

Digital Rights Management 101

What is DRM and How Does It Work?



WHAT IS DRM?

Protection of video content is a basic mechanism at the heart of any video service business. You don't need to be a major Hollywood studio to want such protection over your media assets - any proprietary or valuable asset is likely to require a layer of security and a mechanism to monetize it. Protection of video often involves encryption of the media and a controlled way to distribute the key(s) required for playback. At a basic level, Digital Rights Management (DRM) technology combines these mechanisms and enables a video service to control how, where and when people can view your content.

Most people don't think very much about DRM on a day to day basis - and it is not a topic raised at the average cocktail party. But from a business perspective it's a vital tool - a tool that helps the business of video delivery happen in an organized fashion.

DRM has been - and will remain - a basic requirement for a commercial video service because:

- Content owners require protection of the intellectual property rights embedded in their video assets when rights are negotiated to deliver that content as part of a video service.
- Commercial video services require an ability to switch on/off viewing rights to an individual or a device to build a business model around payment for the service. If consumption can't be metered and controlled, then payment models can't be enforced.
- Protection of video streams during delivery helps enable other forms of monetization, such as ad insertion, remain effective and secure.

DRM technology and usage has evolved dramatically in this environment over the last 20 years - but has also become a much bigger business with the advent of large scale on demand and live streaming services. At the same time, the landscape for video consumption has become more diverse and complex.

For a full discussion of this topic, please visit our web page DRM FAQ at www.ezdrm.com/DRM-Industry-FAQ

DRM WORKFLOW

To follow the logic of how a DRM can be effective, its best to start with a quick summary of a typical modern video workflow:

- **Encoding and packaging:** After video is compressed, it is cut into a series of short time segments and then encrypted for delivery. The encryption process is a combination of encryption keys, unique to this video, and an algorithm that determines how each video segment is scrambled. Importantly, a record of where the keys for this video can be requested is kept in a manifest file together with the associated collections of video segments.
- **Media delivery:** A video is selected for playback by choosing a link to the manifest file through a browser or app on the playback device. The manifest file is then delivered to the device.
- **Media playback:** As the manifest is read by the device, it sets in process the parallel operations of requesting the necessary segments of video and passing the key references to a local DRM client component. The DRM client then makes a request to a DRM service to retrieve a license object that contains the decryption keys. The DRM client applies the keys and the same algorithm used to scramble the video to make it playable on the screen of the device.

Note that license requests from DRM clients are not always granted by the DRM service. No license would be issued to client device that isn't associated with a legitimate user for example. And a license for UHD movies would not be issued to a device that did not have adequate playback security for such valuable content.

DRM IN DEVICES

In general, each type of video playback platform or device will use a single type of DRM client software. The major DRMs being used on devices today are:

- Apple Fairplay
- Google Widevine
- Microsoft PlayReady

More details of each of these DRMs and tables showing the devices that support these different DRMs can be found on our web site.

WHAT IS CENC?

As mentioned above, video encryption is a process using a combination of keys and an algorithm. Until recently, the algorithms used were determined by the individual DRMs - which meant that video files and streams playable using one DRM were incompatible with those payable by another. An ISO standard referred to as Common Encryption is now helping to standardize the encryption (and decryption) process, but without interfering with the proprietary way keys are chosen and used in license objects by individual DRM technologies.

MULTI-DRM

The use of CENC during packaging leads to a limited compatibility of MPEG-DASH format streams that are readable and playable on devices with different DRM clients. The same manifest file - and therefore the same stream - is read by devices using Google Widevine and Microsoft PlayReady DRMs. But the DRM client reading the manifest in each device uses its own mechanisms to retrieve and interpret a license that includes the decryption keys. The DRM clients need to talk to a Multi-DRM license service to make these requests - one that can service different types of request that all refer to the same encrypted media file.

WHAT ABOUT FAIRPLAY DRM?

Devices that use Apple Fairplay - and these not surprisingly are Apple branded devices - still have some distinct stream format and encryption algorithm differences. These HLS format streams will often need to be packaged in parallel with those in other formats to service the considerable base of Apple devices. Luckily the

same DRM service can support Fairplay license requests alongside those from Widevine and PlayReady.

ONLINE & OFFLINE PLAYBACK

Not all video playback happens on a device that is connected to the Internet. In fact, a popular playback option is to download a video from a service and watch it when offline. To make this possible, the DRM client - and the service that the DRM client communicates with - must support the use of a persistent license. A persistent license is one that can be requested by the DRM client as the video content is being downloaded but not used by the DRM client until the video playback is actually started. Persistent licenses are typically only valid for a certain limited duration, so devices must reconnect to the video service to renew or refresh the offline playback rights.

WHAT IS CMAF?

The Common Media Application Format (CMAF) is a newer initiative that builds on MPEG-DASH standardization, but also attempts to reconcile the Apple defined HLS format with some of the DASH related advances to move forward to a common encrypted video file format that can be used as the origin of all streaming delivery. There are many in the industry who believe this convergence cannot come fast enough.

EZDRM FEATURES

EZDRM is truly a specialist in cloud-based DRM services - that's all we do! And using best of breed cloud components is where the video service market has been headed for the last several years. Because of this specialization, we offer a source of application expertise and a solution that has continued to evolve with the industry, addressing the challenges of our customers deployments as their needs have changed. This unique approach includes:

- Highly reliable technology management and maintenance
- Full native DRM capabilities and feature set
- Effortless service scaling with business growth
- Expert service and support

Take a look at our service demonstrations today - it really can be that easy!