryption and the Shaka Packager for adaptive streaming. Once prepared, the content is encrypted with licenses which are stored on the Widevine License Server. Later, when the encrypted content streams to the Player via a Content Delivery Network, the License Server provides license information to a supported media player. The encrypted content is then passed to the device's Content Decryption Module, enabling secure playback with the OEMCrypto Module. [...] Media Packaging

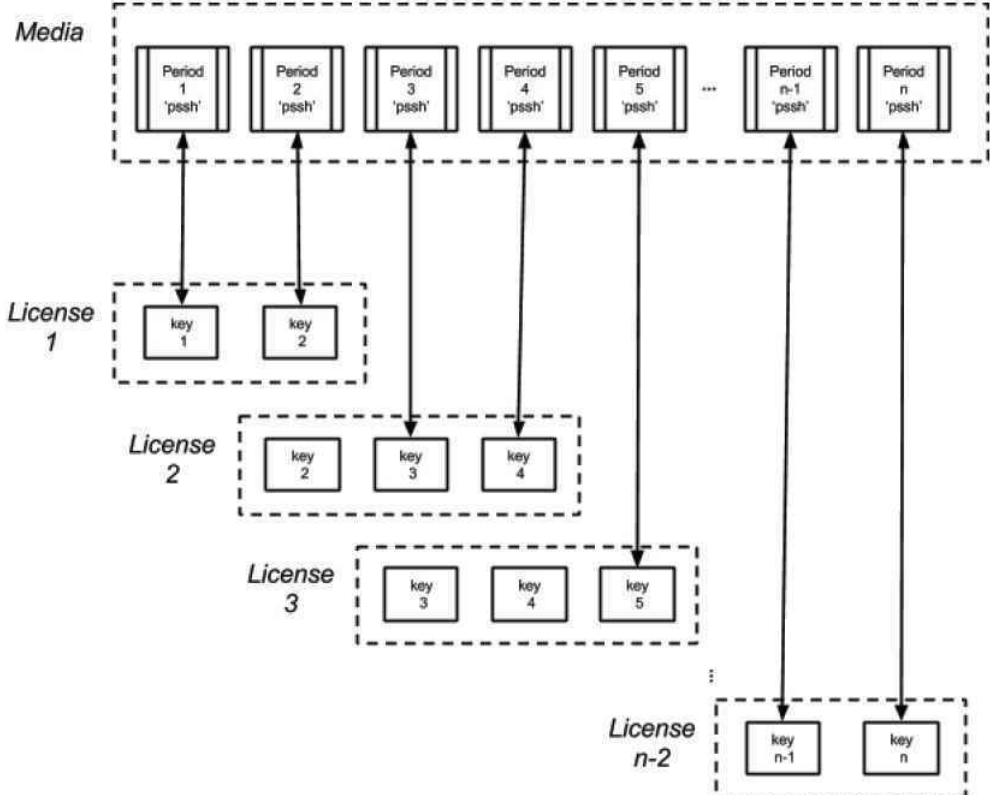
INFRINGEMENT CLAIM CHART FOR
LENOVO MOBILE PHONES – U.S. PATENT NO. 9,313,178

	Widevine DRM provides a complete open-source DASH packaging system called Shaka Packager. The packager converts files of different resolutions and bandwidth to fragmented MP4, defining equal-length segments for all desired files. A manifest (MPD) is prepared that describes the different resolutions and bandwidth for each file. When a player receives encrypted content, it requests the appropriate segment that will provide optimal viewing at that moment, but can request different segments as bandwidth conditions change. [...] 1. Receive Media from Content Delivery Network (CDN) The browser's media engine determines that the media is encrypted. The initialization data (InitData) is extracted from the content by the browser and sent to the Player as an event.
detecting content encryption key rotation boundaries between periods of use of different content encryption keys in decryption retrieved content;	When a user operates an Accused Device, which implements the Google Widevine DRM system, the user is causing the device to perform the step of “detecting content encryption key rotation boundaries between periods of use of different content encryption keys in decryption retrieved content.” The Motorola Edge (2022) media player detects key rotation boundaries between key rotation periods by encountering a new ‘pssh’ box and issuing a new license request. Ex. 80 at 3: Rotation boundary The key rotation boundary occurs whenever the client encounters a new ‘pssh’ box, at which point it will issue a new license request, but can in the meantime continue to decrypt content, as it already has the keys required to decrypt the new key period, whether playing forwards or backwards.
issuing requests to a license server ahead of a key rotation boundary to retrieve a second content encryption key to be used after a content encryption key rotation boundary is reached; and	When a user operates an Accused Device, which implements the Google Widevine DRM system, the user is causing the device to perform the step of “issuing requests to a license server ahead of a key rotation boundary to retrieve a second content encryption key to be used after a content encryption key rotation boundary is reached.” The Motorola Edge (2022) media player issues license request ahead of a key rotation period to the license server for keys for the current, upcoming, and previous key rotation periods. Ex. 80 at 3:

