

[Developers](#) [Adopters](#) [FAQ](#) [Resources](#) [News](#) [About](#)

Marlin DRM FAQ

Learn more about content security principles, differences between conditional access systems (CAS) and digital rights management (DRM), DRM license mechanics, Marlin DRM, and more.

How do I protect digital video distribution and over-the-top (OTT) streaming services?



Anybody intending to offer an over-the-top (OTT) digital video streaming service, such as live sports, premium movies and Ultra HD (UHD) programming, will need to protect the media assets from unlicensed use and outright theft during content preparation, delivery and storage. This need stems from the fact that Hollywood studios and sports rights holders require strong content protection, represented by digital rights management (DRM), as a condition for licensing the desired programming for pay-TV distribution. The role of pay-TV and OTT security is to manage the content monetization while preventing media piracy and thus safeguarding the associated revenue, which is a critical requirement for both content providers and service operators.

So how can digital assets be protected? DRM technology works by combining *content encryption* with advanced *key management* and an associated *licensing policy* that grants access for end-user devices that meet the criteria required by the policy. Moreover, combining DRM with other tools such as forensic watermarking and anti-piracy services, offers an effective solution to secure

content and revenue.

The end result is that seamless modern multi-DRM services have transformed the media landscape – enabling OTT streaming providers to create all-new pay-TV business models – and allowing more viewers to watch content whenever and wherever they want around the world.

Download our [free e-book](#) to learn more about securing advanced OTT video delivery with multi-DRM service.

What is encrypted digital media?



The first step in the process of content protection is to apply encryption to the payload. The content is encrypted during the packaging phase of the content preparation. Typically the content packaging, for example for DASH-CENC or SAMPLE-AES, relies on AES encryption. An AES-128 bit key, known as the content encryption key, is used to encrypt the video and audio tracks. That is, nobody will be able to watch an encrypted file or program unless they also have access to the same key that was used to render the content unwatchable. The reverse process is called decryption, by applying the same key to restore the content to a clear (watchable) state. Secure content delivery is enhanced by “rotating” or changing the key with a predefined period, e.g. 10 seconds, so that even if somebody obtains such a key in the clear, it is only good for one key rotation period. A program usually consists of separate files or streams for video, possibly with different quality levels or resolutions, and multiple audio files (original language and one or more alternative languages).

The content encryption keys need to be transmitted to the receiver in a secure fashion so that only authorized viewers can decrypt and watch the content. This is all part of the management of “pay-TV secrets” and usually referred to as key management. Beyond encryption keys there are several other keys that are used to protect other secrets such as the entitlement management message (EMM), which holds information regarding the channels or programs a viewer may watch, a.k.a. “channel line-up” in multi-channel pay-TV systems. All this is managed by the content security system with its license servers.

Watch our brief What is DRM and how does it work video

Why were conditional access systems (CAS) created, and how has content security evolved?



Until the late 1950s, the TV industry had a single business model: Sell advertising or product placement to pay for programming and monetize content. With the gradual introduction of pay-TV in the '60s, this model began to change.

The basic requirement of pay-TV was (and still is) to be able to manage access control. To control access, pay-TV operators encrypt content so only subscribers can access and watch it. Pay-TV operators adopted conditional access systems (CAS) to manage content security and ensure that they and other rights holders could monetize their assets. Digital CAS technology became the norm with the introduction of the digital video broadcasting (DVB) standard in the mid '90s, but non-DVB content protection systems were also created in the United States by companies such as General Instrument (later Motorola). The DVB standard includes a Common Scrambling Algorithm (DVB-CSA), and a standard for connecting one or more CA systems to multiplexers/scramblers called DVB Simulcrypt.

The CAS model is still used to protect DVB pay-TV services transmitted over satellite and terrestrial "one-way" networks, as well as telco IPTV (a.k.a. managed IPTV), although they both have been complemented with digital rights

management technology to protect IP-based over-the-top (OTT) streaming services (video transmitted over the internet).

