

5 THINGS

You Need To Know About Multi-DRM Technology

Understand the components of Multi-DRM such as three major DRM schemes, content packaging, and playback integration



TABLE OF CONTENTS



1	Introduction	4
2	Part 1 - Microsoft PlayReady DRM	
	• History of PlayReady	5
	• PlayReady Components and How They Work	6
	• Features and Benefits	7
	• Use Cases	8
	• Supported Platforms and Content Formats	9
3	PART 2 – Google Widevine DRM	
	• History of Widevine	10
	• Widevine Components and How They Work	11
	• Features and Benefits	12
	• Use Cases	13
	• Supported Platforms and Content Formats	14
3	PART 3 – Apple FairPlay DRM	
	• History of FairPlay	15
	• FairPlay Components and How They Work	17
	• Features and Benefits	19
	• Use Cases	20
	• Supported Platforms and Content Formats	21

4	PART 4 – DRM Packaging and CPIX/SPEKE API	
	• Output of Multi DRM packaging	22
	• Various DRM packaging methods	23
4	PART 5 – MULTI-DRM CLIENT INTEGRATION	
	• Playback Process of DRM Content	27
	• DRM license integration method	28
	• Multi-DRM Content Playback by Client Type	31
5	CONCLUSION	
	• References	34
6	Contact Us	35

INTRODUCTION

We are living in a world of online video streaming and OTT. As the growth of OTT video services, the need for content security is getting higher.

One of the biggest concerns for paid content providers is that their content can be illegally leaked and the number of paid subscribers may decline or growth may slow.

To prevent unauthorized use and leakage of content, many online content services are applying a multi-DRM solution provided by professional DRM vendors. A multi-DRM solution basically has license management features for multiple DRM systems such as PlayReady, Widevine and FairPlay to support major web browsers and mobile OS.

In this whitepaper, we will examine each of the DRMs and related elements of multi-DRM technology.



PART 1 – MICROSOFT PLAYREADY DRM



WHAT IS MICROSOFT PLAYREADY

Microsoft PlayReady DRM is a set of technologies that can be used to securely distribute audio/video content over the network and prevent unauthorized use. This technology is used to define and enforce the user's rights to digital media content. (Ref. #1)

Content service providers can control the expiration date of the content's playback, the resolution of the content that can be played on the screen, the type of screen on which the content is rendered, and many others.

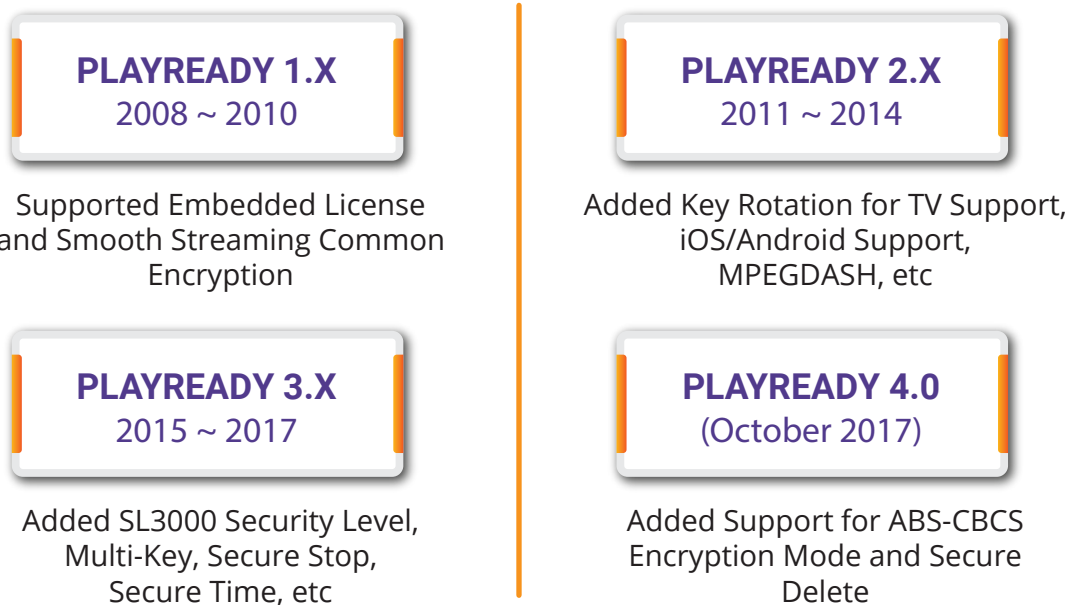
PlayReady technology can be integrated into media applications on televisions, set-top boxes, cell phones, tablets, personal computers, and other devices to enforce content access rules defined by content owners.

HISTORY OF PLAYREADY

PlayReady was first announced at the 2007 3GMS World Congress (now it's called as Mobile World Congress) in Barcelona, Spain. (Ref. #2)

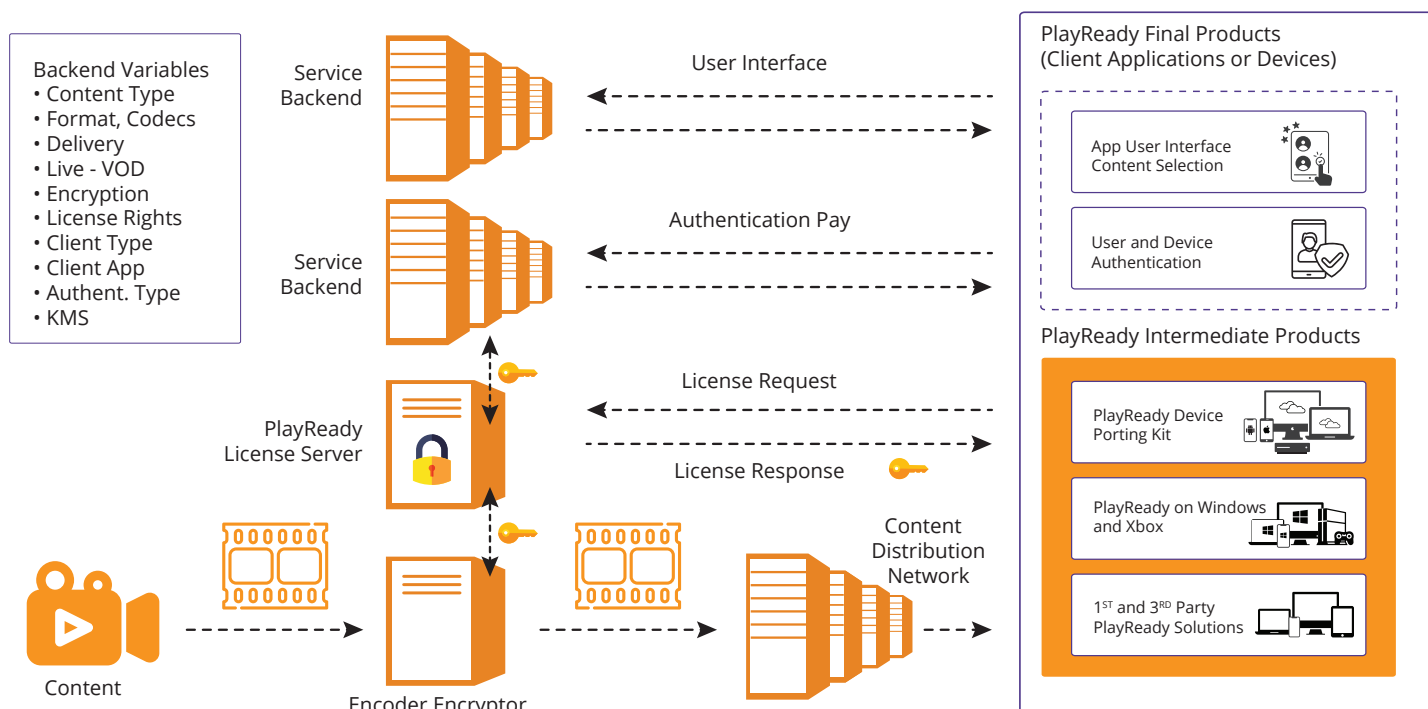
PlayReady was the successor to Windows Media DRM (WMDRM), which was built into Microsoft's Windows Media platform, and provided backward compatibility with WMDRM 10. Windows Media DRM was completely replaced by PlayReady with the Windows 10 Anniversary Update in 2016. (Ref. #3)

FEATURES OF PLAYREADY BY VERSIONS (REF. #4)



PLAYREADY COMPONENTS AND HOW THEY WORK

PlayReady ecosystem consists of two main components: the client and the server. These components communicate using protocols specified by Microsoft. (Ref. #5)



- ▶ Content is encrypted by a content packager that supports PlayReady, and then sent to clients that decrypt and play content using information stored in the DRM license
- ▶ A PlayReady client is a device that can play protected content when licensed for that content. It can be a media player on personal computers or an application on devices such as mobile phones, tablets, and smart TVs. The PlayReady client enforces the rights and restrictions associated with the policies contained in the license when playing the DRM content.
- ▶ A PlayReady server enables the integration with clients. Content service providers or DRM solution vendors use the PlayReady Server Software Development Kit (SDK) to build servers that support service-specific business logic.

For more information, please refer to the [PlayReady online documentation](#).