INFRINGEMENT CLAIM CHART FOR
LENOVO MOBILE PHONES – U.S. PATENT NO. 9,313,178

	Generate License The license exchange protocol requires no changes. If the user tunes into the live stream described above, the client will issue a license request containing the ‘pssh’ box from the media segment at the playback starting point. The license server will then issue a license containing the keys for that media segment, as well as the keys for the previous key rotation period, and the following key rotation period. Fewer keys may be provided if playing the media near the start (previous period key omitted), or near the end (following period key omitted). This allows content for the following key rotation period to be decrypted while the license request for it is being processed, and for reverse trickplay.
applying the second key for content decryption after the key rotation boundary is reached.	When a user operates an Accused Device, which implements the Google Widevine DRM system, the user is causing the device to perform the step of “applying the second key for content decryption after the key rotation boundary is reached.” The Motorola Edge (2022) media player applies keys from the license to continue to decrypt content after a key rotation boundary is reached, as the license from the license server included keys to decrypt content from the following key rotation period. Ex. 80 at 3, 4: Rotation boundary The key rotation boundary occurs whenever the client encounters a new ‘pssh’ box, at which point it will issue a new license request, but can in the meantime continue to decrypt content, as it already has the keys required to decrypt the new key period, whether playing forwards or backwards. [...]

INFRINGEMENT CLAIM CHART FOR
LENOVO MOBILE PHONES – U.S. PATENT NO. 9,313,178

	 The diagram illustrates the Widevine DRM system architecture. At the top, a dashed box labeled 'Media' contains a sequence of periods: 'Period 1 'pssh'', 'Period 2 'pssh'', 'Period 3 'pssh'', 'Period 4 'pssh'', 'Period 5 'pssh'', an ellipsis, 'Period n-1 'pssh'', and 'Period n 'pssh''. Below this, four license layers are shown, each in a dashed box. 'License 1' contains 'key 1' and 'key 2', with arrows pointing to 'Period 1' and 'Period 2'. 'License 2' contains 'key 2', 'key 3', and 'key 4', with arrows pointing to 'Period 3' and 'Period 4'. 'License 3' contains 'key 3', 'key 4', and 'key 5', with an arrow pointing to 'Period 5'. 'License n-2' contains 'key n-1' and 'key n', with arrows pointing to 'Period n-1' and 'Period n'. Vertical ellipses between 'License 3' and 'License n-2' indicate intermediate licenses.
16. A computerized device operable as a client for handling secure distribution of content, comprising:	A Motorola Edge (2022), which implements the Google Widevine DRM system, is a “computerized device operable as a client for handling secure distribution of content.” A Motorola Edge (2022) is a client for live streaming content secured with encryption keys. The Motorola Edge (2022) includes a Widevine Content Decryption Module (CDM), with a Security level L1, which is used to decrypt content for playback. A Widevine CDM with Security level L1 is incorporated into the Motorola Edge (2022) by the manufacturer. The “computerized device operable as a client” corresponds to the Motorola Edge (2022). The “secure distribution of content” corresponds to live streaming content secured with encryption keys. Ex. 76 at 1:

INFRINGEMENT CLAIM CHART FOR
LENOVO MOBILE PHONES – U.S. PATENT NO. 9,313,178



The DRM Info app was installed to reveal the DRM software already loaded on the Accused Device, as follows. Ex. 77 at 1-3:

INFRINGEMENT CLAIM CHART FOR
LENOVO MOBILE PHONES – U.S. PATENT NO. 9,313,178

4:52

DRM Info

motorola motorola edge (2022)

Brand
motorola

Hardware
mt6879

SoC Manufacturer
Mediatek

SoC Model
MT6879V/ZA

Build
S2TS32.71-53-3-1-4

Build Type
user

Build Fingerprint
motorola/tesla_g_sys/tesla:12/S2TS32.71-53-3-1-4/
aab5af:user/release-keys

SDK Level
31

Release or Codename
12

Supported ABI
arm64-v8a, armeabi-v7a, armeabi

Supported Hardware Decoder
audio/gsm, image/vnd.android.heic, video/3gpp, video/avc, video/hevc, video/mp4v-es, video/mpeg2, video/x-vnd.on2.vp8, video/x-vnd.on2.vp9

