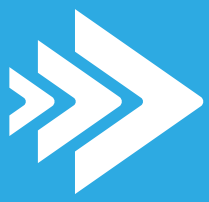


BITMOVIN

Video Infrastructure for the Web

The State of Web-DRM 2016

About Bitmovin

Bitmovin builds video infrastructure for the web with a feature rich API, built by developers for developers, so it is easy to integrate and adaptable enough to fit into any existing system.

The **Bitmovin Cloud Encoding Service** offers a scalable cloud infrastructure capable of encoding video into Apple HTTP Live Streaming (HLS) and MPEG Dynamic Adaptive Streaming over HTTP (MPEG-DASH) up to 100x faster than any other service. We are also multi-cloud enabled, which gives your video infrastructure unbeatable reliability and performance.

The **Bitmovin Adaptive Streaming Player** uses patented software technology to predict and avoid buffering better than any other player on the market. Play your MPEG-DASH or HLS videos native in HTML5 with no plugins and no buffering.

Bitmovin is a leader in adaptive streaming technology and supports MPEG-DASH and HLS, DRM integration, Ad servers, HEVC, VR and 360° and more.

Product demonstrations

The Bitmovin team is always ready to demonstrate any of our services or products. The quickest way to organise a demonstration is via our website at https://bitmovin.com/demonstrations/.

Request a Demo

BITMOVIN

Contents

Request a Demo

What is DRM?

Digital rights management (DRM) systems provide you the ability to control how people can consume your content. Usually content owners and producers such as Hollywood studios and TV stations will insist that their distributors use DRM systems to protect their content according to the constraints of their licensing agreements.

Hollywood-grade DRM protection is not always needed, and sometimes it's enough to provide basic protection through token-based secure authentication or simple AES encryption of the video without sophisticated license exchange and policy management.

How Does It Work?

A standard workflow for DRM on the web needs encoding, packaging, play-out, and a communication mechanism to one or more license servers. In the following sections we will describe these steps in detail.

As a content provider, it is important to understand each step in the process, but in practical terms the most efficient way to implement a reliable DRM workflow is to use an "out of the box solution" from one provider. This ensures that every step in the process is seamlessly connected to the next and avoids unnecessary integration costs. Bitmovin offers exactly this type of solution by providing encoding, packaging, and a player that is pre-configured to communicate with a variety of licensing servers. (See Figure 1.)

License servers are offered by companies such as Irdeto, EZDRM, ExpresssPlay, BuyDRM™ and Axinom, which provide a multi-DRM solution. It's also possible to run your own license servers and negotiate terms directly with Google (Widevine), Microsoft (PlayReady), Adobe (PrimeTime), or Apple (FairPlay), but this is usually not necessary.

BITMOVIN

"Digital Rights Management (DRM) systems provide you the ability to control how people can consume your content"

Request a Demo

How does DRM work?

AWS S3

Google Cloud Storage

FTP/SFTP

1 Source
The input files can start from a variety of sources, such as AWS S3, Google Cloud Storage, FTP/SFTP, etc.

Files are transferred via HTTP or FTP

2 Encoding
The cloud encoding system will encode the source files into adaptive streaming formats such as MPEG-DASH and HLS.

3 Encryption
As this process takes place the encoder will **encrypt the files with media keys** from one or more DRM providers.

Media Keys from the DRM providers

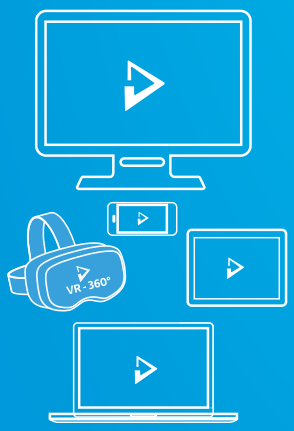
DRM Servers

Microsoft Adobe Google

The encoded and encrypted files are transferred to storage or CDN for streaming

4 Storage
The adaptive video is usually stored in a content delivery network ready for a user to click the play button.

The video is streamed to the adaptive player



5 Authentication
The player communicates with the DRM server to ensure that the license is valid.

6 Playback
Once the authentication process is successful the player can unencrypt the video and play it for the end user.

