GlobalLogic®

Digital Rights Management in the OTT Ecosystem

Authored by
Ajinkya Jawanjal

Contents

Introduction 1

What is Encryption? 2

- Is Encryption Enough?

What is DRM? 2

Content Packaging & Consumption 3

- Content Packaging
- Content Consumption

Leading DRM Systems 5

Encryption & Adaptive Streaming 6

CPIX 8

How Does Playback Work? 8

Multi-DRM Overview 9

Advancements in the DRM Market 10

- SPEKE
- CMAF

Conclusion 12

References 13

Introduction

This white paper focuses on the role of DRM in the OTT ecosystem. We will understand the workflow of DRM and understand how the protected content is delivered to an end-user.

Content delivered over the internet, known as over-the-top content (OTT), is becoming more popular than ever. Users are gravitating to online media consumption, and streaming platforms are witnessing a 100% increase in sign-ups. Sooner or later, OTT services will sideline traditional TVs and grab the lion's share of the media consumption market.

This is good news for streaming platforms, but there is also the potential for major revenue losses due to piracy. Recent research revealed that media platforms in the US alone lost $9.1B in 2019 and are expected to lose $12.5B by 2024. These figures are alarming, and may continue to rise at the rate at which this market is growing.

Rising demand has resulted in an increasing need for secure media access and management; It is crucial to restrict unauthorized access. One option is to have encryption in place, but encryption alone will not solve the problem. In the sections below, we will discuss why encryption is insufficient and explore end-to-end content solutions.

What is Encryption?

Encryption helps users protect data by scrambling text into an unreadable format. When a provider wants to sell encrypted content to a user, they need to provide an encryption key (to decrypt the content) along with the content.

Is Encryption Enough?

Encryption only works when the user holding the key is authorized to access the digital content - providing the key to anyone else negates the purpose of encryption - but it can't prevent users from copying a file and sharing the content with unauthorized users. Unauthorized users can then access premium content without paying a premium fee to the provider.

So, how can we distribute the key to the authorized user to access the content while at the same time protecting content from illegal access?

Apart from encryption, we need a system to manage the key (which is required to decrypt the content). Also, content owners or broadcasters want to apply specific rules and regulations to how the media is being consumed. This is where digital rights management (DRM) comes to the rescue and is one of the best solutions available to satisfy our requirements. In today's era, DRM is an integral part of the OTT ecosystem.

What is DRM?

DRM (Digital Right Management) is a systematic approach to the copyrighted protection of media content. It is a comprehensive system for managing online media content that provides protection from unauthorized access, securing the distribution, promotion, and sale of digital content.

DRM prevents consumers from copying content and converting it to other media formats and helps content owners enforce content access policies. These access policies are determined by the content owner and contain details on how the content is meant to be consumed.

Content Packaging & Consumption

Two major parts are required for an end-to-end solution: how the content is packaged before distribution and how the consumer consumes the content. An understanding of both processes helps to explain both encryption and decryption.

Content Packaging

Once content is created, the primary task is to encode and encrypt it before it is made available to the consumer.

1. The packager requests a key from the DRM.
2. The DRM returns a key, which it maintains at license servers.
3. The packager encodes and encrypts the content with the key.
4. The encrypted content is transferred to the storage or content delivery network (CDN) and available for users.