The evolution of content security technology can be divided into four phases:

Phase 1: Hardware-based CAS security clients, such as smart cards, were used in set-top boxes (STB) to store the content protection “secrets” due to the lack of two-way connectivity in one-way broadcast networks

Phase 2: Smart cards are no longer required in modern CA systems, partly because modern system-on-a-chip (SOC) technologies include separate processing and storage environments intended for content security

Phase 3: Introduction of digital rights management (DRM) systems, which are either software based or implement combinations of software with hardware support found in modern SoCs, for delivery of IP-based OTT streaming services

Phase 4: DRM systems are gradually extended to the broadcast scenario too, taking advantage of two-way communication to manage secrets such as entitlements (“channel lineups”), and supporting the introduction of [hybrid broadcast-OTT STBs and smart \(connected\) TVs](#)

In short, legacy CAS technology is gradually being superseded by DRM-based content protection as the world moves from traditional broadcasting to hybrid broadcast-OTT solutions, as well as to pure OTT streaming over the internet.

What is digital rights management (DRM)?



Digital rights management (DRM) refers to the tools, standards and systems that are used to protect and monetize intellectual property and copyrighted materials from misuse or theft in the digital sphere, including Internet Protocol (IP) video pay-TV services transmitted over the internet.

Traditionally, digital content has been protected with encryption. Using a secret key, content is encrypted (and thus made unwatchable) so that only somebody who has the key can decrypt and view it. But because key, like all digital information, is easy to copy and share, on its own it is not sufficient to protect the content.

To bolster key encryption, business rules were added that define when and how

the keys can be used. The enforcement of those rules on the client devices that were used to consume the content came next and with it arrived digital rights management (DRM).

DRM consists of two main logical components: 1) data protection, and 2) data governance. Encryption technologies are generally used to provide data (content) protection, while trust management and policy management technologies are used to allow protected information to be distributed and used by trusted entities. This includes DRM license management performed by a DRM license server.

The components of a DRM ecosystem work together and borrow from the basic principles of computer security:

Secrecy / Confidentiality - This is achieved by the encryption of the content.

Authentication and Authorization - This is achieved by the certificate exchange between the DRM client and the DRM license server for mutual authentication purposes during the license acquisition phase.

Integrity - The licenses (that carry the rights by which the content is accessed) are encrypted and signed so that their integrity can be checked against unwanted manipulation.

Trust - The trust of the overall DRM system is given by the trust model it relies upon.

DRM systems are key to achieving secure content delivery for OTT services transmitted over any open network such as the internet. Secure OTT streaming uses adaptive bitrate (ABR) protocols, such as HTTP Live Streaming (HLS) and MPEG-DASH, to deliver multi-screen services to all kinds of video-enabled devices such as iOS and Android smartphones and tablets, PCs and Macs, smart TVs and streaming devices (such as Roku, Fire TV, Apple TV, and Chromecast).

DRM technology can be very flexible and may include business rules for secure download and offline playback, enabling a viewer on-the-go without internet access to enjoy subscribed content.

To learn more about DRM principles, please download our whitepaper [What is DRM](#).

How is DRM different from CAS?



CAS was designed to protect pay-TV content during transport from the digital video processing head-end (a.k.a. network operations center, or NOC) to STBs over various kinds of broadcast or “one-way” networks. DRM, on the other hand, is a broader asset protection mechanism that also safeguards content when at rest in addition to the transport phase, made possible by IP-based “two-way” networks such as the internet.

The first Conditional Access System (CAS) was designed during the mid ‘90s with the emergence of the MPEG-2 and Digital Video Broadcasting (DVB) standards, although there are also non-DVB CAS products from other vendors. DRM technology was developed during the end of the ‘90s although the majority of DRMs only came a decade later with the proliferation of the internet.

The role of a CAS is to provide key management and protect television transmissions over RF-based networks, such as satellite (DVB-S/DVB-S2 standards), terrestrial/over-the-air (DVB-T/T2), and cable (DVB-C/C2). The CAS design had to take into account that the transmission was “one-way” in nature, without any return channel from the STB back to the head-end. Because of the lack of a return channel, it was necessary to find ways to hide the “pay-TV secrets” in the STB, such as subscriber entitlements (“channel line-up”) and various keys used to access/decrypt entitlement management messages (EMM), and entitlement control messages (ECMs), holding the content encryption key required for the STB to decrypt the content. This led to the emergence of so-called smart cards (similar to chip-based credit cards) to store and protect those secrets. Removable smart cards turned out to be costly since they were subject to various forms of piracy, including smart card cloning, and have to be replaced every couple of years, typically at the expense of the pay-TV operator. For U.S. cable networks, CableCARD filled the same role. Later, various software-based CAS were offered, taking advantage of advanced STB system-on-a-chip technology.