Supported HDR Types
HDR10, HDR10+, HLG

Supported Refresh Rate (Hz)
48, 60, 90, 120, 144

ClearKey CDM

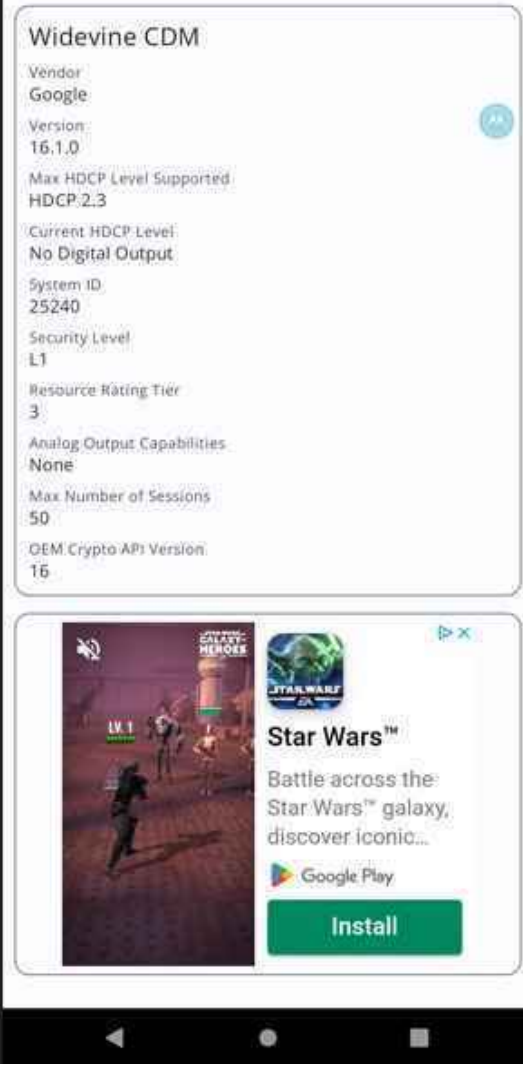
Vendor
Google

Version
1.2

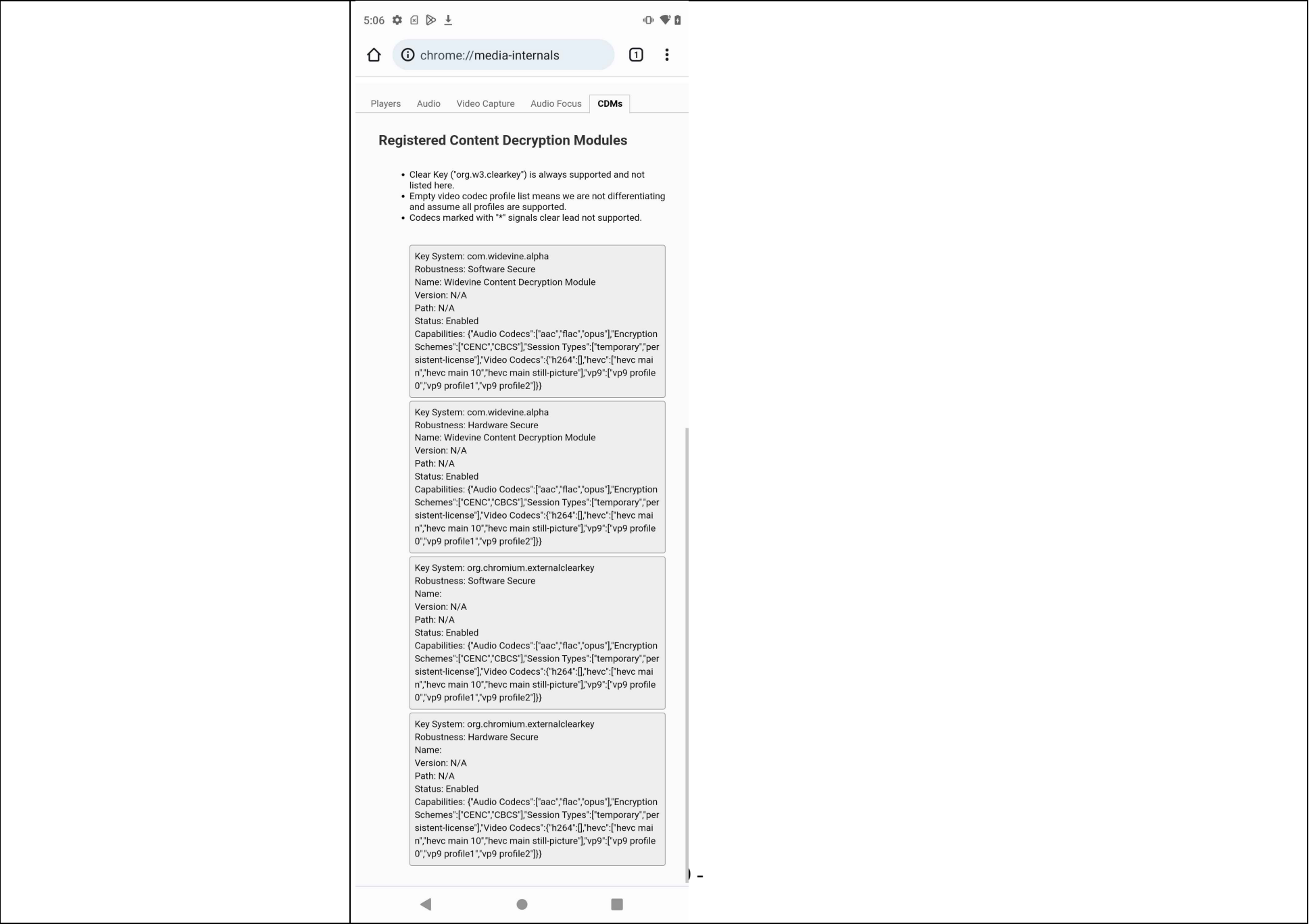
Max HDCP Level Supported
No Digital Output