BITMOVIN
Video Infrastructure for the Web

Need to know more about DRM? Ask a question at Bitmovin.com/contact

Encoding & Packaging

From an encoding and packaging point of view there is little difference whether the video is "just" AES encrypted or Hollywood-grade DRM encrypted, because AES is used in both cases. The major difference is that for Hollywood-grade DRMs, further metadata information needs to be added in the packaging step. Hollywood-grade DRMs such as PlayReady, Widevine, PrimeTime, and Fairplay don't differ much on the encryption side; they differ on the configuration features that are provided. Examples of these might be features such as offline playback, fine-grained policies (e.g., allow only SD playback, rights visibility for users, APIs, different payment modes such as subscription, purchase, rental, gifting, etc.), and probably most important, platforms/browsers that are supported (e.g., Chrome, Firefox, IE, Safari, Android, iOS, etc.).

Multi-DRM with MPEG-CENC

Typically, each platform/browser combination supports just a single DRM. This means that if you want to achieve maximum device reach it's impossible to use just one DRM. You need to use multiple DRMs in parallel. The MPEG Common Encryption (MPEG-CENC) standard enables this in the most efficient way as it allows key association from different DRMs with the same video. The player then decides, based on the platform/browser support, which specific DRM will be used.

MPEG-CENC is a huge improvement on the traditional Multi-DRM model as it prevents duplication by avoiding the need to create one output package for each DRM. This is a huge saving on encoding, storage, distribution, and file management resources.

HLS with FairPlay

Apple doesn't officially support MPEG-CENC and enforces the use of FairPlay with HLS (Apple HTTP Live Streaming) on Apple devices and Apple web browsers such as Safari. FairPlay uses SAMPLE-AES for encryption, where only media samples are encrypted rather than the entire segment, similar to MPEG-CENC. To cover a wide variety of devices and platforms—including the Apple ecosystem—with DRM streams, there is no way around the usage of both MPEG-DASH with MPEG-CENC and HLS with FairPlay together.

BITMOVIN

"On the player side it's possible to utilize the HTML5 Encrypted Media Extensions (EME) to enable DRM playback without plugins"

Request a Demo

Playback

If your content is MPEG-CENC multi-DRM encrypted, a player could automatically choose the DRM that is natively supported on the given platform to playback the content, using HTML5/JS without the need for plugins. The authentication and the license acquisition will be handled by the player through the HTML5 Encrypted Media Extensions (EME) with the metadata that is provided with the content. If the DRM is not supported through the EME, you can fallback to a third-party system such as Flash and Adobe Access, if supported by the player.

Licensing Server

The licensing server is the management backend of your DRM setup. It allows you to create, modify, and revoke licenses for your content and users. Licensing servers and DRMs differ in their features such as offline playback, fine-grained policies, rights visibility for users, APIs, different payment (subscription, purchase, rental and gifting), etc. License servers are provided by several companies such as Irdeto, EZDRM, ExpresssPlay, or Axinom.

Basic Encryption

A Hollywood-grade DRM is not always needed; sometimes it's enough to just add another layer of security through AES encryption. HLS and MPEG-DASH both support this use case.

BITMOVIN

"If your content is MPEG-CENC multi-DRM encrypted, a player could automatically choose the correct DRM"

Request a Demo

BITMOVIN

HLS AES Encryption

Apple HLS supports two encryption methods:

- **AES-128**
- **SAMPLE-AES**

AES-128 encrypts the whole segment with the Advanced Encryption Standard (AES) using a 128-bit key, Cipher Block Chaining (CBC) and PKCS7 padding. The CBC will be restarted with each segment using the Initialization Vector (IV) provided.

SAMPLE-AES encrypts each individual media sample (e.g., video, audio, etc.) separately with AES. The specific encryption and packaging depends on the media format, e.g., H.264, AAC, etc. SAMPLE-AES allows fine grained encryption modes, e.g., just encrypt I-frames, just encrypt 1 out of 10 samples, etc. This can decrease the complexity of the decryption process. This method can be advantageous as fewer CPU cycles are needed, which reduces power consumption. This is particularly useful for mobile devices.

DASH Clear Key Encryption

Clear Key handling has to be implemented by all browsers, supporting the EME. Using this system, media can be encrypted with a key and then played back simply by providing that key. MPEG-DASH signals the key in the Media Presentation Description (MPD), which is the manifest of MPEG-DASH. All the relevant information that is needed for decryption is included in the MPD.

Hollywood & UltraViolet

When implementing a DRM strategy you should check that the DRM is accepted by the content owner. This means that if you distribute Hollywood content you need to implement a DRM that is accepted by the Hollywood studios.