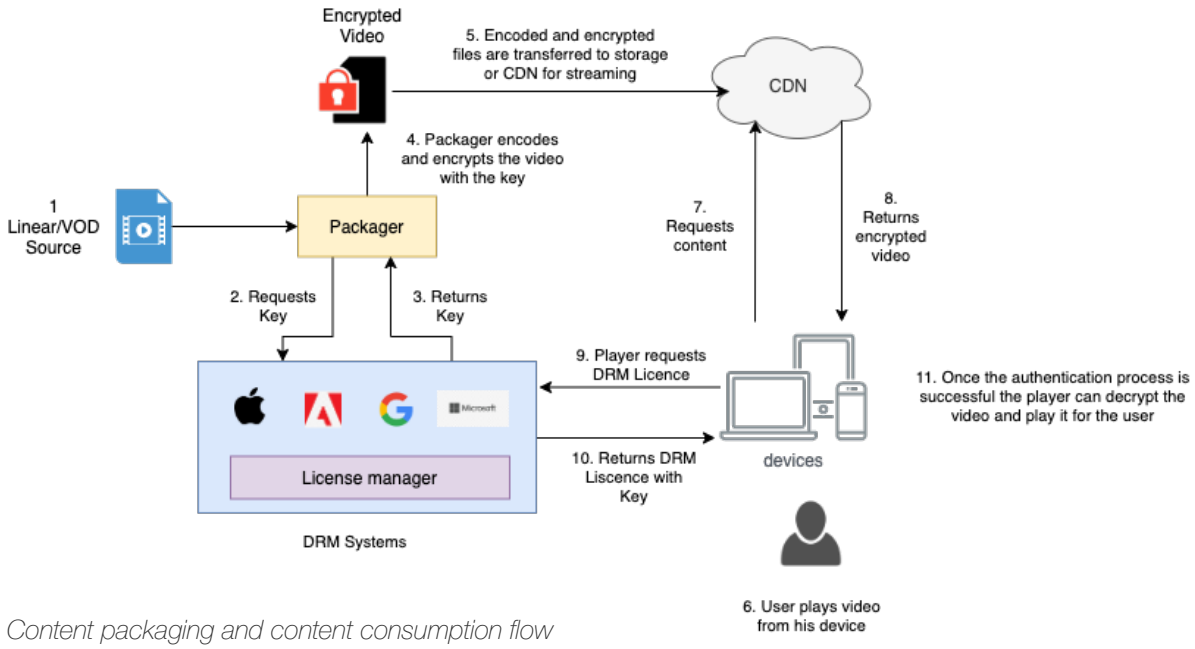

Figure 1: Content packaging and content consumption flow

Content Consumption

1. The user requests content from a device.
2. The client requests the content played by the user.
3. The content delivery network (CDN) returns the requested encrypted content to the client.
4. The client initiates a license request from the DRM system (requested either before playing back the content or once it discovers a license is required after playback begins).
5. The DRM system processes the license request and sends the response back to the client. The license* will contain the key to unlock the encrypted media, along with a set of rights and rights restrictions that specify exactly what can be played back.
6. After receiving the license response, the client parses the rights and rights restrictions and begins playback.

**The license consists of the encrypted key, as well as the access policies for that content. To ensure safety and avoid compromising the license data and tampering with access policies, the DRM License is also encrypted and protected with the unique key of the client's device.*

Leading DRM Systems

There are various DRM platforms and providers available. Below are the prominent players in this space. Focusing on these DRMs can deliver protected content to the vast majority of relevant platforms in browsers, smartphones, gaming consoles, and smart TVs.

Widevine is a proprietary DRM technology provider used by Google Chrome and Firefox web browsers (and some of its derivatives), Android MediaDrm, Android TV, and other consumer electronic devices. Google acquired Widevine Technologies in 2010.

PlayReady is a successor of Windows Media DRM. It is available on most connected TV devices (LG, Samsung, etc.), Windows operating systems, Windows Mobile, and Xbox. It was announced in February 2007.

FairPlay is a DRM technology developed by Apple Inc. This DRM solution is intended to encrypt content packaged using HLS and is meant for use with all iOS devices, Apple TV, QuickTime, and content stored locally on Apple Music.