FEATURES AND BENEFITS

High Compatibility and Support for Various Devices

Microsoft PlayReady is a massively distributed content protection technology worldwide. PlayReady runs on a wide variety of devices, apps and operating systems. PlayReady is used by thousands of services and more than 4 billion devices worldwide.

PlayReady is embedded in the latest Windows OS and can support PlayReady protected contents in PC application and Edge/IE11 browser. Most smart TVs and OTT devices also support PlayReady DRM.

HARDWARE-BASED ENHANCED CONTENT SECURITY

The media industry recognized the need for improved content security when introducing the higher resolution content beyond HD and the early window movie content concept. PlayReady uses hardware-based DRM technology and is trusted by studios and content owners.

Implementing the client with the latest version of the PlayReady Porting Kit on devices that support the Trusted Execution Environment (TEE) can meet hardware security requirements for Enhanced Content Protection.

PlayReady-enabled devices, such as Xbox One or Windows 10 PC in certain hardware environments, are able to play premium content such as Netflix UHO content with hardware-based enhanced content security. (Ref. #6)

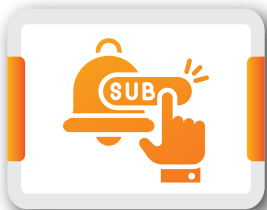
USE CASES

PlayReady is applicable to a variety of service scenarios such as:



Rental

For rental content, the license provided for the content specifies the expiration date and time. After this date and time, the content may still be on the user's device and the license may still be maintained in the user device's data store, but the PlayReady client of the user's device may use the device's secure time to expire the license.



Subscription

Microsoft PlayReady supports scenarios in which content providers use online media storage to sell subscriptions to music or video catalogs. The PlayReady Server does not include business logic, but it can connect to the business logic backend via the Web API, so you can specify the expiration time for PlayReady licenses for subscription content the same as the rental content. Clients request individual licenses for each piece of content they play, and content services may also provide multiple licenses in a single license response for optimization.

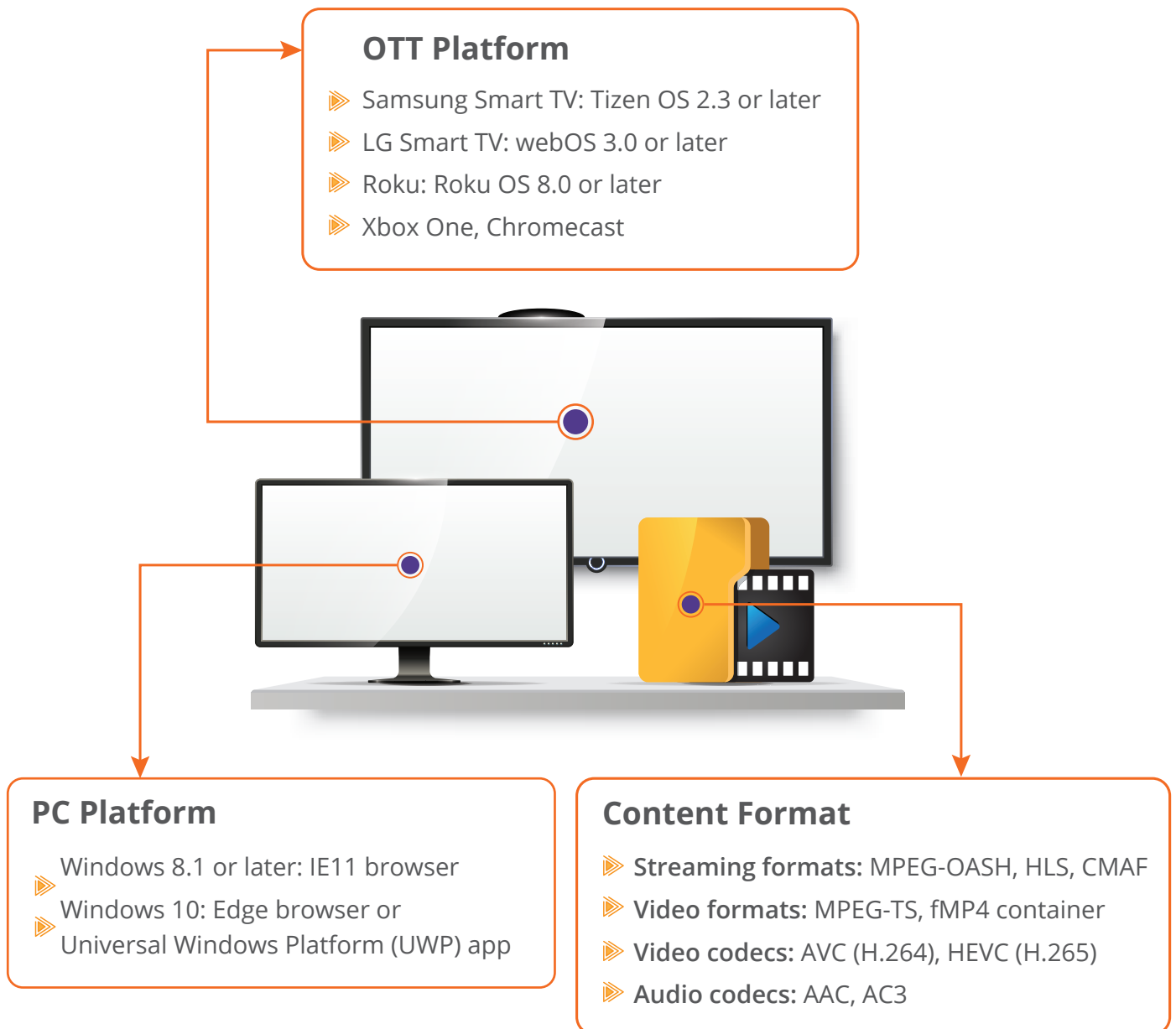


Purchase & Download

In a content purchase scenario, content providers use the online media store to sell media to consumers. Users expect their purchased content to play indefinitely on their device, and content services often issue licenses for content without setting an expiration time. However, if the user changes the device or the PlayReady ID of the device is changed, content providers need to reissue licenses for that content for users or devices.

SUPPORTED PLATFORMS AND CONTENT FORMATS

PlayReady DRM supports the following platforms and content formats:



“

When using PlayReady alone, it can also support other content formats such as Smooth Streaming, WMV/WMA. However, for Multi-DRM applications, it is recommended to support the most compatible format considering client support and Widevine content integration.

”

PART 2 – GOOGLE WIDEVINE DRM



WHAT IS WIDEVINE

Widevine DRM is Google's content protection system for premium media. Widevine is used by major content services around the world, including Google Play, YouTube, Netflix, Hulu, Amazon, and more. Widevine is embedded in web browsers such as Chrome and Firefox, and devices with Android OS and other various OTT devices.

HISTORY OF WIDEVINE

Widevine DRM was developed by Widevine Technologies to replace smartcard-based content security technologies. Since Google acquired Widevine Technologies in 2010, Widevine has been built into Google's various platforms, including Chrome, Android Mobile and Android TV. (Ref. #7)

WIDEVINE VERSIONS

WIDEVINE CLASSIC (V1~V6)

Widevine Classic was supported by older version of Android (3.7 ~ 5.7) and older smart TVs. It is no longer available for new services or devices because Google stopped the support. Widevine Classic uses WVM file format, which is a proprietary packaging format.

