

# HOW TO TRUST ▶ YOUR PLAYER

Presented by



**BITMOVIN**

Friend MTS 

**intertrust**

## Building an OTT Service for Today's World: The Complete Series

Over the last several years, consumer viewing habits have been shifting from linear broadcast to over-the-top (OTT) platforms and streaming services. Just as viewing audiences are changing, so is piracy, and there's a lot at stake: content, revenue and brand – even investment in delivery infrastructure of systems, software, operations, and technical support. The impact of piracy on OTT streaming services is a direct and significant blow to the bottom line, but steps can be taken up front to secure your content and protect your revenue.

The “How to Trust Your Player” series presented here, walks through the ‘content distribution chain’, the importance of partner integration and the critical connection points in protecting content delivery from pirates through the implementation of multi-DRM services, hardening the player and watermarking/monitoring for the most technologically sound content protection strategy, so protecting content with technology, within and around the video player.

Also addressed is protecting content from your “players” – your audience, your subscribers. The human factor. What are they doing? This is often overlooked when creating a technical architecture of a streaming service but can provide insight when looking at the patterns of usage.

This 2020 article series culminating with a webinar, scratches the surface for OTT platforms and streaming services in providing best practices to develop secure content protection plans, making sure your users are as trustworthy as the technology you've implemented.


### TABLE OF CONTENTS

<b>Article 1</b> – Tips from the top: Secure Content Delivery and Playback	2
<b>Article 2</b> – Securing Content Access with Digital Rights Management Best Practices	5
<b>Article 3</b> – Tips and Tricks: How to Secure Your Content in Challenging Streaming Environments	13
<b>Article 4</b> – Beyond Digital Rights Management: Video Watermarking Weighs In	19
<b>Article 5</b> – From One End to the Other: Protecting Content From Origination to Playback, Once and for All	25

# HOW TO TRUST ▶ YOUR PLAYER

Presented by



Friend MTS 

intertrust

## Article 1 – Tips from the Top: Secure Content Delivery and Playback

Published date: August 20, 2020

*Joshua Shulman, Digital Marketing Specialist, Bitmovin*

*Alan Ogilvie, Lead Product Manager, Friend MTS*

*Ali Hodjat, Product Marketing Director, Intertrust*

### Overview of Over-the-Top (OTT) Platforms

Are you in the OTT world? You're not the only player in this business.

Over the last several years, consumer viewing habits have been shifting from linear broadcast to over-the-top (OTT) platforms and streaming services.

Along with a sudden increase in video consumption and in subscriptions to established OTT streaming services, several new OTT consumer streaming services have launched. Some of those have even adjusted their launch timelines to meet the increased consumer demand for unique content.

Developing the advanced technology needed for an OTT service is challenging. On top of that, companies today face the very real issue of securing content delivery and playback at a multi-player level. First is protecting the technology within your player – the consumer playback device. Beyond that, today's media and entertainment world faces the challenge of protecting your content from the ultimate "players": the potential bad actors, or pirates, at the end-user level. Skip a step and the market opportunities will quickly fade and disappear.

### The Shift in Content Consumption

Along with the surge in video consumption and streaming subscriptions, there is also a need to understand the corresponding change in OTT audiences, and what impact that has on your plans.

Before the pandemic began, a large portion of OTT streaming was live sports programming. When sporting events were put on hold, audience viewing shifted toward movies and other premium content. For example, a recent survey from **Altman Vilandrie & Company** showed that half of U.S. viewers are watching more TV and movies since COVID-19 started. Twenty-two percent of consumers are watching an additional five hours of TV or movies per week than they did before COVID-19.

That same survey found that approximately 60% of respondents said they are using a streaming video service. And the most recent projections from **Rethink Research** data show that changing behaviors during the lockdown period worldwide will result in an increase in subscriptions of almost 9% and an increase in revenue of almost 8%.