Platform	Widevine	FairPlay	PlayReady
Chrome	✅		
Firefox	✅		
Edge			✅
Safari		✅	
Android	✅		
iOS		✅	
Android TV	✅		
Apple TV		✅	
Roku	✅		✅
Fire TV	✅		
Playstation			✅
Xbox One			✅
Samsung Smart TV			✅

Figure 2: Popular platforms and their compatibility with the DRMs

Encryption & Adaptive Streaming

Platform	Adaptive Bitrate supported	Encryption supported
Google Widevine	MPEG-DASH	AES-128 CENC
Microsoft PlayReady	MPEG-DASH	AES-128 CENC
Apple FairPlay	HLS	AES-128 CBCS

Figure 3: ABS and Encryptions supported by Major DRMs

Dash (Dynamic Adaptive Streaming over HTTP) and HLS (HTTP Live Streaming) are adaptive bitrate streaming protocols that enable high-quality streaming of media content over the internet. Both work by breaking the actual media content into various small media segments encoded at different bit rates and are delivered to the client using a playlist.

The references for these segments are maintained in the manifest file. The manifest file also contains the DRM system data and additional metadata info. The industry-standard manifest files for HLS and DASH are .m3u8 and .mpd, respectively.

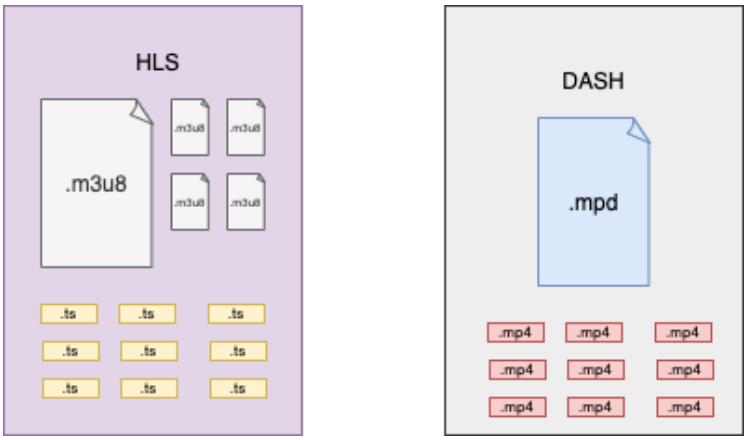

Figure 4: Pictorial representations of HLS and DASH stream

ABS ensures consistent playback without any interruptions due to bandwidth issues. The player switches between different encoded bit rates, depending upon the available bandwidth. If the bandwidth is good, the player will switch to higher rate streams. In cases of low bandwidth, it will automatically switch to lower bit rate streams. ABS enables the best media viewing experience with very little buffering and load time.

PlayReady and Widevine support common encryption standards, as mentioned in MPEG-CENC*. Apple officially supports SAMPLE-AES.

**The Common Encryption Scheme (CENC) specifies standard encryption and key mapping methods that can be utilized by one or more digital rights and key management systems (DRM systems) to enable decryption of the same file using different DRM systems.*

The media content can be encrypted using a single key or multiple keys, as per business rules and requirements. A multi-keys approach can be used in many ways. Here are a few:

1. Encrypt audio and video using different keys
2. Encrypt different bit rate streams with the help of different keys
3. Implement key rotation over time, etc.