WIDEVINE MODULAR

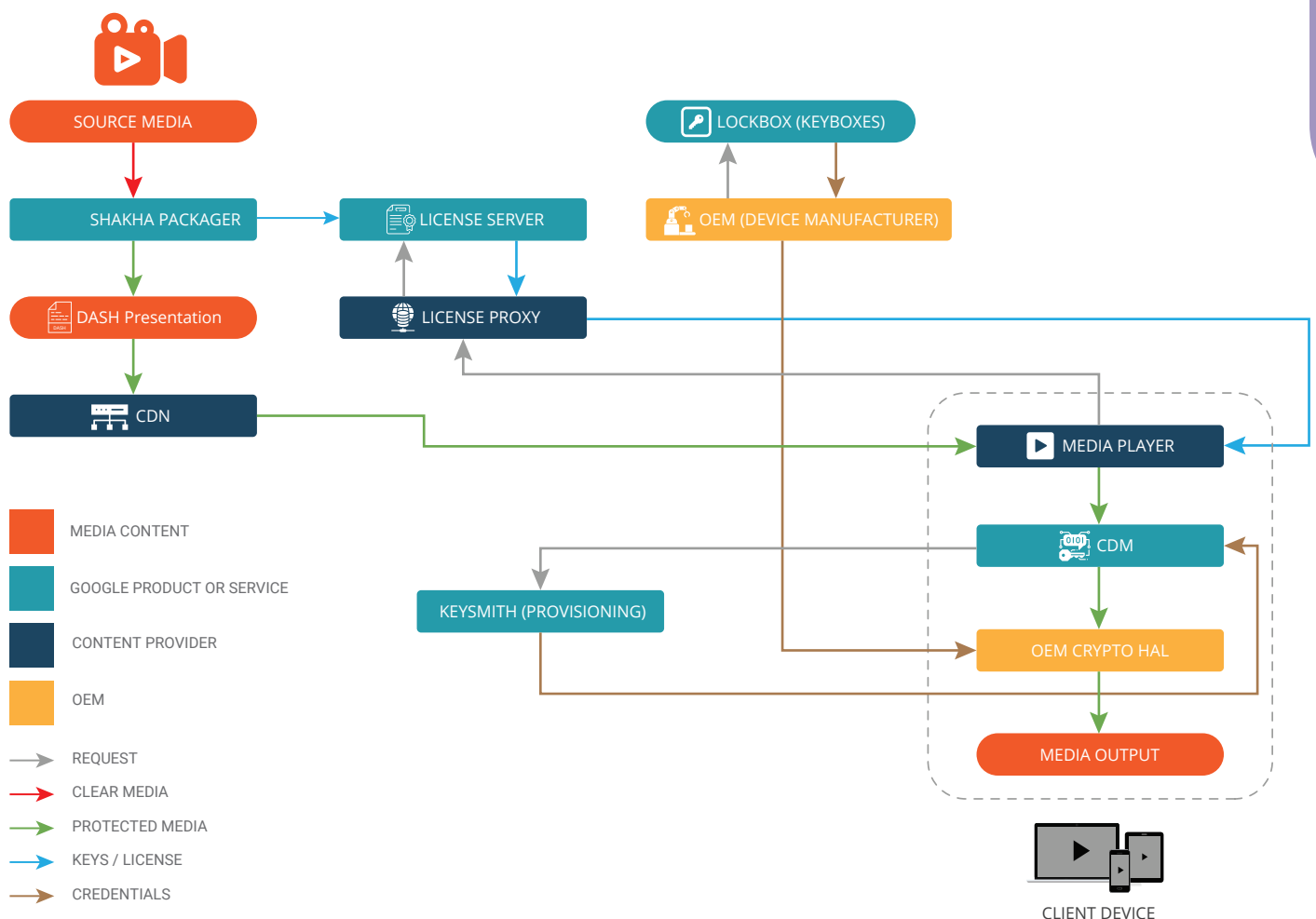
It is current Widevine DRM which is developed with new specifications and features. Widevine Modular supports adaptive streaming formats such as DASH/HLS as well as HTML5 standards (EME/MSE). The term 'Widevine' is now commonly used to refer to the Widevine Modular version.

Widevine Modular manages individual versions of each component instead of the version of DRM itself.

WIDEVINE COMPONENTS AND HOW THEY WORK

The Widevine DRM ecosystem consists of Widevine cloud licensing services, licensed proxy servers, and client devices supporting Widevine.

Widevine Cloud Licensing Service is operated directly by Google, and it generates and delivers DRM licenses upon request from a license proxy server in a content service or DRM solution. Access to cloud licensing services is only allowed through organization-specific credentials.



The **license proxy server** handles user authentication and authorization for DRM license requests from client devices and delivers licenses issued from the Widevine cloud licensing service to clients.

Client devices include Android mobile, TV, set-top box, Chrome, and Firefox browser. To manufacture Widevine client devices, a separate contract with Widevine is needed to get the key box and CDM module and test the integration.



In order to establish a license proxy server and provide Widevine licenses for content services, 3rd party solution providers must complete and qualify for Widevine's Certified Widevine Implementation Partner (CWIP) program. DoveRunner is an official Widevine partner with CWIP qualification.



FEATURES AND BENEFITS



CONTENT PROTECTION

Widevine DRM supports a wide range of client devices and works synergistically with multiple content protection systems such as Multi-DRM.



VIDEO PLAYBACK SUPPORT

Widevine comes with an HTML5 player that supports adaptive streaming, QoS, and accessibility features across a variety of devices. Shaka Player, an open source web player developed by Google, supports DASH and HLS streaming and can play Multi-DRM content in most web browsers and mobile devices.



STANDARDIZED FORMAT

With the support for industry-recognized media containers such as ISO BMFF (MP4) and WebM, single encrypted content can be played anywhere.



DEVICE SECURITY

Content services can utilize powerful device security by applying hardware-based root of trust, decryption, and content rendering with factory provisioned key boxes.



Widevine DRM applied to Android or OTT devices can support hardware-based content security (Widevine L1) depending on the model. However, PC browsers such as Chrome and Firefox support a software-based (Widevine L3) DRM which is vulnerable to screen recording.



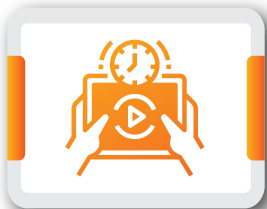
USE CASES

When issuing a DRM license to a Widevine client, Widevine license server can set the following rules for the duration of content playback (Ref #8)



LICENSE DURATION

The validity period of the license. It is about 'How long you can play content with the license' (play time). Common rule for all of the below scenarios.



PLAYBACK DURATION

The period of time that the license is valid since the initial playback of the content (when the license was first used). Only used in office scenario or license renewal scenario.



RENTAL DURATION

The period of time that the license is valid before the initial playback of the content. Used only in offline scenarios.

These licensing settings allow service providers to implement a variety of scenarios, including:

▶▶ BASIC STREAMING SCENARIO

In streaming scenarios, the playback device is always considered to be connected to the internet, and you can set the 'License Duration' to limit the duration of playback.

▶▶ LICENSE RENEWAL SCENARIO

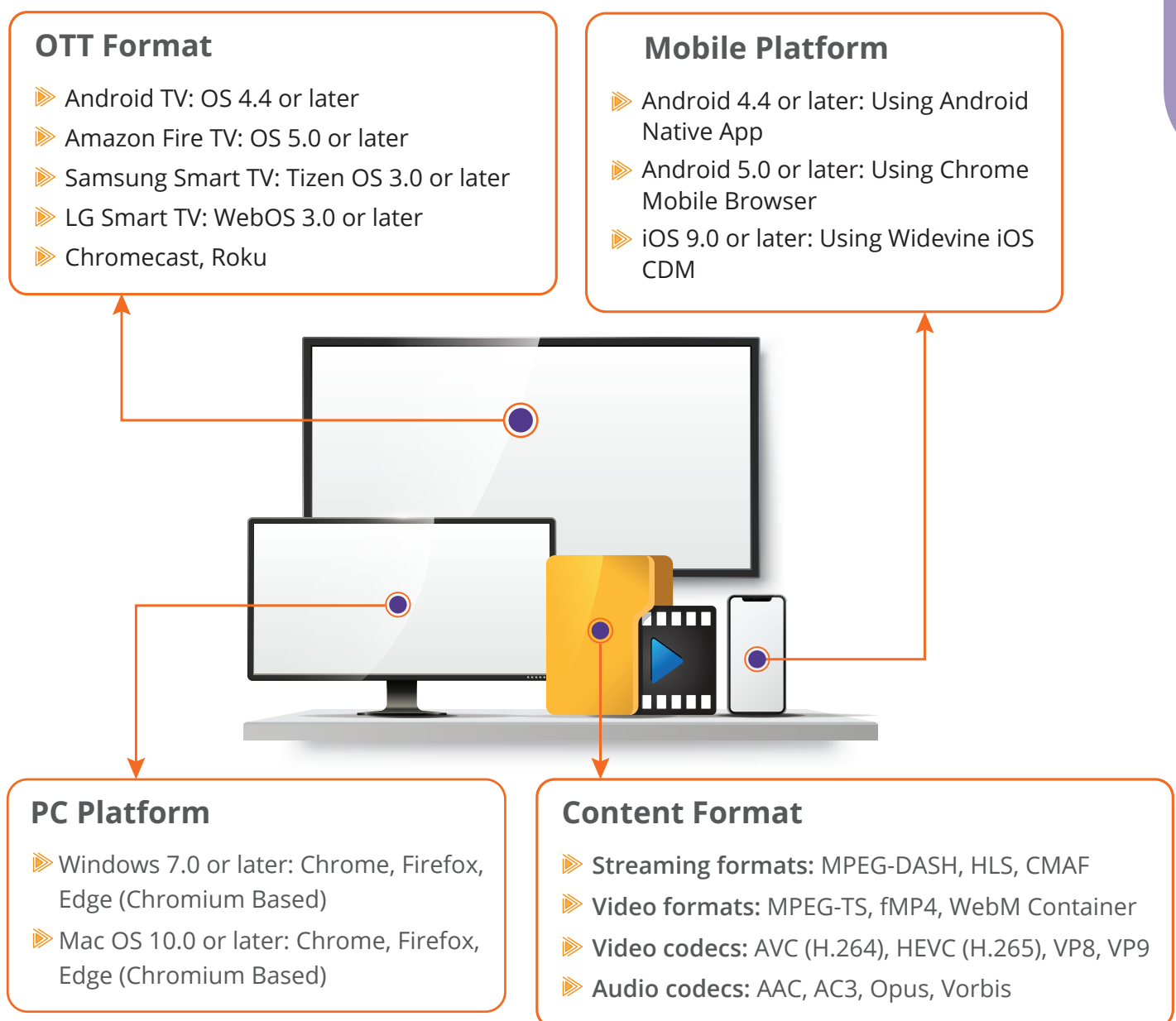
To support live (linear) content or simultaneous playback limits, you can periodically renew your license through the License Renewal feature while playing content in streaming. If you set the total playable duration to 'Playback Duration' and set the 'Renewal Delay' value to a shorter period, the license renewal is performed at that interval. (E.g. Playback Duration 180 minutes, Renewal Delay 15 minutes -> Reissue license every 15 minutes, up to 3 hours of content playback).