---

*Linked content is protected under the individual Privacy Policies and Terms & Conditions of the companies listed.*

©December 2020 Bitmovin Inc. All rights reserved. ©December 2020 Friend MTS Limited. All rights reserved. ©December 2020 Intertrust Technologies Corporation. All rights reserved.

### Evolving Piracy

These changes in viewing behaviors and streaming services have generated new content, subscribers, and services – and interest from content pirates. A recent report from **Parks Associates** finds that the value of pirate video services accessed by pay TV and non-pay TV consumers will exceed \$67 billion (USD) worldwide by 2023. Another report from **ABI Research** estimates that more than 17% of worldwide video streaming users access content illegally.

Just as viewing audiences are changing, so is piracy. Now, with the resumption of some sports leagues and live events, pirates who've gained a fitting in movies and other premium content will return to their sports stronghold as well. The current market situation means being continually on the lookout for ways to exploit weaknesses in delivery systems so that they can continue and resume, their illicit (but major revenue-generating) services. For OTT streaming services, it means a real potential blow to the bottom line.

### Protecting Your Bottom Line

Launching an OTT service is a complex, labor-intensive, and expensive venture. There are challenges in content acquisition, preparation, and delivery to your audience. Some may think about building a working video consumption environment as simply bolting a few complimentary services together: encoding audio/video, with packaging, for target devices; enabling a Digital Rights Management (DRM) service for license delivery; distributing assets through a Content Delivery Network (CDN); and setting up playback through a player framework.

Yet, all of that work can quickly become a waste of resources without the steps to protect content and revenue and fully combat piracy. Today, companies creating OTT services need to implement a nuanced approach that requires insight and diligence, especially when it comes to the communication between components, and the delivery of assets from content-preparation systems to consumers.

In the race to launch a service, with looming deadlines and high-value marketing programs providing no latitude for changes in go-live dates, companies often drop features from launch requirements. While this happens across the service delivery pipeline, the systems designed to protect a company's revenue lines through secure content delivery are often among the most frequent victims.

We've seen it happen time and time again. A large service launches with premium exclusive content, only to discover the same exclusive content appearing and being distributed through pirate services within hours. The good news: It doesn't have to happen to you. Take steps upfront to secure content, and you'll not only realize a timely return on your investment but see bottom-line numbers that would be impossible otherwise.

### OTT Service Tips and Best Practices From Industry Experts

This is the time to move swiftly, yet carefully and precisely. So, to help guide you in building and implementing an effective, protected OTT service, we've come together to share tips and best practices in a five-part article series. As partners, we've protected OTT content and revenue for media and entertainment companies across the globe. Now, we'll share our collective knowledge with you.

Following the best practices we outline will ensure that you are protecting your content from the technology side as well as the ultimate end-user side. You can make sure that your end users are as trustworthy as the technology you've implemented.

We'll show you how to secure the delivery of your content from origination all the way through to your end users via browser-based players. We'll walk you through the common mistakes companies make when securing access to content catalogs. We'll explain how and when multi-DRM service works, when and how watermarking comes into play, and how hardening the player all play a part in disrupting the redistribution of valuable content outside its legitimate intent.

## *Tips from the Top: Secure Content Delivery and Playback*

---

In discussing the challenges faced during implementation, testing, and delivery, we'll outline best practices for:

- Packaging high-value assets for secure delivery
- Securing and protecting DRM license acquisition workflow
- Authenticating user sessions before content delivery
- Configuring playback session concurrency and device limits
- Hardening the browser playback environment to mitigate attacks
- Forensic watermarking and active monitoring

In addition, we'll demonstrate a Reference Implementation using technology from each partner, addressing the best practices covered in the article series. By reviewing this best-practice implementation of multi-DRM services, watermarking, and hardening the player within a working demonstration environment – on a web browser – you'll clearly understand the process of delivering streaming media content from content through to a player device in the most secure and protective environment achievable.

---

To learn more, view the associated fireside chat.