Current HDCP Level
None

INFRINGEMENT CLAIM CHART FOR
LENOVO MOBILE PHONES – U.S. PATENT NO. 9,313,178

	 The screenshot shows two panels from an Android device. The top panel, titled 'Widevine CDM', displays the following information: Vendor: Google; Version: 16.1.0; Max HDCP Level Supported: HDCP.2.3; Current HDCP Level: No Digital Output; System ID: 25240; Security Level: L1; Resource Rating Tier: 3; Analog Output Capabilities: None; Max Number of Sessions: 50; OEM Crypto API Version: 15. The bottom panel is an advertisement for the 'Star Wars™' game on Google Play, featuring a character in a desert environment and an 'Install' button. The Android navigation bar is visible at the bottom of the screen.	The following screenshot from the pre-installed Google Chrome browser pointing to the internal chrome://media-internals URL also reveals the DRM software loaded on the Accused Device. Ex. 77 at 4:
--	--	--

INFRINGEMENT CLAIM CHART FOR
LENOVO MOBILE PHONES – U.S. PATENT NO. 9,313,178



INFRINGEMENT CLAIM CHART FOR
LENOVO MOBILE PHONES – U.S. PATENT NO. 9,313,178

Ex. 79 at 6, 12:

Widevine Client Security Levels

The following security level definitions are used by Widevine:

Security Level 1 (L1)

Widevine DRM keys and decrypted content are never exposed to the host CPU. Only security hardware or a protected security co-processor uses clear key values and the media content is decrypted by the secure hardware.

Key requirements of this security level:

- Device manufacturers must provide a secure bootloader. The chain of trust from the bootloader must extend through any software or firmware components involved in the security implementation, such as the ARM TrustZone protected application and any components involved in the enforcement of the secure video path.
- The Widevine keybox must be encrypted with a device-unique secret key that is not visible to software or probing methods outside of the TrustZone. The Widevine key-box must be installed in the factory or delivered to the device using an approved secure delivery mechanism.
- Device manufacturers must provide an implementation of the Widevine Level 1 OEMCrypto API that performs all key processing and decryption in a trusted environment.

All content processing, cryptography, and control is performed within the Trusted Execution Environment (TEE). In some implementation models, security processing may be performed in different chips.