▶ OFFLINE (RENTAL) SCENARIO

For offline playback of downloaded content, the 'Rental Duration' and 'Playback Duration' settings allow you to specify 'How long you can keep the downloaded content' and 'How long you can play the content' separately. (E.g. Rental Duration 30 days, Playback Duration 3 hours-> watch within 30 days after download, up to 3 hours after playback starts)

SUPPORTED PLATFORMS AND CONTENT FORMATS

Widevine DRM supports the following platforms and content formats:



PART 3 – APPLE FAIRPLAY DRM



WHAT IS FAIRPLAY

FairPlay is Apple's Digital Rights Management (DRM) specification. FairPlay DRM has been used exclusively by Apple for its iTunes media service. Since FairPlay Streaming was announced in 2015, other media services can also apply FairPlay DRM to content delivered to Apple devices. (Ref. #9)

This White Paper mainly discusses about FairPlay Streaming Technology.

Apple's FairPlay Streaming (FPS) DRM is a technology that securely delivers streaming media to client devices through HTTP live streaming protocol. FPS technology enables content providers, encoding vendors, and content delivery networks (CDNs) to encrypt content, securely exchange keys, and protect playback on iOS, tvOS, macOS, and iOS Safari browsers. (Ref. #10)

HISTORY OF FAIRPLAY

IPOD AND ITUNES

FairPlay DRM was developed by Apple based on Veridisc technology. (Ref. #11) In the early 2000s, when Apple launched its iPod MP3 player and iTunes music service, FairPlay DRM was used to protect the music content of iTunes Store from illegal use. However, it caused 'DRM compatibility issue' that users could use purchased music only on Apple devices.

WHAT IS FAIRPLAY

FairPlay is Apple's Digital Rights Management (DRM) specification. FairPlay DRM has been used exclusively by Apple for its iTunes media service. Since FairPlay Streaming was announced in 2015, other media services can also apply FairPlay DRM to content delivered to Apple devices. (Ref. #9)

This White Paper mainly discusses about FairPlay Streaming technology.

Apple's FairPlay Streaming (FPS) DRM is a technology that securely delivers streaming media to client devices through HTTP live streaming protocol.



FPS technology enables content providers, encoding vendors, and content delivery networks (CDNs) to encrypt content, securely exchange keys, and protect playback on iOS, tvOS, macOS, and iOS Safari browsers. (Ref. #10)



'DRM FREE' BY STEVE JOBS

In February 2007, Apple's CEO Steve Jobs wrote an email titled 'Thoughts on Music'. He declared that Apple would no longer apply DRM to its iTunes content to address the 'DRM compatibility issue'. Since then, major record companies have agreed to remove DRM from all music content on the iTunes Store since 2009. (Ref. #12)

REVIVAL OF FAIRPLAY DRM AND FPS ANNOUNCEMENT

Even after Steve Jobs' 'DRM FREE' declaration, FairPlay DRM continued to be applied to movie content available on iTunes Store. And the issue of 'DRM compatibility' of music content has become less significant since subscription-based streaming services became a major trend for music content.

FairPlay Streaming was announced at WWDC event in 2015. Whereas FairPlay DRM was a closed technology exclusively applied to iTunes service, Apple released FPS integration specifications, allowing other content services to use it.

FAIRPLAY COMPONENTS AND HOW THEY WORK

FPS DRM consists of the following components: (Ref. #13)

KEY SERVER AND KEY SECURITY MODULE (KSM)

Key server manages the keys used for encrypting / decrypting DRM content. DRM solution or content service provider can implement a Key Security Module for FPS on their own key server by referring to the KSM sample provided by Apple.



KSM validates the key request data sent from the client and securely passes the requested content key.



CLIENT APPLICATION

The FPS client app runs on Apple devices' OS such as iOS, tvOS, and macOS. It requests the key for FPS content to the key server and processes the response. Content service providers can use Apple's sample code to develop their own FPS client app or use a FPS SDK provided by DRM solution provider.

FPS CONTENT

To apply FPS to HLS content, each HLS segment must be encrypted by SAMPLE-AES method. The encryption method used for FPS content is AES-128 CBCS. Using packages or solutions that support FPS packaging, such as Shaka Packager, the KEY tag can be added to the m3u8 playlist of encrypted HLS content with related information.

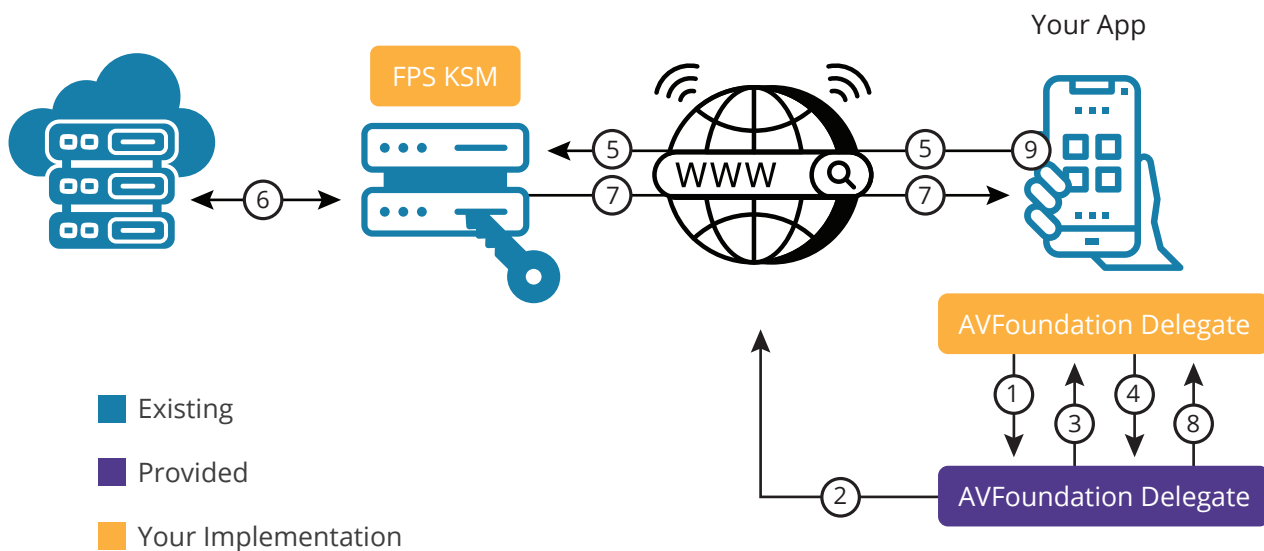


Cipher-block chaining (CBC) is an encryption method that uses the encryption result of the previous block as the IV (Initial Vector) of the next block. The AES-CBCS method encrypts only a few sub-samples in CBC instead of the entire data of the content. (Ref. #14)



FPS KEY REQUEST PROCESS

The FPS key request and response from the iOS / tvOS client app is as follows:



1. Client app notifies the OS's AVFoundation framework to play FPS content
2. AVFoundation downloads HLS playlist (m3u8) from content server and checks KEY tag
3. AVFoundation requests the key of the content from the client app (AVFoundation Delegate)
4. App Delegate requests Server Playback Context (SPC) data from AVFoundation
5. App Delegate sends generated FPS SPC data to key server
6. Key server interprets SPC data through KSM module and retrieves key required for content playback from key DB
7. The key server sends the retrieved content key to the client app in the form of Content Key Context (CKC) data
8. AVFoundation Delegate in Client app enters CKC data into AVFoundation
9. AVFoundation decrypts and plays content securely using keys contained in CKC data



In Mac OS and iOS Safari, content key transfer and playback is similar to the above process. In this case, the Content Decryption Module (CDM) and Encrypted Media Extension (EME) standards built into the Safari browser are used instead of the implementation in the client app.



FEATURES AND BENEFITS

▶▶ **HARDWARE DRM SUPPORT**

All client environments that support FPS DRM, such as Mac OS, iOS, and tvOS, are highly secure at the hardware level. Widevine DRM can also be applied to Apple devices via the Chrome browser for Mac OS or the Widevine CDM SDK for iOS, but that is not suitable for premium content security because hardware DRM is not available.

FPS DRM is a must for content that requires a high level of security, such as the early-window movies from Hollywood studios.

▶▶ **APPLE AIRPLAY SUPPORT**

FPS DRM natively supports Airplay, Apple's wireless content delivery protocol. FPS content on Apple devices can be played on Apple TV through AirPlay without any additional coding.

Key delivery and decryption of FPS content played through Airplay is performed on Apple TV, the target device, with the same level of security as playing on the original device such as iPhone.

▶▶ **DOWNLOAD AND OFFLINE PLAYBACK**

Starting with iOS 10, download and offline playback of FPS content are supported. The relevant APIs provided by the OS can be used to handle downloading and managing HLS content with offline licenses.

“

If a content service provider adopts a Multi-DRM solution provided by a DRM solution vendor, it can use Widevine and PlayReady DRM directly without a separate application or registration process. However, FPS DRM requires content service providers to apply for and issue an FPS Deployment Package from Apple.