Even if you don't deliver Hollywood content it's good to know what is acceptable to deliver Hollywood content in case you need to in the future. Replacing an existing DRM solution is difficult and because Hollywood has already done the due diligence on the DRMs for you, it's an easy precaution to take.

The Digital Entertainment Content Ecosystem (DECE) is a consortium of 85 companies (e.g., studios, manufactures, etc.) that created the UltraViolet standard that ensures that after you purchase your content, you are able to watch it on broad range of devices. DRM is a major part of UltraViolet and therefore six DRM technologies have been approved:

- **Widevine**
- **PlayReady**
- **PrimeTime**
- **Marlin**
- **OMA**
- **DivX DRM**

Apple Fairplay is not part of this list as Apple is not a member of the DECE and Fairplay has just recently entered the market.

DRM Systems

If DRM is a requirement for your project you should take a look at the major DRM systems. Microsoft, Google, Adobe and Apple provide high profile DRM systems with various features. In the end you will probably end up with a Multi-DRM setup where you utilize several or all of these DRMs in parallel to reach all the major devices.

The following pages have more details about the major DRM systems.

"A Hollywood grade DRM is not always needed, sometimes it's enough to just add another layer of security through AES encryption"

Microsoft

PlayReady

Microsoft released PlayReady in 2008 and it's one of major DRM systems on the market, with broad device support and sophisticated features. It has been used at scale by many events already, such as the 2014 Winter Olympics in Sochi, Russia. PlayReady supports domain licenses which means that one user could share the license for the content on multiple devices that belong to this user. In general PlayReady is platform independent and could probably also run on non Microsoft software but typically it is integrated with Microsoft products.

Which devices and browsers have native PlayReady support?

- Internet Explorer on Desktop
- Microsoft Edge on Desktop
- ChromeCast
- Many Televisions

Bitmovin & PlayReady

The Bitmovin encoding service supports PlayReady encryption and packaging with MPEG-CENC and the Bitmovin player plays PlayReady encrypted videos on platforms that support the PlayReady DRM natively, like Internet Explorer and Microsoft Edge in HTML5 without plugins.

BITMOVIN

"In the end you will probably end up with a Multi-DRM setup where you utilize several or all of these DRMs in parallel to reach all the major devices"

Request a Demo

Widevine

Widevine is a Hollywood grade DRM technology initially developed by Widevine Technologies and acquired by Google in 2010. For Google it was not only a technology acquisition it was also a strategic play. The acquisition opened new connections into the premium video sector and also deepened the relationship with Hollywood. This technology also fits perfectly into the Google ecosystem and plays well together with Android and YouTube, which will help to expand Google's overall video business. Widevine is natively supported on broad range of devices and browsers such as Google Chrome Browser, Android, Chromecast, etc.

Which devices and browsers have native Widevine support?

- Chrome Browser on Desktop
- Firefox Browser on Desktop
- Opera Browser on Desktop
- Chrome Browser on Android
- Native Android Apps
- ChromeCast

Bitmovin & Widevine

The Bitmovin encoding service supports Widevine encryption and packaging with MPEG-CENC and the Bitmovin player plays Widevine encrypted videos on platforms that support the Widevine DRM natively, like Chrome, ChromeCast, Android, Firefox etc. without plugins.

Fairplay

Apple's Fairplay DRM was initially used only in the iTunes store to protect AAC encoded audio files but was soon adopted for Apple's video products that are now part of the iTunes store. Fairplay is specifically designed for Apple HTTP Live Streaming (HLS) with Apple playback devices such as iPhone, iPad, Apple TV and Mac OS X. Fairplay is also used as a Content Decryption Module (CDM) of the Safari browser. This enables HTML5 native playback of DRM encrypted Fairplay streams without plugins in Safari.

Which devices and browsers have native Fairplay support?

- Safari on Desktop
- AppleTV

Bitmovin & Fairplay

The Bitmovin encoding service supports Fairplay encryption and packaging with HLS and the Bitmovin player plays Fairplay encrypted videos on platforms that support the Fairplay DRM natively, like Safari and AppleTV, without plugins.

PrimeTime

Adobe PrimeTime is the successor of Adobe Access and was officially launched on the National Association of Broadcasters (NAB) show in 2013. PrimeTime is a DECE approved Hollywood grade DRM that is also approved by the UltraViolet standard. Adobe's DRM offers a fine grained policy management system that allows to whitelist applications, devices, domains etc. and it also has support for key and license rotation. The Mozilla Firefox browser supports PrimeTime as Content Decryption Module (CDM) and therefore PrimeTime is natively supported through HTML5 in the Firefox browser.