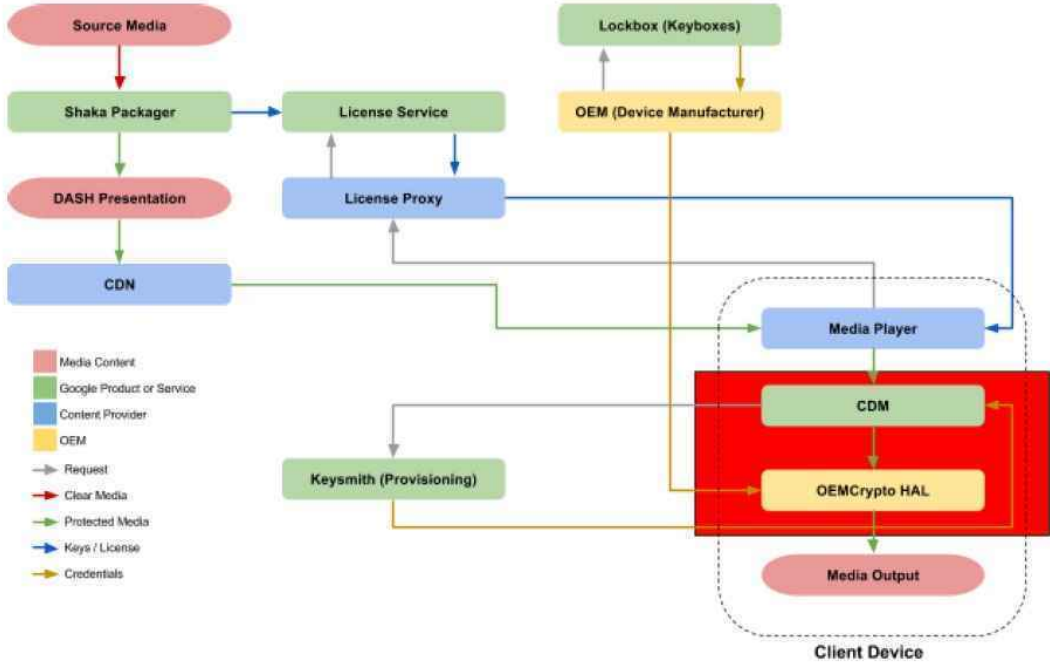
This level of security requires factory provisioning of the Widevine keybox or requires the Widevine keybox to be protected by a device key installed at the time of manufacturing.

The [Device Provisioning Models document](#) provides additional information about Widevine device provisioning models.

This is the recommended path for any device integration as it provides the highest level of security.

[...]

INFRINGEMENT CLAIM CHART FOR
LENOVO MOBILE PHONES – U.S. PATENT NO. 9,313,178

	Ecosystem  Ex. 80 at 2: Introduction This document describes changes to the Widevine common encryption API to support key rotation. Key rotation allows the key used to encrypt the content to change midstream, typically for use in live streaming.
memory operative to store computer program instructions; one or more processors; input/output interface circuitry; and	The Motorola Edge (2022) includes “memory operative to store computer program instructions; one or more processors; input/output interface circuitry; and interconnect circuitry coupling the memory, processors, and input/output interface circuitry together, wherein the processors are operative to execute the computer program instructions from the memory to cause the computerized device to” perform the functions

INFRINGEMENT CLAIM CHART FOR
LENOVO MOBILE PHONES – U.S. PATENT NO. 9,313,178

interconnect circuitry coupling the memory, processors, and input/output circuitry together;
wherein the processors are operative to execute the computer program instructions from the memory to cause the computerized device to:

described herein. The Motorola Edge (2022) includes 6 or 8 GB of RAM and 128 or 256 GB of internal memory storage (depending on model) and an Octa-core MediaTek Dimensity 1050 System-on-a-Chip (SoC). The Motorola Edge (2022) includes an Android Operating System and the Widevine CDM, both stored on the internal memory.

Ex. 76 at 1:

PLATFORM	OS	Android 12, planned upgrade to Android 13
	Chipset	MediaTek Dimensity 1050 (6 nm)
	CPU	Octa-core (2x2.5 GHz Cortex-A78 & 6x2.0 GHz Cortex-A55)
	GPU	Arm Mali-G610 MC3
MEMORY	Card slot	No
	Internal	128GB 6GB RAM, 256GB 8GB RAM

Ex. 77 at 1-3:

INFRINGEMENT CLAIM CHART FOR
LENOVO MOBILE PHONES – U.S. PATENT NO. 9,313,178

	4:52 DRM Info motorola motorola edge (2022) Brand motorola Hardware mt6879 SoC Manufacturer Mediatek SoC Model MT6879V/ZA Build S2TS32.71-53-3-1-4 Build Type user Build Fingerprint motorola/tesla_g_sys/tesla:12/S2TS32.71-53-3-1-4/ aab5af:user/release-keys SDK Level 31 Release or Codename 12 Supported ABI arm64-v8a, armeabi-v7a, armeabi Supported Hardware Decoder audio/gsm, image/vnd.android.heic, video/3gpp, video/avc, video/hevc, video/mp4v-es, video/mpeg2, video/x-vnd.on2.vp8, video/x-vnd.on2.vp9 Supported HDR Types HDR10, HDR10+, HLG Supported Refresh Rate (Hz) 48, 60, 90, 120, 144	ClearKey CDM Vendor Google Version 1.2 Max HDCP Level Supported No Digital Output Current HDCP Level None
--	--	---