Digital rights management (DRM) systems, on the other hand, were designed for IP-based, two-way networks, as exemplified by the internet. DRM technology takes advantage of the two-way nature of communication, which allows the receiver (STBs, mobile devices, PC/Macs, etc.) to request information (keys and licenses) from the head-end. Because of the two-way nature, DRM systems are inherently more flexible. This may include rules for how many times, or for how long time, specific content may be played back, and whether it can be copied to other

devices and even downloaded for offline playback, for example during travel.

With the rapid growth of video streamed (transmitted) over the internet using adaptive bitrate protocols such as those used by major OTT operators like Netflix and Hulu, OTT DRM technology has advanced to the forefront. CAS technology is gradually being phased out as broadcasters add on-demand services over IP and thus can take advantage of the two-way nature of IP-based networks. For today's OTT pay-TV operators, a [cloud-based multi-DRM service](#) is the best choice to achieve secure OTT streaming.

Effectively, DRM functionality is a superset of CAS. While CAS is generally limited to broadcast devices and it only applies to video/audio content, DRM protects content on any device with various distribution models (offline, online, with or without return channel), and can also be applied to other types of digital content such as e-books, bytecode, and more.

Two-way IP-based networks have of course also had a major impact on other technologies and services such as video analytics and addressable advertising.

For broadcasters with legacy CAS deployments and an intention to modernize the security infrastructure to support hybrid broadcast-OTT services, read the blog post [How DRM-based converged security reduces TCO of Broadcast TV](#).

How does a typical DRM license mechanism work?



When a viewer selects a program to watch, for example a movie that is protected by DRM, the user's media player will need DRM-specific licensing information in order to prepare the protected content for playback. Such information is managed and dispensed by a DRM license server, and DRM license management is the foundation for secure OTT streaming.

A DRM license is typically a small file that contains the content decryption key (in encrypted form) along with some rules/policies defining how the content may be used. Typical rules set in a license define the output controls (for example HDCP requirements) and/or license validity period. Like the encrypted content, the DRM license can be delivered freely and openly as the key itself is encrypted and the entire file is signed preventing any modifications to the specified rights.

Apart from the DRM license, a secure client is required in the receiving device, such as a smart TV. The secure client is responsible for evaluating the rules/policies contained in the DRM license. The client may be hardened via software and/or hardware against tampering (via white-box cryptography), and it is responsible for ensuring that the content decryption key is released only to trusted playback systems on the device. All major browsers and operating systems ship with a pre-integrated (native) trusted client.

The DRM licensing information sent to a client device equipped with Microsoft PlayReady will be different from what is sent to somebody using Google Widevine.

This is one reason why using a proven multi-DRM service is so important – the service is responsible for ensuring that the licensing information sent securely to each DRM system is in the format it expects. Other typical OTT DRMs are Apple Fairplay Streaming, and the long established Marlin DRM from Intertrust.

Even though the licensing information may differ from one DRM system to another, the core information always consists of several common pieces defining the business rules:

Content Key: The unique data used with an encryption algorithm to encrypt and decrypt the content. To maximize security, different keys should be used for different digital assets. It all forms part of a DRM system's key management strategy and mechanisms.

Playback Duration: A way to administer playback frequency, for example, "play any number of times during 48 hours" or, in the case of electronic sell-through, play forever

License Type: A "persistent license" means that no further DRM license requests will be required after the first one has been received, as opposed to sending a new license request each time the content is selected for playback

Output protection: Administering hardware output requirements ,for example. mandate the use of HDCP 2.x on external screens

Miscellaneous: For example, a hardware-secured DRM is required to enable playback

Learn more about [multi-DRM client compatibility](#)

How is DRM different from stand-alone AES encryption?



The short answer is that Advanced Encryption Standard (AES) is a widely used standard to encrypt data in banking transactions and medical records, as well as digital content such as music and video. AES can be used to encrypt the content by many content packing solutions. The associated encryption key can be delivered to the client by a DRM license acquisition protocol, or in the clear for Clear Key encryption supported by DASH and HLS.