”

USE CASES

In addition to basic streaming scenarios, the following usage scenarios can be applied to FPS DRM content:



VIDEO RENTAL SCENARIO

If you use a content key set to the rental type, decryption for content playback will stop after that key's validity period. You can apply this scenario to contents purchased on a rental basis rather than for a permanent collection, making it available only for a certain period of time.

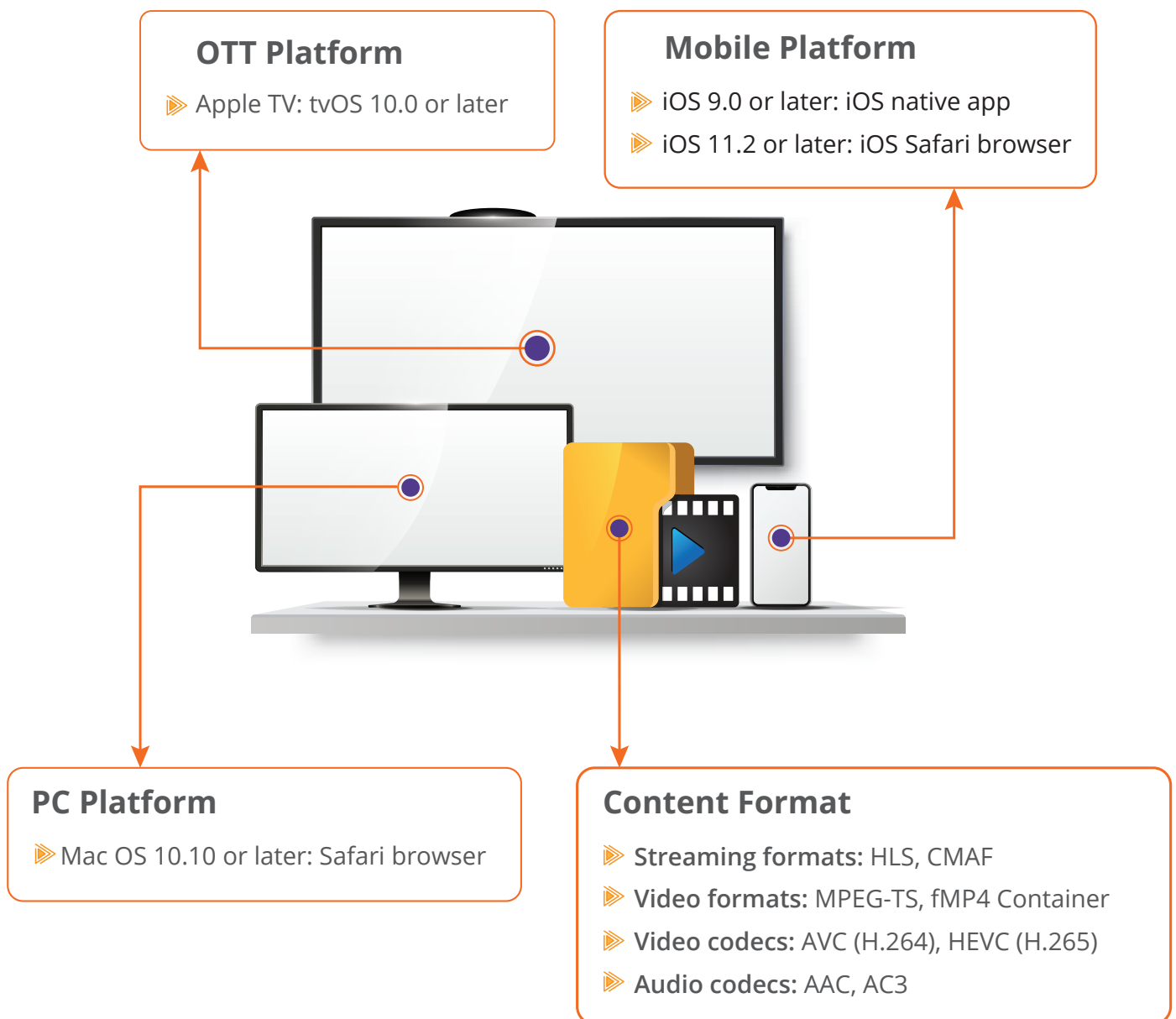


SECURE LEASE

By periodically renewing content keys set for the lease type during content playback, you can check and limit the number of client devices that can be played simultaneously with a single user account.

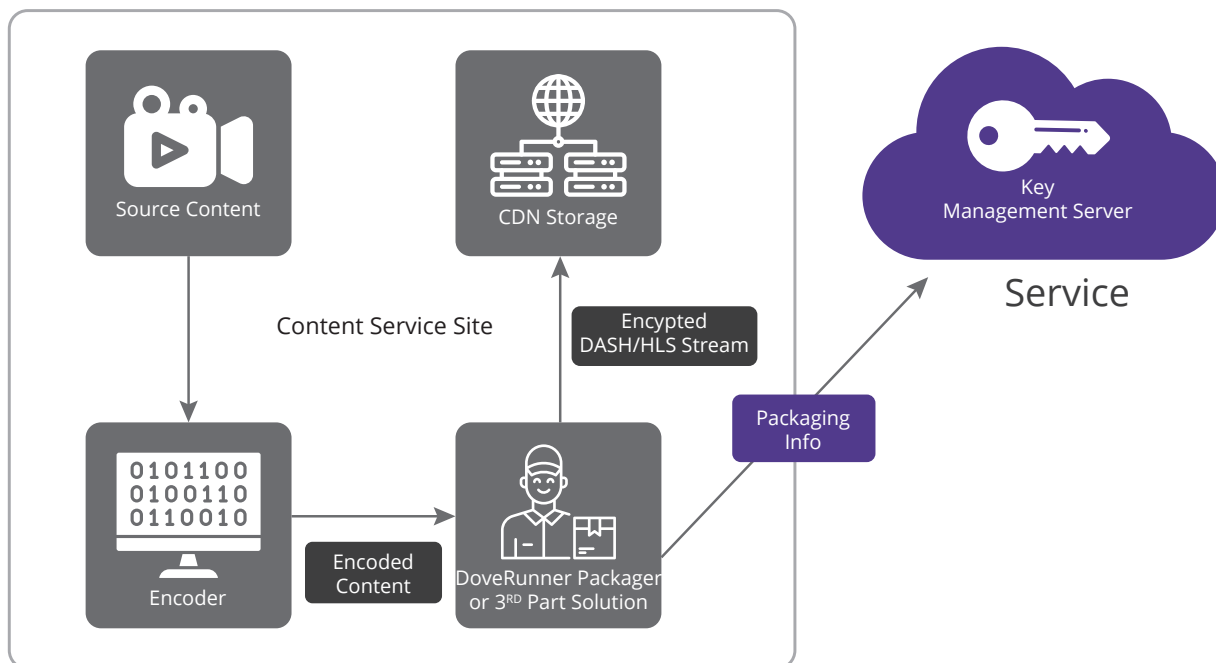
SUPPORTED PLATFORMS AND CONTENT FORMATS

FPS DRM supports the following platforms and content formats:



PART 4 – DRM PACKAGING AND CPIX/SPEKE API

To protect digital content with DRM, content data must be encrypted by default. The process of encrypting source content (such as MP4 video) and converting it into other format (such as DASH or HLS stream data) that will be delivered to end users is known as 'DRM content packaging'. During packaging, the key used to encrypt the content is passed to the DRM license server for safe management, as shown below.



“Among other encryption algorithms, the Advanced Encryption Standard (AES) is the standard for encrypting multimedia content. It mainly uses AES-128, which encrypts with a 128-bit key, and block encryption mode of CTR or CBC is used depending on the client environment. (Ref #15, Ref #16)”

DRM content is delivered (streaming or download) to end-user device in encrypted form. To play the content, the client requires a DRM license with the encryption key which is issued from a DRM license server. Please refer to part 5 for more information on the client-side DRM license integration.



In order to establish a license proxy server and provide Widevine licenses for content services, 3rd party solution providers must complete and qualify for Widevine's Certified Widevine Implementation Partner (CWIP) program. DoveRunner is an official Widevine partner with CWIP qualification.



OUTPUT OF MULTI DRM PACKAGING

The multi-DRM content generated by the packaging process is divided into two types according to the streaming format and encryption method as follows.

MPEG - CENC CONTENT

DASH content encrypted with AES-128 according to the Common Encryption specification and protected with PlayReady and Widevine DRM.

FAIRPLAY STREAMING (FPS) CONTENT

HTTP Live Streaming (HLS) content that is encrypted with SAMPLE AES and protected by FairPlay Streaming DRM.

The following client environments support each content type.

DASH (MPEG - CENC) CONTENTS

Web browsers such as Edge, IE11, Chrome, Firefox, and other devices that support PlayReady or Widevine DRM (Smart TV, Set-Top Box, OTT devices, etc.)

HLS (FPS) CONTENT

Apple devices that support FairPlay Streaming DRM, including Mac/iOS/iPadOS Safari and iOS/iPadOS/tvOS apps.

To support playback on as many clients as possible, including Apple devices, one content must be packaged and delivered in both DASH and HLS.

The **Common Media Application Format (CMAF)** is an upcoming standard to support all devices with a single piece of content to improve storage and CDN costs and inefficiencies due to this duplicated content (Ref. #17).