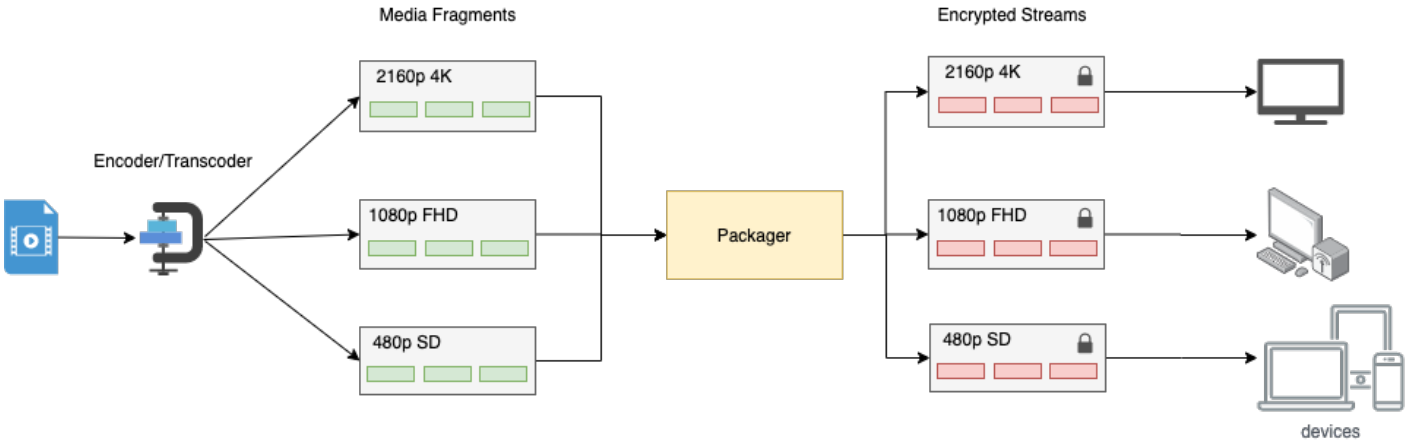

Figure 5: Multiple bit rates being packaged before distribution

The encryption keys are generated at runtime during the encryption process. With each content key, there is an associated key identifier (KID). The content key is a private value, whereas the KID is a public value. The content key and the KID are stored in the key management server. The KID is packaged with encrypted content and delivered to the client. The client, with the help of the KID, requests a license server for the content key. With the help of this content key, the player decrypts the media content and renders it to the user.

CPIX

During encryption and decryption, the keys and other DRM-related information are exchanged across various entities and setups. It is of utmost importance to keep this data extremely secure and make it available to multiple setups whenever required.

There are various ways in which this protected data can be exchanged across multiple setups, but these are DRM vendor-specific. To address this, DASH-IF developed platform-independent specifications known as CPIX (Copy Protection Information Exchange)

CPIX is a specification that states how protected information should be stored. CPIX is an XML-based document that contains the content keys and the DRM-related information required for encryption and decryption of media content. The CPIX document significantly reduces the complexity of exchanging protected data across setups.

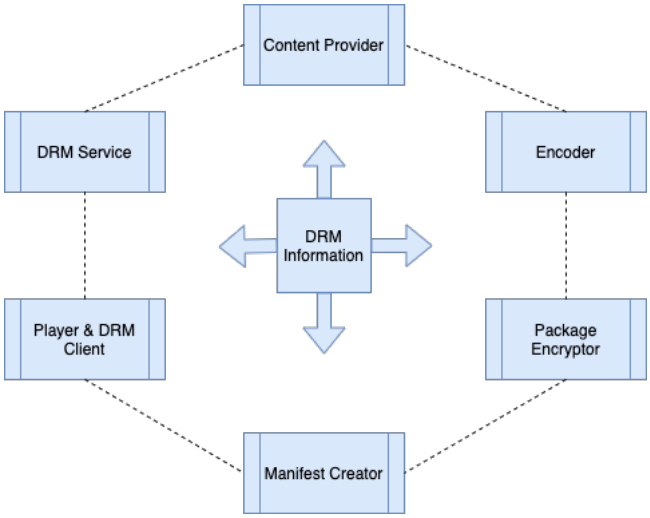

Figure 6: Logical setup that exchanges DRM information and media

How Does Playback Work?

For native applications, the player interacts directly with its native DRMs to acquire the key to decrypt content to play on the device. Apart from this, OS also provides the APIs to handle the license and apply the required access policies. In the case of browsers, playback will be achieved through HTML5 EME*.

**EME (Encrypted Media Extensions) is a specification provided by W3C that enables communication between web browsers and DRM agent software to allow HTML5 video playback of encrypted content without third-party media plugins.*

Multi-DRM Overview

In the past few years, there has been a trend to use a single DRM and its client SDK. We've seen constant growth in the use of streaming devices, but with each new device and platform comes new configurations. It becomes an uphill task to maintain and update numerous settings that vary from platform to platform. As a result, OTT providers are shifting towards a native DRM approach. Each native DRM supports its own native DRM client, so a multi-DRM setup comes into the picture.