For the purposes of pay-TV security for OTT streaming video services, only a DRM system can provide adequate protection of the content and service revenue. Major studios, whether “Hollywood” or others, will not accept just AES encryption (“Clear Key”) without a DRM for the distribution of their content. DRM technology is the basis for the kind of trust management that content providers require in order to license premium content to OTT operators. Let’s look at why that is the case.

When DASH or HLS protocols are used with Clear Key, the content is packaged and encrypted in a similar way as when a DRM is used. In other words, the single segments / chunks are encrypted with an 128-bit AES key. Although the encryption itself can be considered robust from a cryptographic point of view, the overall system can not. With Clear Key, the encryption key is delivered in the clear to the client, which means that anyone who gets hold of that key can decrypt the content using off-the shelf tools (such as openssl , Bento4 or a simple Python script).

When DRM is applied, the 128-bit AES key is delivered in a secure fashion. It is usually encrypted with a device public key whose secret part is handled by the DRM client in respect of the trust model rules it is compliant with.

With DRM systems, not only is the content encrypted but also the keys used for content encryption, decryption, and subscriber entitlements are protected. It is also part of the DRM system to support a DRM license management mechanism that ensures the delivery of DRM licenses only to authorized recipients.

This OTT DRM security mechanism extends to each stage of the content lifecycle, providing content protection during transit (as the content is encrypted) as well as while the content is present, or stored on a receiving device and ultimately when it

is used by the device. It is important to note that a DRM system is typically agnostic of the means used to deliver the content. By design, a DRM system allows the distribution of protected content and licenses over untrusted and open networks such as the internet.

DRM is the only kind of security mechanism that content providers will recognize, and the use of such a security system is a prerequisite for licensing of premium content. Only a DRM platform will be able to manage the pay-TV and OTT business rules, and it's DRM license server will instruct the DRM client what it may or may not perform, including secure download and offline playback. In other words, a DRM system is the foundation for secure OTT streaming.

Download our [free e-book](#) to learn more about securing advanced OTT video delivery with multi-DRM service, and read about secure offline streaming in this [quick guide](#).

How can I protect multi-screen OTT streaming and why are there several DRMs?



It is perhaps no surprise that the largest software companies went their own ways and developed proprietary OS-specific DRMs for Windows OS, iOS and Android OS. Today's DRM systems tend to be tied to the client device OS. Even though an OTT operator may need to support all DRMs to reach the broadest range of client devices such as mobile phones and tablets, PC/Mac computing platforms, smartTVs/STBs and games consoles, there are fortunately some commonalities that facilitate such support.

Here are the characteristics of the major DRMs, which incidentally are all supported by Intertrust's cloud-based ExpressPlay multi-DRM service:

Widevine Modular – Google's DRM technology is pre-integrated with Google Chrome, Chromium, Android mobile, STBs, and TVs.

FairPlay Streaming – Apple's DRM technology is pre-integrated with Safari and iOS devices.

Microsoft PlayReady – Microsoft's DRM technology is pre-integrated with Microsoft browsers, Windows OS as well as some smart TVs and STBs.

There are two more major DRMs:

Adobe Primetime – Adobe’s DRM technology can protect content and enable flexible business models for desktop (Windows, Mac), iOS, Android, Roku, Xbox and embedded device platforms.

Marlin DRM – An open-standard DRM system developed by four major CE manufacturers together with Intertrust. Intertrust provides Marlin DRM client SDKs for smart TVs, STBs, desktops, and mobile systems.

Learn more by reading [Which Cloud-Based Multi-DRM Service Enables High Performance Content Protection](#) and then check out the [multi-DRM client compatibility](#) matrix.

What is Marlin DRM and how is it different?



Understanding the future importance of secure and trusted digital content distribution, Intertrust became an early pioneer of digital rights management (DRM) technology in the late '90s. Intertrust teamed up with four of the largest consumer electronics (CE) manufacturers in the world: Panasonic, Philips, Samsung, and Sony. The result of this unprecedented collaboration was the 2005 release of Marlin DRM specification that would not only be applied for their own devices, but also could be adopted globally.

Since its launch, there have been many collaborations with device manufacturers, streaming services, and content rights holders. As a result, Marlin has become very popular globally. Companies worldwide are involved in Marlin's membership as partners, adopters, developers, and trusted service providers.

Marlin DRM protects digital assets on a variety of client devices in both online and offline content delivery models. It can also be applied to protect non-audiovisual assets such as e-books, bytecode, etc. For more details, read our quick guide [Using Marlin DRM to protect non-audiovisual assets](#).