VARIOUS DRM PACKAGING METHODS

DRM content packaging can be done in a variety of ways:



DRM PACKAGING TOOLS

A separate tool for encrypting content can be used to package source content (e.g. mp4 file). It runs on a content service provider's system (cloud or on-premises).

The following tools are commonly used:

» **Shaka Packager:**

Open source based media packaging tool developed by Google Widevine team. Supports multi-DRM packaging of DASH / HLS content, Video On Demand (VOD) and live content packaging.

» **Bento4:**

Similarly, an open source C++ library that provides a variety of multimedia related features, including the packaging of DASH / HLS content.

» **Dedicated packaging tools** from DRM vendors: Professional DRM solution providers such as DoveRunner provide customers with dedicated DRM packaging tools to help them get up and running quickly and easily.



INTEGRATION OF ENCODING/STREAMING SOLUTIONS

DRM packaging can be integrated into commercial encoding or streaming solutions. DoveRunner Multi DRM works with the following solutions. (Ref. #18)

» **Wowza:**

Multi-DRM packaging is handled as a plug-in to the Wowza Streaming Engine, which handles DASH / HLS packaging in real time.

» **Harmonic:**

Allows multi-DRM packaging to work with encoders / transcoder products and Harmonic Key.



CPIX API

The above method adds the encryption key exchange functions for various DRM companies in each solution such as Wowza and Harmonic.

This requires duplicated development work from solution vendors. To reduce this duplication and complexity, the DASH industry forum has released a standard guide called Common Protection Information Exchange Format (CPIX).

The CPIX API defines a standard for interfacing encryption keys required to apply multi-DRM in the packaging of media content. DoveRunner integrated the following solutions with the CPIX API to enable easy and fast adoption of DRM packaging.

» **Anevia:**

Included in Anevia's Cloud DVR solution, it supports real-time packaging of VOD and Catch-up TV content.

» **Flussonic Media Server:**

A server software that enables you to build online video services for multi-device clients, from video capture, transcoding, recording, security, and delivery.



For more information about the CPIX APIs support ed by DoveRunner Multi-DRM service, please refer to the online guide document.



SPEKE API

The Secure Packager and Encoder Key Exchange (SPEKE) API is an encryption key exchange API announced by AWS. It provides additional features based on the CPIX specification.

Through the SPEKE API, various DRM solutions can be easily integrated into the following AWS services and products.

» **AWS ELEMENTAL MEDIA CONVERT:**

Transcoding service for VOD on the AWS Cloud.

» **AWS ELEMENTAL MEDIA PACKAGE:**

Packaging service for live streaming on the AWS Cloud.

» **AWS ELEMENTAL LIVE:**

On-premise product for live video encoding.

» **AWS ELEMENTAL DELTA:**

On-premise product for live/VOD packaging.

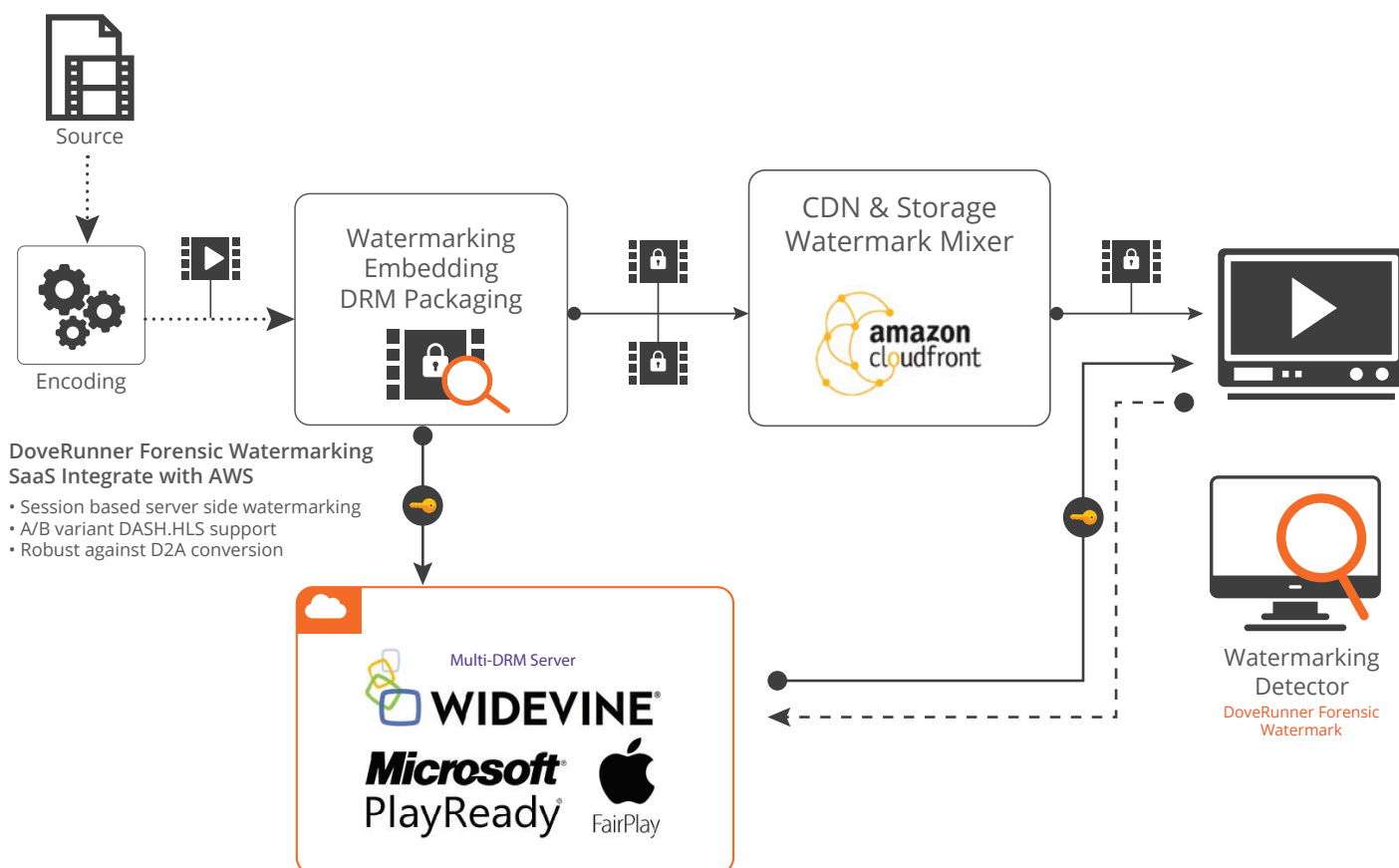


USING A CLOUD-BASED SERVICE

In addition to the methods we've seen so far, you can use a service that handles DRM packaging of the source content on a SaaS (Solution as a Service) basis.

DoveRunner service provides cloud SaaS-based packaging service for contents that simultaneously apply forensic watermarking and multi-DRM.

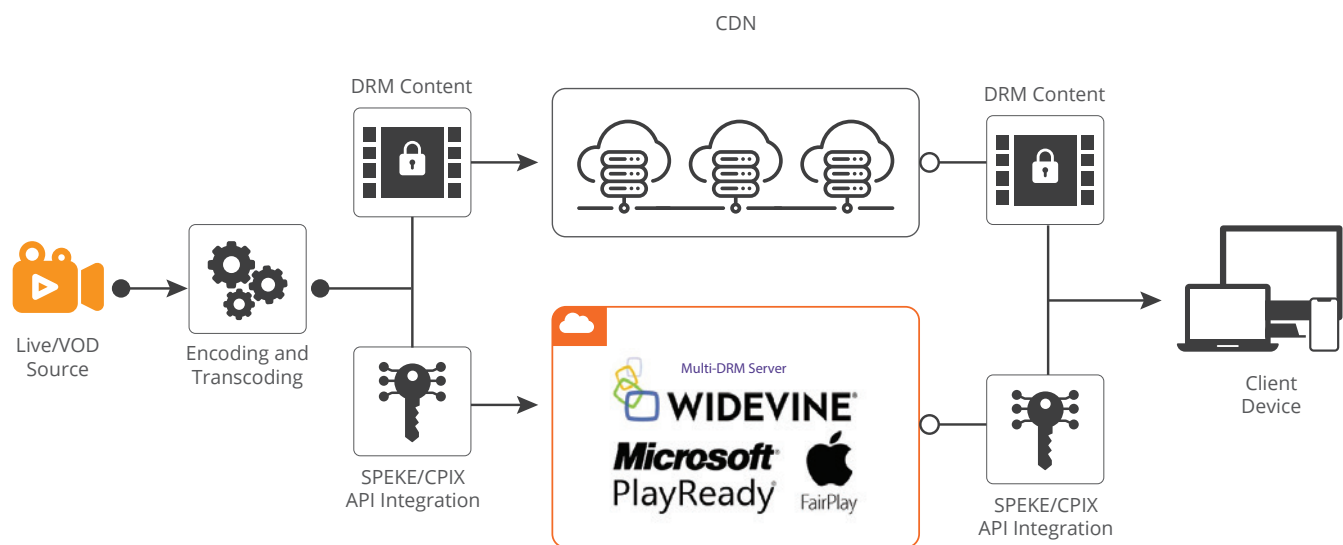
Instead of the complex watermark embedding and DRM packaging process, you can simply register the cloud storage where the original video is uploaded. The packaging service automatically generate DASH / HLS content with multi-DRM and forensic watermarking. (Ref. #19)



PART 5 – MULTI-DRM CLIENT INTEGRATION

PLAYBACK PROCESS OF DRM CONTENT

After the DRM packaging process described in the part 4, encrypted DRM content is delivered via CDN to the end user's device. To decrypt and play the content delivered to the client device by streaming or download method, the client needs to obtain a DRM license from the server as shown below.