The delivery of protected content is simplified with the help of the CENC standard in a multi-DRM setup. Before CENC, each DRM platform supported its own encryption standard. That resulted in multiple encrypted copies of the same asset, which in turn impacted cost and latency. With CENC, many platforms started supporting common standards for encryption. CENC helped reduce the cost of managing the encrypted content, improving latency and storage because fewer encrypted copies now need to be maintained for the same asset (primarily one for HLS and the other for DASH, as discussed in previous sections). A multi-DRM setup also has the advantage of eliminating the licensing cost because native DRM clients are usually free on their platforms.

The main task for service providers is to procure the right to make content available to the consumer. The multi-DRM setup helps service providers gain the trust of content owners, studios, or broadcasters because it assures that their content is highly secured. This is a result of decryption happening at the player level, and the player itself interacts with the DRM systems to decrypt the content.

With CPIX, the exchange of protected information across multiple setups in the OTT delivery ecosystem becomes simplified and interoperable.

One of the important aspects to keep in mind while using a multi-DRM setup is that not all DRMs support similar functionality. Often the supported functionality is rather basic and does not fit the business rules and requirements. For example, FairPlay does not support any business rules at all. It requires significant effort to create a unique experience across all devices.

There are many multi-DRM solution providers present in the market who provide the following:

1. Extended security capabilities to meet content protection requirements as per business rules
2. Enabled service features that are required by end-users and businesses, such as download and pay-per-view
3. Fast recovery, in case there is any data breach or risk

There are many advancements in the DRM market, resulting in universal standardization of encryption and how protected data is exchanged with the help of a unified API. We will discuss this in more detail in the next section.

Advancements in the DRM Market

SPEKE

DRM solution providers need to implement a custom API to exchange protected information between encoders, origin servers, and DRM system key servers. A custom API requires effort to develop and is unique for every solution provider. There is an incremental cost and effort needed for every new integration.

The above-mentioned scenario is solved using SPEKE (Secure Packager and Encoder Key Exchange). The genesis of SPEKE resulted from the need to create an abstracted and standardized way for key exchange between encoders and DRM systems. SPEKE is an open-source Rest API specification that uses CPIX as a standard for key exchange. It builds on CPIX by adding the specifications, such as a method for authenticating and communicating between encoders and DRM systems.

SPEKE has the single purpose of simplifying the complex process of exchanging protected information across the OTT delivery system. It replaces various complex proprietary API integrations between multi-DRM setups with a single open API standard.

SPEKE helps remove the redundant code for these integrations and thus makes applications lighter with improved latencies. It also allows DRM solution providers to focus on core functionalities, rather than spending time and money on developing custom API interfaces.

CMAF

For many years, Apple supported the HLS protocol, which used the MPEG transport stream container format. Other companies used the DASH protocol with the fragmented mp4 form. To serve all the major devices in the market, it was necessary to maintain files in two different formats, one packaged with HLS and the other with DASH.