INFRINGEMENT CLAIM CHART FOR
LENOVO MOBILE PHONES – U.S. PATENT NO. 9,313,178

	Widevine CDM Vendor Google Version 16.1.0 Max HDCP Level Supported HDCP.2.3 Current HDCP Level No Digital Output System ID 25240 Security Level L1 Resource Rating Tier 3 Analog Output Capabilities None Max Number of Sessions 50 OEM Crypto API Version 15 Star Wars™ Battle across the Star Wars™ galaxy, discover iconic... Google Play Install	
initiate a media playback request and receive a playback request response;	The computer program instructions on the Accused Device will cause the device to “initiate a media playback request and receive a playback request response.” The Motorola Edge (2022) includes a media	

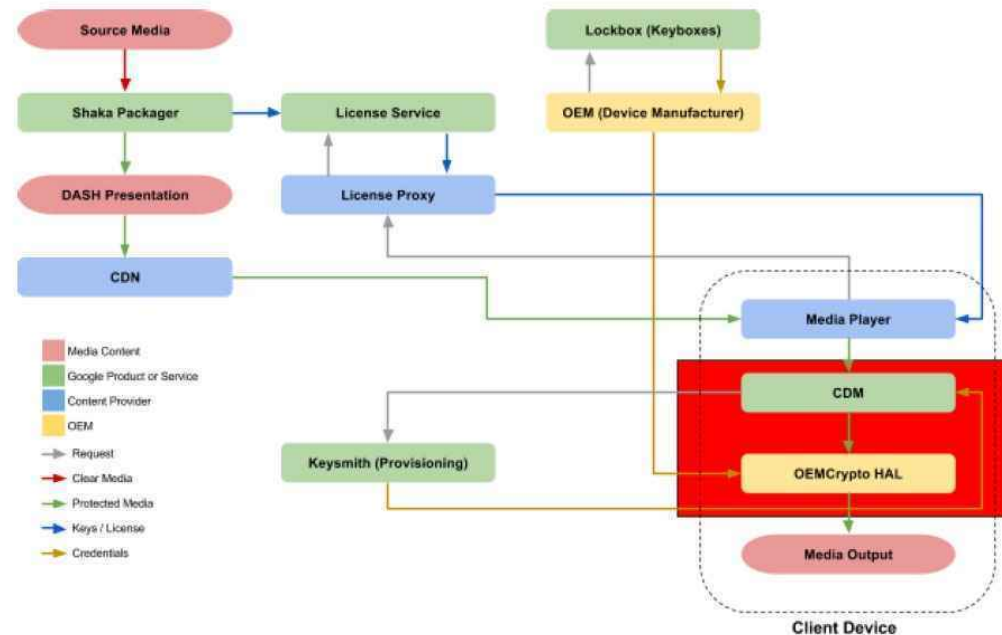
INFRINGEMENT CLAIM CHART FOR
LENOVO MOBILE PHONES – U.S. PATENT NO. 9,313,178

	player, which receives media in response to a request to a Content Delivery Network (“CDN”) and, when the media is encrypted, issues a license request to the license server. The Motorola Edge (2022) media player receives the media from the CDN and a license from the license server. The “media playback request” corresponds to a request for media sent to the CDN and/or the license request. The “playback request response” corresponds to the media and related content received from the CDN and/or receipt of the license from the license server.] Ex. 81 at 11: The following eight steps explain the sequence of security exchanges for decryption: 1. Receive Media from Content Delivery Network (CDN) The browser’s media engine determines that the media is encrypted. The initialization data (InitData) is extracted from the content by the browser and sent to the Player as an event. User authorization is up to the client, not Widevine. 2. Pass Data to the Content Decryption Module (CDM) The Player passes the initData to the Content Decryption Module. The Player is not able to decrypt anything. 3. CDM Passes License Request to the Player Having received data from the Player, the CDM creates a license request and passes the request information back to the Player. 4. Player Passes License Request to License Server (via proxy) Once the Player has the License Request, it can now pass that request to the Widevine License Server (via proxy). But the Player cannot read the request itself or take any action except to pass it on. 5. License Server Passes License to Player When the License Server receives the request, it responds to the request by sending the license back to the Player. The license is an encrypted message that includes license information data. 6. The Player Passes the License to the Content Decryption Module The Player passes the encrypted license to the Content Decryption Module. 7. The CDM Passes Data to the OEMCrypto Module Because the CDM is not in the Trusted Layer of the device, it must pass the information to the OEMCrypto Module, which does reside in the Trusted layer of the device. The actual decryption takes place in the OEMCrypto Module. In some implementations, the decoding takes place there also. The Browser does the actual parsing of the container. 8. OEMCrypto Sends Video Chunks to the Screen
--	---