The [Marlin Trust Management Organization](#) is responsible for granting commercial licenses for using Marlin and underpins the key management element of Marlin offerings.

Learn more about [Marlin DRM client compatibility](#)

What is MovieLabs and its Enhanced Content Protection specification?



Motion Picture Laboratories, Inc. ("MovieLabs") is a non-profit research and development joint venture founded by the six major motion picture studios: Paramount Pictures, Sony Pictures Entertainment, Twentieth Century Fox, Universal City Studios, Walt Disney Pictures and Television, and Warner Bros. Entertainment.

Tools for copyright infringement and piracy have advanced significantly over the years and with the introduction of Ultra HD (UHD) and High Dynamic Range (HDR) quality content, it was time to define an enhanced specification for protecting content against unlicensed use. In 2013, MovieLabs published a high-level specification defining the key elements that can serve as the basis for individual

studio protection requirements for new content distribution formats and platforms. The “MovieLabs Specification for Enhanced Content Protection” (ECP) was developed in conjunction with the “MovieLabs Specification for Next Generation Video.” [The latest version, 1.2, was published in August 2018.](#)

Each member company of MovieLabs shall decide independently the extent to which it will utilize, or require adherence to, these specifications.

How do set-top box chipsets enable protection of premium Ultra HD content? ↑

Two of the many requirements for a device to consume pay-TV Ultra HD content are to support content decryption, decoding and DRM license evaluation in the hardware and the Secure Video Path (SVP). In addition, service providers may be required to support watermarking, however, this may not have any impact on the device.

To meet the UHD security requirements, vendors of CE devices can license the hardware-based technology, or implement the content protection technology relying on the security framework that is available in the chipset used in their case. The latter is what DRM providers such as Intertrust, Google and Microsoft promote and support.

Modern chipsets enable the execution of Trusted Application (TA) in the so-called Trusted Execution Environment (TEE), which guarantees integrity protection and confidentiality for the code and the associated data loaded into it. Within the TEE, a TA that implements the DRM functionality, is able to securely perform all the necessary operations such as license evaluation, content key setting into the descrambler, HDCP engagement, and ultimately to interact with other subsystem a such the hardware descrambler and decoder.

As mentioned above the TEE represents a very suitable environment for handling protected content. A DRM vendor usually provides an SDK that allows the device maker to implement and integrate the DRM stack as part of their platform.

What is the difference between software-based and hardware-based security? ↑

For OTT and pay-TV streaming services, the video stream quality and screen resolution is usually the determining factor, whether software-based pay-TV security is deemed sufficient or a hardware-based security solution will be required. A flexible DRM system should be able to support both kinds. Ultimately, each studio decides on the security level required for each type of content, which will be the basis for content licensing to video service providers. Generally, the higher the video quality (going from SD to HD to Ultra HD), the more stringent the security requirements. The content release window also plays a role. For example, an older movie in HD will not have the same security requirements as an early-release movie with the same resolution.

For the lowest level of video stream quality such as standard definition (SD; 480p), a purely software-based DRM may be acceptable. For high definition content (HD; 720p and up and especially Ultra HD), a hardware-based security system will be required. Beyond hardware-secured DRM, additional security technologies may be specified. For example, the MovieLabs ECP specification calls for video watermarking for the highest content qualities.

Advanced security depends on the use of modern system-on-a-chips (SoC), which will provide protected environments where only DRM processing is permitted. A Trusted Execution Environment (TEE) is provided for the DRM to execute sensitive security processes, and for protecting secret keys and other data such as decrypted video frames. A software-based TEE may also be referred to as a Software Secure Element (SSE) or White-Box Cryptography (WBC).

Some SoCs have a TEE inside the chipset providing a closed-system for all secrets, decryption, and decoding operations. This provides the highest possible level of security, and prevents outside access. To compromise data and code running inside a chip is obviously significantly more difficult compared to a software-based approach.

There are too many considerations to describe here depending on the types of SoCs and receiver type, whether an Ultra HD smart TV or a low-resolution mobile device screen, etc. We invite you to [contact our team](#) for a no-obligation consultation to find the right solution for your needs.

Privacy Terms and Conditions

Copyright © 2024, MTMO. All rights reserved.