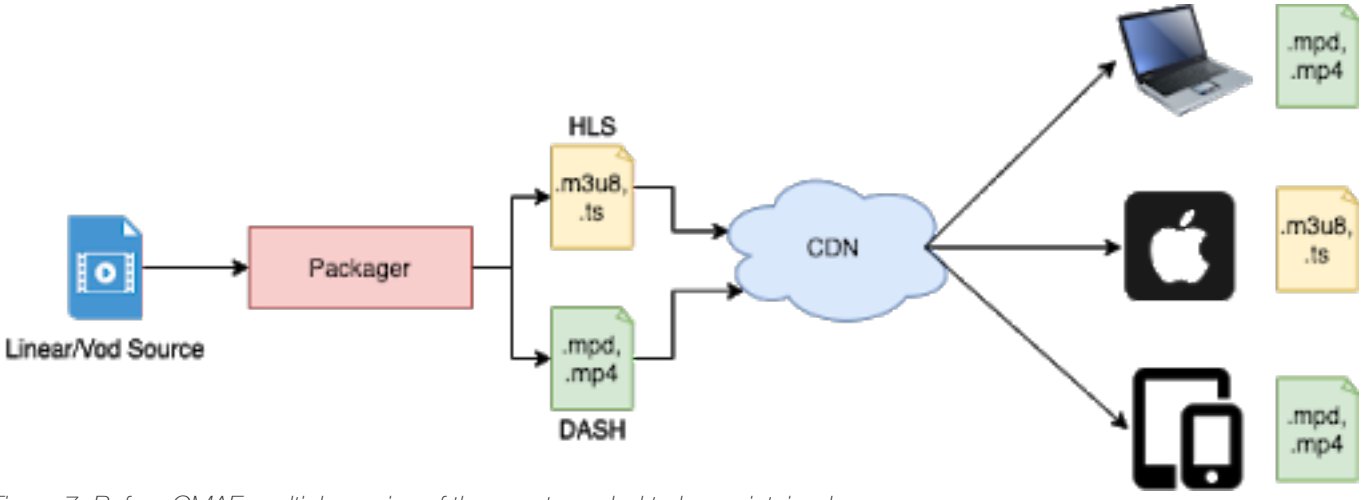

Figure 7: Before CMAF, multiple copies of the asset needed to be maintained

In recent years, there has been a lot of traction to support a single set of encryption and maintain a single copy instead of two (to support both HLS and DASH). This is now possible with the help of CMAF (Common Media Application Format).

CMAF was designed in a collaboration between Microsoft and Apple with linear streaming, content protection, and ad signaling in mind. CMAF uses the ISO Base Media File Format (ISOBMFF) container with common encryption (CENC).

Unlike DASH and HTTP Live Streaming (HLS), CMAF isn't a presentation format. It's a container format that can contain one set of audio/video files, with manifest files for multiple presentation formats and multiple DRMs.

In a nutshell, CMAF replaces these multiple copies with a single set of audio/video mp4 files and their respective adaptive bitrate manifest files.

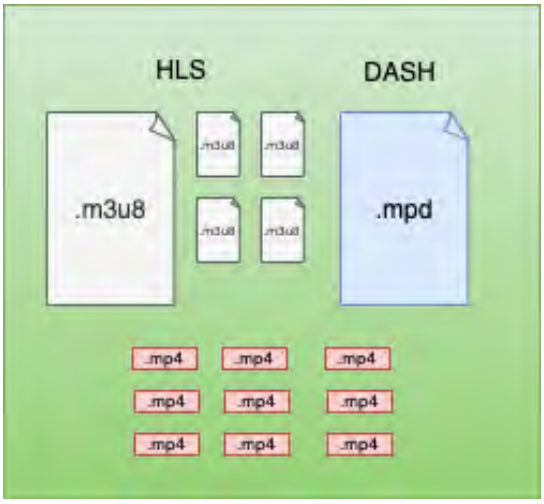

Figure 8: CMAF container structure

CMAF is superior to legacy systems in many ways. Here are a few:

- DASH/HLS with CMAF reduces storage and packaging costs
- Improves edge caching latency, essential for linear streaming and Origin Storage Source
- Enables device interoperability