INFRINGEMENT CLAIM CHART FOR
LENOVO MOBILE PHONES – U.S. PATENT NO. 9,313,178

Ex. 79 at 6:

Ecosystem



Ex. 80 at 3:

Generate License

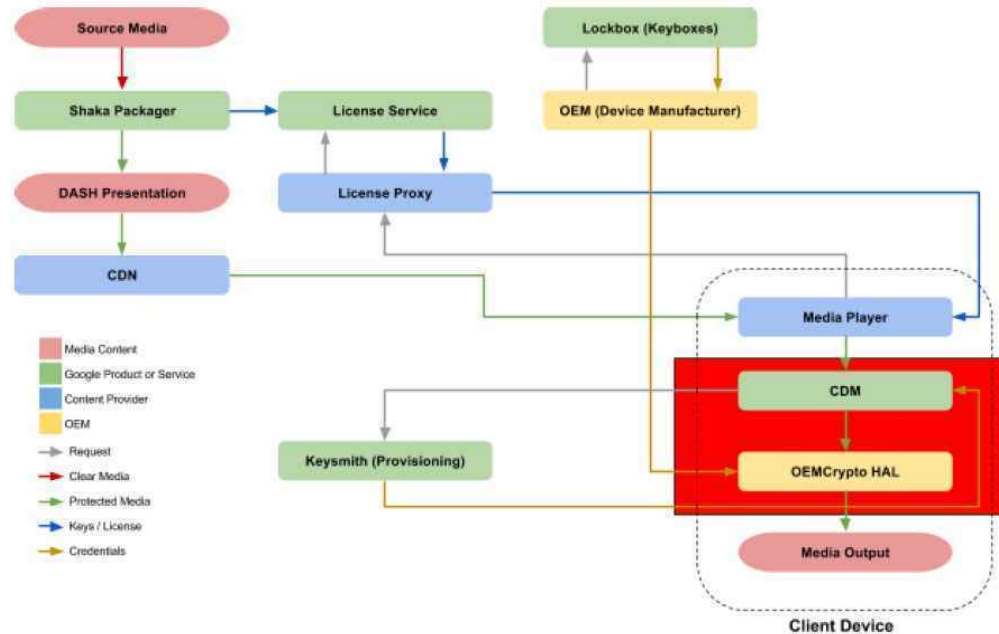
The license exchange protocol requires no changes. If the user tunes into the live stream described above, the client will issue a license request containing the 'pssh' box from the media segment at the playback starting point. The license server will then issue a license containing the keys for that media segment, as well as the keys for the previous key rotation period, and the following key rotation period. Fewer keys may be provided if playing the media near the start (previous period key omitted), or near the end (following period key omitted). This allows content for the following

INFRINGEMENT CLAIM CHART FOR
LENOVO MOBILE PHONES – U.S. PATENT NO. 9,313,178

	key rotation period to be decrypted while the license request for it is being processed, and for reverse trick-play.
parse content information from the playback request response, the content information including content encryption keys, content encryption key identifiers, and content encryption key expiration times;	The computer program instructions on the Accused Device will cause the device to “parse content information from the playback request response, the content information including content encryption keys, content encryption key identifiers, and content encryption key expiration times.” The Motorola Edge (2022) media player retrieves information from the CDN and from the license received from the license server. The information includes: keys for the media segment, keys for the previous key rotation period, and keys for the following rotation period; key_ids, which identify the keys; and the crypto periods, which identify the key rotation periods. The “content encryption keys” correspond to the keys for the current, previous, and following key rotation periods. The “content encryption key identifiers” correspond to the key_ids. The “content encryption key expiration times” correspond to the key rotation periods. Ex. 79 at 6:

INFRINGEMENT CLAIM CHART FOR
LENOVO MOBILE PHONES – U.S. PATENT NO. 9,313,178

Ecosystem



Ex. 80 at 3:

Generate License

The license exchange protocol requires no changes. If the user tunes into the live stream described above, the client will issue a license request containing the 'pssh' box from the media segment at the playback starting point. The license server will then issue a license containing the keys for that media segment, as well as the keys for the previous key rotation period, and the following key rotation period. Fewer keys may be provided if playing the media near the start (previous period key omitted), or near the end (following period key omitted). This allows content for the following key rotation period to be decrypted while the license request for it is being processed, and for reverse trick-play.