“

The DRM license consists of the key used for encryption when packaging the content and the usage rights information for that content (playback period, online playability, security level, etc.). To ensure that the key value used to decrypt content is not compromised and the usage rights are not tampered, the DRM license data is also encrypted and protected with a client device's unique key.

”

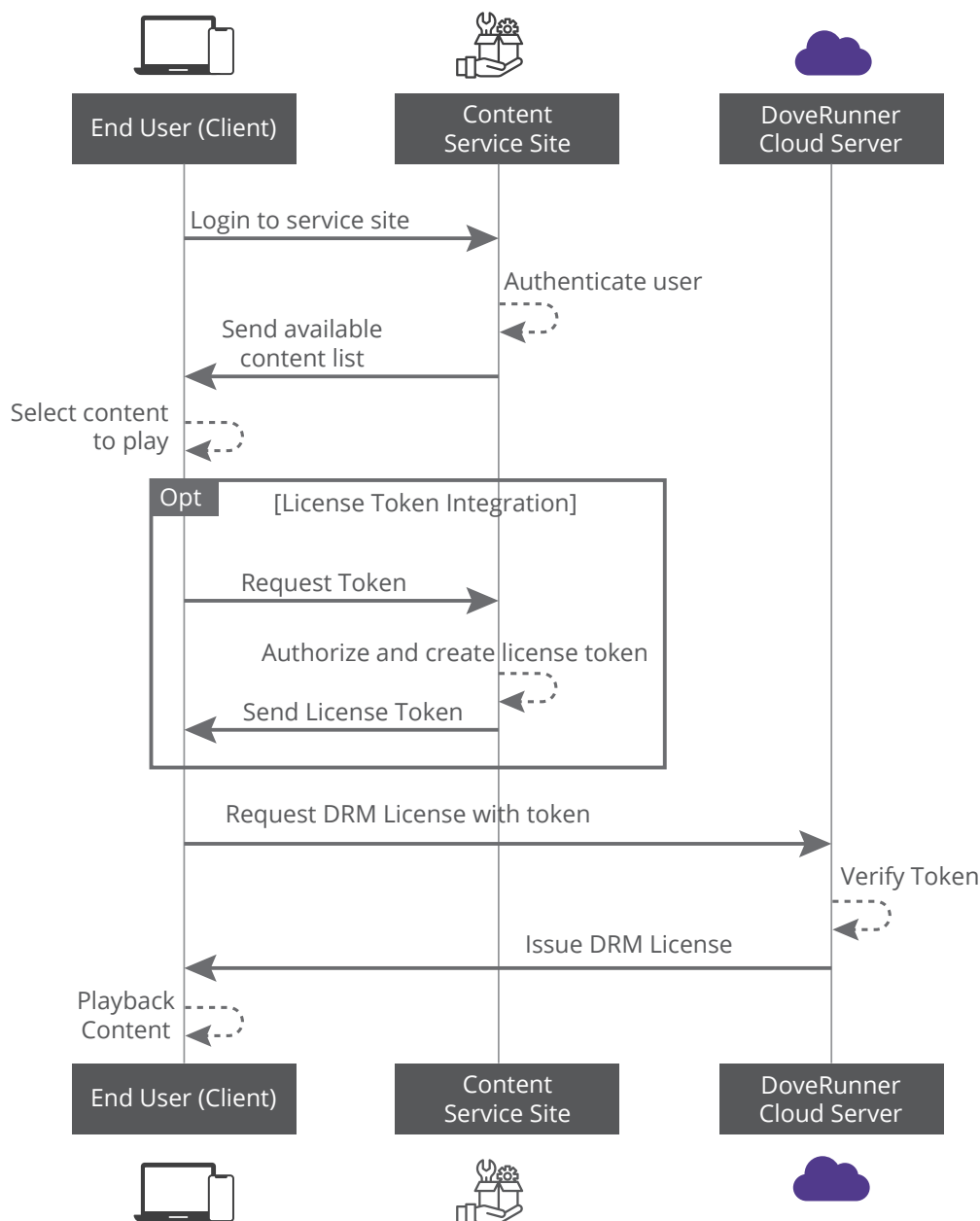
DRM LICENSE INTEGRATION METHOD

Before the DRM license server can process license requests from client devices, you must first ensure that the user has permission to use the content. To this end, most DRM solutions / services support integration methods with the system of content services as below.

► INTEGRATION WITH LICENSE TOKEN

A method of issuing DRM licenses through tokens generated by the back-end system of the content service according to predefined rules.

Token-based license issuance is performed as follows:



The advantage of the token method over the callback method described below is that communication between the content service system and the DRM server is not required, which reduces the delay in starting content playback.

Instead, the initial integration requires more resources because the content service operators must implement the functions to generate tokens and pass them securely to clients.



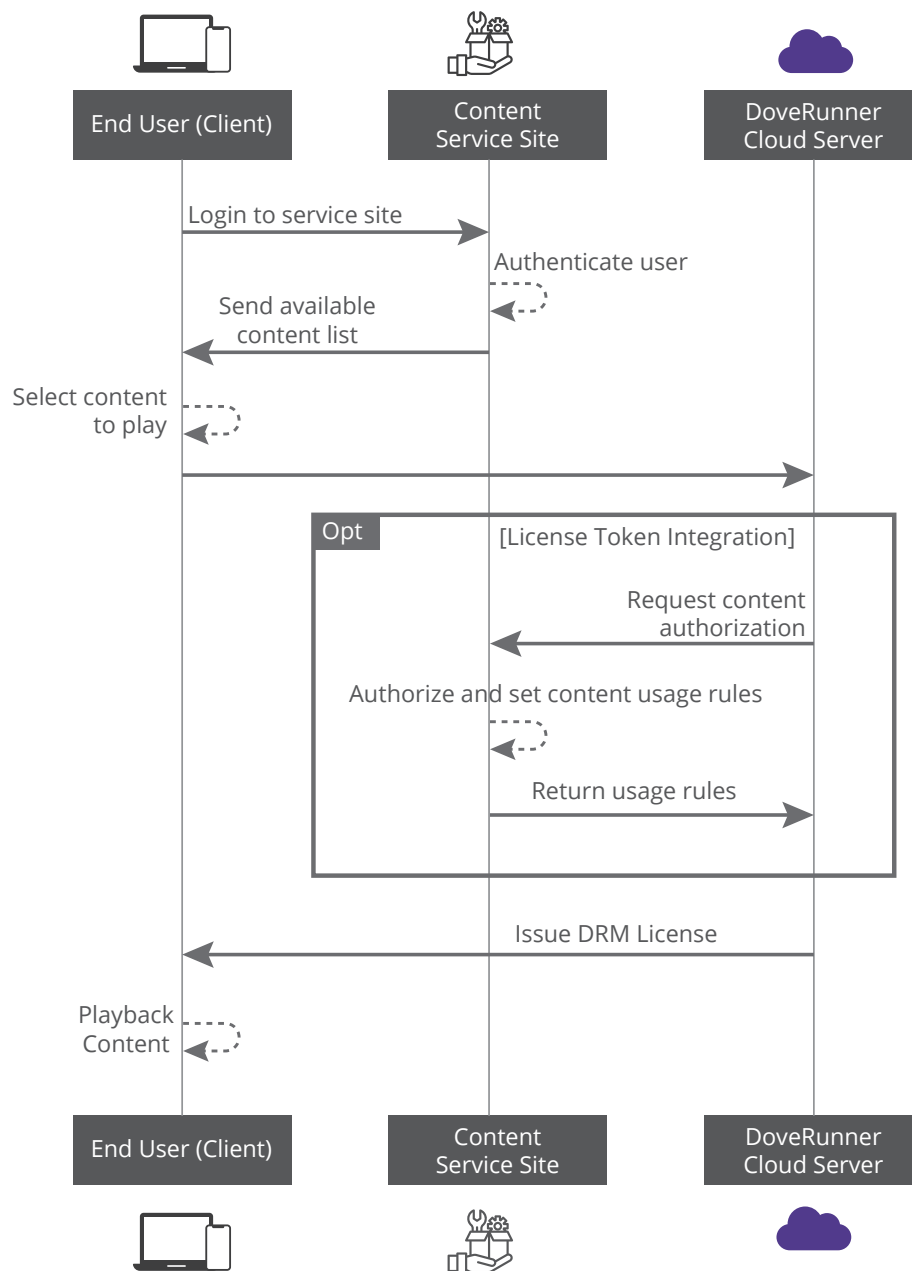
In the case of a large number of requests in a short time or a global service, we recommend using token-based license integration to maximize license issuance performance and minimize latency.



INTEGRATION THROUGH CALLBACK URL

In callback type license integration, the DRM license server verifies the user's rights to use the content through HTTPS URL communication with the content service's system when a license request is received from a client.

Callback license integration is as follows.