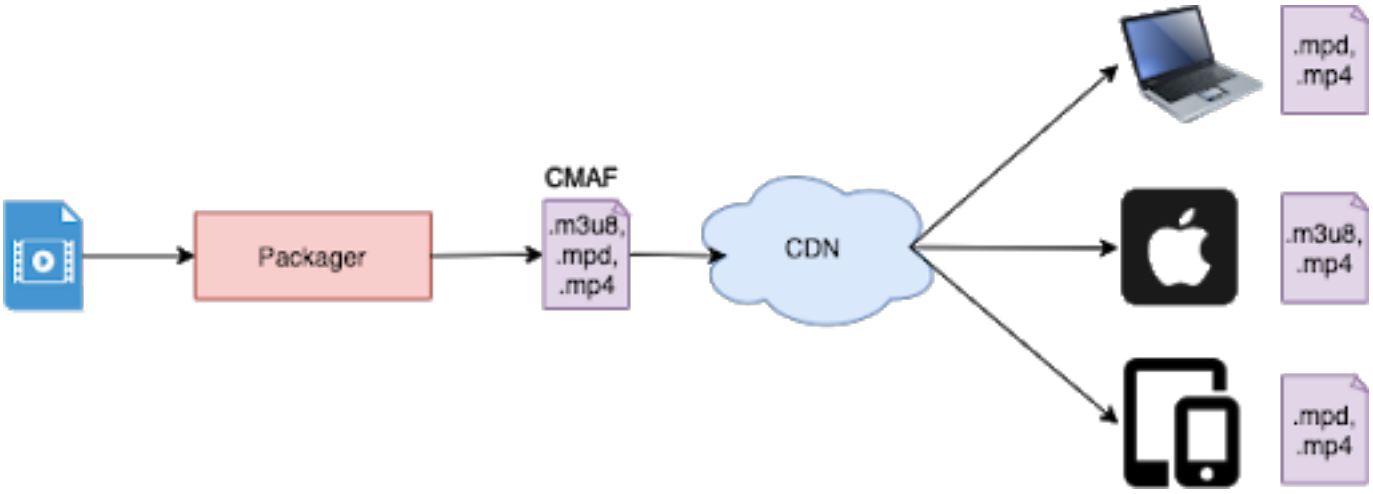

Figure 9: With CMAF, a single copy with multiple manifest files

Conclusion

In the era of OTT, content is the most crucial resource, and DRM helps safeguard it. DRM is here for good and has already gone through many changes. In the foreseeable future, it will also see the same growth. Currently, the DRM market is moving toward standardization and unification to make the setup simpler and more manageable.

CMAF is unquestionably the game-changer in the DRM market. But being new in the market, many legacy systems and devices do not have support for it. To reach a broader market, providers still need to manage multiple copies of assets. This scenario will change in the coming year as legacy devices and systems start phasing out.

A multi-DRM setup is best suited to support a larger audience and a more extensive range of devices. Numerous multi-DRM solution providers in the market help deliver protected content. By choosing the right multi-DRM solution provider, companies gain agility, reduce costs, and strengthen security. The best provider also reduces the time required to launch a product to the market and take advantage of the OTT wave.

About the Author

Ajinkya Jawanjal works as an Associate Consultant at GlobalLogic. He has 7+ years of experience in developing iOS, tvOS, and Roku applications, with vast experience in developing Media Streaming and OTT applications.

References

- Digital Rights Management (DRM) Architectures
- ISO/IEC 23001-7:2015 - Information technology — MPEG systems technologies — Part 7: Common encryption in ISO base media file format files
- MPEG-DASH — Unified Streaming
- DASH-IF Implementation Guidelines: Content Protection Information Exchange Format (CPIX)
- ISO/IEC 23000-19:2018 - Information technology — Multimedia application format (MPEG-A) — Part 19: Common media application format (CMAF) for segmented media
- WAVE Overview Part 1: CMAF and the WAVE Content Specification

GlobalLogic®

GlobalLogic is a leader in digital product engineering. We help our clients design and build innovative products, platforms, and digital experiences for the modern world. By integrating strategic design, complex engineering, and vertical industry expertise,— we help our clients imagine what's possible and accelerate their transition into tomorrow's digital businesses. Headquartered in Silicon Valley, GlobalLogic operates design studios and engineering centers around the world, extending our deep expertise to customers in the communications, automotive, healthcare, technology, media and entertainment, manufacturing, and semiconductor industries.



www.globallogic.com