INFRINGEMENT CLAIM CHART FOR
LENOVO MOBILE PHONES – U.S. PATENT NO. 9,313,178

	[...] In addition to the 100 KIDs, 100 'pssh' data blobs are returned. Each 'pssh' data blob contains key Id, content Id, and track type. For key rotation, the 'pssh' will also contain the crypto period, which for the example above would be as follows: <i>'pssh' (1) : crypto_period_index = 383517</i> <i>'pssh' (2) : crypto_period_index = 383518</i> ... <i>'pssh' (100) : crypto_period_index = 383616</i> Note that even without key_period, the pssh is sufficient to locate a key by key_id. Including key_period enables us to also prefetch adjacent keys in the same stream.
retrieve content and manifest files from a content delivery server;	The computer program instructions on the Accused Device will cause the device to “retrieve content and manifest files from a content delivery server.” The Motorola Edge (2022) media player retrieves premium video content, distributed in files, and manifest files (MPDs) from a Content Delivery Network. The “content” corresponds to the premium video content. The “manifest files” correspond to the manifest (MPD), which describe the different resolutions and bandwidth for each media file. Ex. 81 at 5-6, 10-11: Architecture Component Relationships The Widevine DRM components work together to create an end-to-end platform for protecting premium video content, and provides all the tools you need to go from the content preparation stage to the final delivery on any device. The flow process begins by preparing your media with Common Encryption and the Shaka Packager for adaptive streaming. Once prepared, the content is encrypted with licenses which are stored on the Widevine License Server. Later, when the encrypted content streams to the Player via a Content Delivery Network, the License Server provides license information to a supported media player. The encrypted content is then passed to the device's Content Decryption Module, enabling secure playback with the OEMCrypto Module. [...]

INFRINGEMENT CLAIM CHART FOR
LENOVO MOBILE PHONES – U.S. PATENT NO. 9,313,178

	Media Packaging Widevine DRM provides a complete open-source DASH packaging system called Shaka Packager. The packager converts files of different resolutions and bandwidth to fragmented MP4, defining equal-length segments for all desired files. A manifest (MPD) is prepared that describes the different resolutions and bandwidth for each file. When a player receives encrypted content, it requests the appropriate segment that will provide optimal viewing at that moment, but can request different segments as bandwidth conditions change. [...] 1. Receive Media from Content Delivery Network (CDN) The browser's media engine determines that the media is encrypted. The initialization data (InitData) is extracted from the content by the browser and sent to the Player as an event.
detect content encryption key rotation boundaries between periods of use of different content encryption keys in decrypting retrieved content;	The computer program instructions on the Accused Device will cause the device to “detect content encryption key rotation boundaries between periods of use of different content encryption keys in decrypting retrieved content.” The Motorola Edge (2022) media player detects key rotation boundaries between key rotation periods by encountering a new ‘pssh’ box and issuing a new license request. Ex. 80 at 3: Rotation boundary The key rotation boundary occurs whenever the client encounters a new ‘pssh’ box, at which point it will issue a new license request, but can in the meantime continue to decrypt content, as it already has the keys required to decrypt the new key period, whether playing forwards or backwards.
issue request to a license server ahead of a key rotation boundary to retrieve a second content encryption key to be used after a content encryption key rotation boundary is reached; and	The computer program instructions on the Accused Device will cause the device to “issue request to a license server ahead of a key rotation boundary to retrieve a second content encryption key to be used after a content encryption key rotation boundary is reached.” The Motorola Edge (2022) media player issues license request ahead of a key rotation period to the license server for keys for the current, upcoming, and previous key rotation periods. Ex. 80 at 3:

INFRINGEMENT CLAIM CHART FOR
LENOVO MOBILE PHONES – U.S. PATENT NO. 9,313,178

	Generate License The license exchange protocol requires no changes. If the user tunes into the live stream described above, the client will issue a license request containing the ‘pssh’ box from the media segment at the playback starting point. The license server will then issue a license containing the keys for that media segment, as well as the keys for the previous key rotation period, and the following key rotation period. Fewer keys may be provided if playing the media near the start (previous period key omitted), or near the end (following period key omitted). This allows content for the following key rotation period to be decrypted while the license request for it is being processed, and for reverse trick-play.
apply the second key for content decryption after the key rotation boundary is reached.	The computer program instructions on the Accused Device will cause the device to “apply the second key for content decryption after the key rotation boundary is reached.” The Motorola Edge (2022) media player applies keys from the license to continue to decrypt content after a key rotation boundary is reached, as the license from the license server included keys to decrypt content from the following key rotation period. Ex. 80 at 3, 4: Rotation boundary The key rotation boundary occurs whenever the client encounters a new ‘pssh’ box, at which point it will issue a new license request, but can in the meantime continue to decrypt content, as it already has the keys required to decrypt the new key period, whether playing forwards or backwards. [...]

INFRINGEMENT CLAIM CHART FOR
LENOVO MOBILE PHONES – U.S. PATENT NO. 9,313,178