Which devices and browsers have native PrimeTime support?

- Firefox Browser on Desktop

Bitmovin & Primetime

The Bitmovin encoding service supports PrimeTime encryption and packaging with MPEG-CENC and the Bitmovin player plays PrimeTime encrypted videos on platforms that support the PrimeTime DRM natively, like Firefox, without plugins.

DRM Browser & Device Support

Desktop MPEG-DASH HTML5 DRM

Browser	Streaming Format	DRM	Bitmovin Support
Chrome	DASH HTML5	Widevine Modular	✓
Firefox	DASH HTML5	PrimeTime & Widevine Modular	✓
Internet Explorer[1]	DASH HTML5	PlayReady	✓
Microsoft Edge	DASH HTML5	PlayReady	✓
Opera	DASH HTML5	Widevine Modular	✓

Desktop HLS Encryption

Browser	Streaming Format	DRM	Bitmovin Support
Chrome	HLS HTML5	AES HLS	✓
Firefox	HLS HTML5	AES HLS	✓
Internet Explorer[1]	HLS HTML5	AES HLS	✓
Microsoft Edge	HLS HTML5	AES HLS	✓
Safari	HLS HTML5	AES HLS & Fairplay	✓
Opera	HLS HTML5	AES HLS	✓

Mobile Devices DRM Support

Device	Streaming Format	DRM	Bitmovin Support
Chrome on Android	DASH HTML5	Widevine Modular	✓
Safari on iOS	HLS HTML5	AES HLS	✓
Edge on Win for mobile	DASH HTML5	PlayReady	✓

Streaming Devices

Device	Streaming Format	DRM	Bitmovin Support
Chromecast	DASH HTML5	Widevine Modular & Playready	✓
Apple TV	HLS HTML5	Fairplay	✓

1 Internet Explorer 11 Windows 8.1+

BITMOVIN

"Bitmovin provides you an easy to use interface for Multi-DRM encoding and playback with a low friction API and excellent support"

Request a Demo

Maximum Device Reach with Multi-DRM

The Bitmovin encoding and player solution allows you to use multiple DRMs in parallel. This means that you encode, encrypt and package your content once and you can playback with several different DRMs, such as Widevine, PlayReady, PrimeTime, etc. This is especially important if you want to increase your device reach. Due to fragmentation in the market it is not possible to reach all major devices with just one DRM. Therefore, you need to use multiple in parallel which is possible as all DRM systems use AES for encryption. If you use the same key in the different DRM systems for the same video you just need to add additional metadata for each DRM to this video and then it can be played back with DRM systems.

In detail it's a little bit more complex as this needs additional logic on the encoding as well as on the player side but Bitmovin provides you solutions for both. What you also need for such a setup is a 3rd party Multi-DRM provider such as Irdeto, EZDRM, ExpressPlay, BuyDRM™, Axinom, etc. It's also possible to create your own licensing backend if you have a contract with Google (Widevine), Microsoft (PlayReady), Adobe (PrimeTime) or Apple (Fairplay) directly and you implement the specification.

Conclusion

The DRM market is still very fragmented and if you want to reach a reasonable amount of the major devices you will need to use multiple DRM providers. Bitmovin provides you an easy to use interface for Multi-DRM encoding with a low friction API and excellent support. You can encode your content once and make it compatible with all DRM systems that you want to support. This not only decreases the storage footprint of the content, it also makes it more efficient on the distribution side as content can be reused more effectively.

On the other end of the chain the Bitmovin player enables HTML5 based DRM playback without the need for plugins. The player automatically detects which DRM is natively supported on the given platform and uses the right DRM system for decryption. You will also need a license server or license server provider. The easiest way to achieve this is to use a Multi-DRM provider that has already contracts in place with Microsoft, Google, Adobe and Apple and provides a uniform interface for all these DRM systems.

Request a Demo

BITMOVIN
Video Infrastructure for the Web

Bitmovin, Inc.
530 Lytton Avenue, 2nd Floor
Palo Alto | CA 94301 | USA
+1 650 4585453

Schleppe Platz 7
9020 Klagenfurt
Austria | Europe
+43 463 203014
sales@bitmovin.com

bitmovin.com