The callback method has a longer playback start delay due to communication between systems than the token method, and thus has a disadvantage in the simultaneous processing when a large number of license requests are concentrated in a short time.

However, it can be tested relatively easily compared to the token method during the initial integration process. And it has the advantage of reducing the burden of safe management of token data by content service operator.

MULTI-DRM CONTENT PLAYBACK BY CLIENT TYPE

Most OTT content operators provide services to a variety of client devices to support as many users as possible. Multi-DRM solution / service providers support multiple platforms and devices in the following ways to meet these requirements.

Apple's FairPlay Streaming (FPS) DRM is a technology that securely delivers streaming media to client devices through HTTP live streaming protocol.



HTML5 WEB PL AYER INTEGRATION

Web browsers that support HTML5's Encrypted Media Extension (EME) standard can play multi-DRM content through the Content Decryption Module (CDM) provided by each OS and browser. (Ref. #20)

Open source HTML5 players, such as Shaka Player and VideoJS, and most commercial players, such as Bitmovin and THEOplayer, provide the APIs needed to integrate multi-DRM licenses.

You can configure DRM-supported HTML5 players with a DRM license URL and license request data (CustomData) as well as the URL of DRM content (DASH .mpd or HLS .m3u8 address) to play.

“

The custom data used to request DRM license uses its own specifications for each DRM solution / service provider. For detailed guides and samples of DoveRunner Multi DRM's HTML5 web player integration, check out the DoveRunner online docu-

”

MOBILE WEB BROWSER INTEGRATION OR APP DEVELOPMENT

There are two ways to support DRM content playback in mobile environment such as Android and iOS.

USING A MOBILE WEB BROWSER

Plays in a mobile browser that supports multi DRM through the HTML5 player integration described above.

USING NATIVE MOBILE APPS

Content service provider can implement the integration directly by following the custom data specification, or apply mobile client SDKs provided by a multi DRM vendor.

PLAYBACK ON VARIOUS OTT DEVICES

In addition to PC web browsers and mobile devices, various OTT devices such as smart TVs, set-top boxes, and game consoles also support multi-DRM.

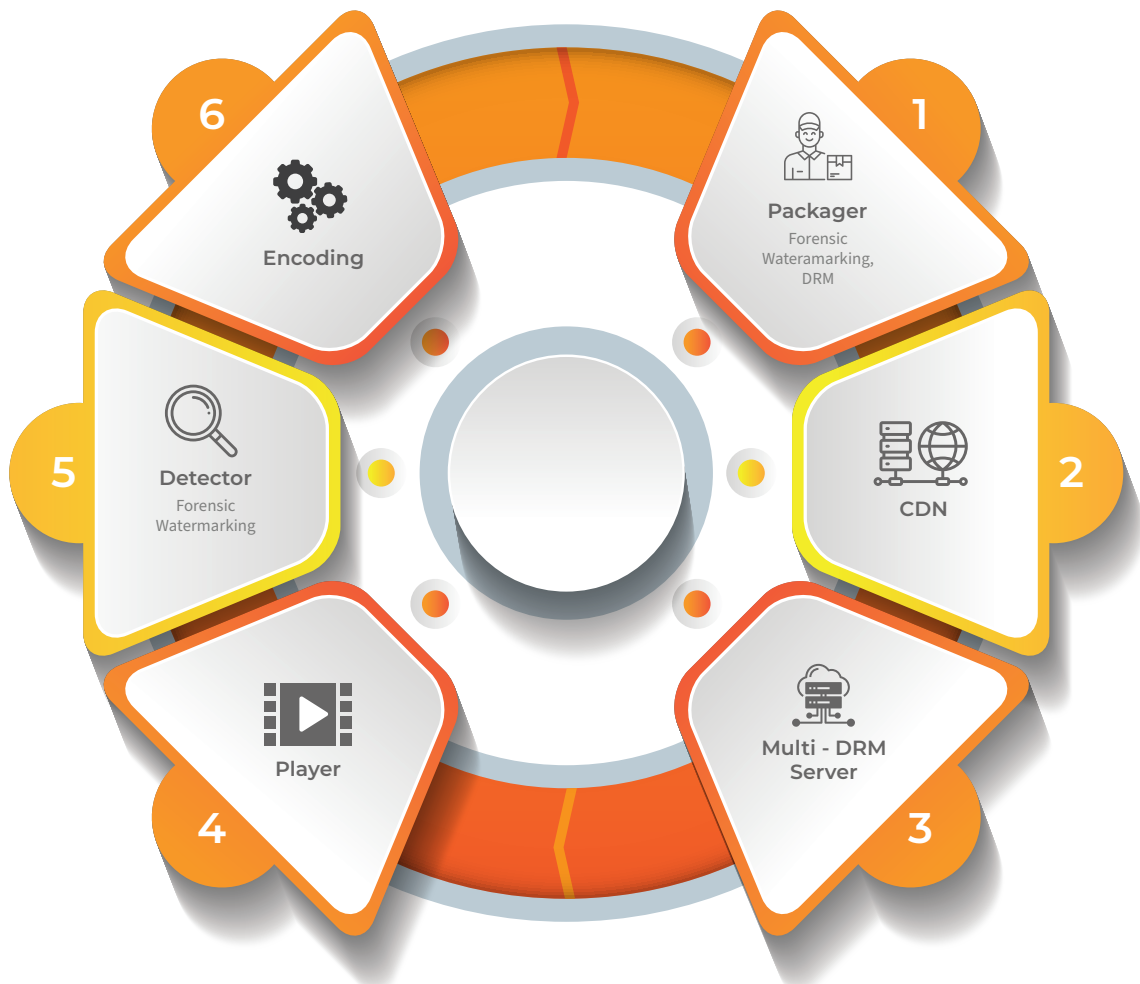
To service multi-DRM content on these OTT devices, you can use the device-embedded browser through the EME-based web player integration. Or you can develop native apps by applying multi-DRM SDKs for each OTT device. (Ref. #21)



CONCLUSION

As this white paper explained about the basics of multi-DRM technology. Multi-DRM is a complex technology that requires multiple technologies, standards, and various solutions to work with.

To apply this complex multi-DRM technology quickly and easily, it is recommended to use a multi-DRM company that integrates multiple DRM technologies to provide a unified API and works with various media related solutions such as encoders and players.



DoveRunner Multi DRM is a cloud-based, one-stop multi-DRM service provided by INKA Entworks, a content and application security technology company. We provide a variety of integration guides and APIs / SDKs to help our customers quickly and easily adapt multi DRM.

REFERENCES



- #1. <https://www.microsoft.com/playready/features/DigitalMediaStrategy.aspx>
- #2. <https://news.microsoft.com/2007/02/12/microsoft-announces-breakthrough-technology-enablingsimple-access-to-broad-set-of-digital-content-including-music-games-video-ring-tones-and-pictures/>
- #3. <https://support.microsoft.com/en-us/help/25975/windows-10-anniversary-update-loss-of-music-andvideo>
- #4. <https://docs.microsoft.com/en-us/playready/overview/product-versions>
- #5. <https://docs.microsoft.com/en-us/playready/overview/simple-end-to-end-system>
- #6. <https://docs.microsoft.com/en-us/windows/uwp/audio-video-camera/hardware-drm>
- #7. <https://googleblog.blogspot.com/2010/12/on-demand-is-in-demand-weve-agreed-to.html>
- #8. https://storage.googleapis.com/wvdocs/Widevine_DRM_Proxy_Integration.pdf
- #9. <https://developer.apple.com/videos/play/wwdc2015/502/>
- #10. <https://developer.apple.com/streaming/fps/>
- #11. <https://www.headendinfo.com/fairplay-drm/>
- #12. <https://en.wikipedia.org/wiki/FairPlay>
- #13. <https://developer.apple.com/videos/play/wwdc2015/502/>
- #14. <https://medium.com/@takusemba/hls-with-widevine-for-androidde3f41027ed2>
- #15. https://en.wikipedia.org/wiki/Advanced_Encryption_Standard
- #16. https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation
- #17. <https://DoveRunner.com/docs/en/multidrm/packaging/wowza-integration/>
- #18. <https://DoveRunner.com/blog/cmaf-the-quest-for-single-format-streaming/>
- #19. <https://DoveRunner.com/docs/en/watermarking/embedding/packaging-service/>
- #20. <https://www.html5rocks.com/en/tutorials/eme/basics/>
- #21. <https://DoveRunner.com/sdk/>

CONTACT

Headquarter / Korean Sales

 1F, 608, Nonhyeon-ro,
Gangnam-gu, Seoul, South Korea

 +82 2-538 -9058

 contact@doverunner.com

India Office / Overseas Sales

 Unit No. 916, 9th Floor, Building
No. A-1, Rupa Solitaire, Millennium
Business, Sector 1, Mahape, Navi
Mumbai – 400710

 +91 (22)-40146908

 contact@doverunner.com

&

 No 2, Awfis Space Solution Pvt Ltd,
A block, 2nd Floor, Dayananda
Sagar University, Kudlu Gate,
Hongasandra Village, Begur Hobli,
Hosur Road, Bangaluru,
Karnataka-560068

 +91 (22)-62785717

 contact@doverunner.com

USA Office / Overseas Sales

 3003 North First Street#322, San
jose, California 95134

 +213-550-5473

 contact@doverunner.com