**Video 1 – Tips from the Top: Secure Content Delivery and Playback**

# HOW TO TRUST ▶ YOUR PLAYER

Presented by

▶▶ BITMOVIN

Friend MTS

intertrust

## Article 2 – Securing Content Access with Digital Rights Management Best Practices

Published Date: September 1, 2020

*Ali Hodjat, Product Marketing Director, Intertrust*

*Nicolas Bredy, Senior Solutions Architect, Intertrust*

### Overview of Online Piracy and Digital Rights

As discussed in the first article of our series on “[How to Trust Your Player](#),” piracy is a big business, and leverages the same technology advances as legitimate OTT service operations in streaming and other components.

Globally, the volume of global OTT streaming has grown 63% between Q2 2019 and Q2 2020, according to a report from [Conviva](#), a leading supplier of video analytics technology. Similarly, total losses to piracy of streamed content worldwide are skyrocketing, impacting live and on-demand services alike. [Digital TV Research](#) projects that by 2022, global losses to online video piracy will reach \$51.6 billion – nearly double the amount lost in 2016.

### Piracy and Digital Rights Management

This article will provide an overview of digital rights management (DRM) license acquisition models, and recommended DRM best practices for leveraging a cloud-based DRM service to protect high-value streaming content. These practices are essential to:

- Maintain a secure interface for delivery of content keys to the encoder and packagers;
- Prevent attacks against the DRM license acquisition servers;
- Make sure only verified browsers and players can access the media and DRM license in different devices.

Consider that hackers have honed their technical skills to develop and adopt new ways of defeating defenses and responding to detection with new brands and sites. The least technically sophisticated approaches that pirates use to get around the robust protection of sophisticated DRM systems include high-quality camcording from 4K UHD TV displays. Advanced methods, similar to those of professional pirates, include high-bandwidth digital content protection (HDCP) strippers.

Other attacks target the multi-DRM service to extract the content keys, or exploit the DRM license acquisition server to circumnavigate license checking rules and retrieve DRM licenses. Pirates can also capture in-the-clear content from device memory as it awaits playback in the buffering process, in devices that don't support Trusted Execution Environment (TEE) and Secure Video Path (SVP). In some cases, if the same content keys and licenses are used for different resolutions, pirates will subscribe to the lower-quality content (e.g. SD resolution) and extract the keys to steal and redistribute higher-resolution – such as HD and 4K – variants of the content.

As we discuss and demonstrate DRM best practices in a real-world application (and reveal what a premium service should provide), portions of this article will refer to Intertrust's ExpressPlay DRM as an example of a cloud-based, multi-DRM service.

### Securing Content Encryption Key Acquisition

An integral part of content packaging is the insertion of DRM signaling in the media, such as the common encryption Protection System Specific Header (PSSH). Because the content packaging and playback workflows need to coordinate the DRM signaling and Content Encryption Keys (CEK), it is critical that the content packaging workflow and the multi-DRM system are tightly integrated. The content packager needs to retrieve the CEK from a multi-DRM service provider that manages these keys securely.

To maintain the security exchange of CEKs, Bitmovin encoders/packagegers and Intertrust ExpressPlay DRM have integrated the Secure Packager and Encoder Key Exchange (SPEKE) protocol, which enables secure retrieval of the encryption keys and DRM signaling from the ExpressPlay key store. The content protection industry has broadly adopted the SPEKE protocol. The protocol provides a simple and secure interface for delivery of CEKs and DRM signaling using a standard API that streamlines secure communications between the ExpressPlay DRM and encryptors, which in this case include encoders, packagegers, and origin servers.

### Preventing DRM License Acquisition Attacks

DRM technology is designed to protect the video content during transport, at rest, and during consumption. Although such technology can involve some very advanced security concepts, OTT streaming service operators still need to pay detailed attention to the overall system architecture that is deployed and avoid loopholes that allow hackers to defeat the purpose of DRM protected content.

In particular, the workflow for DRM license acquisition has to be thoughtfully designed. There are two deployment workflows that are typically used:

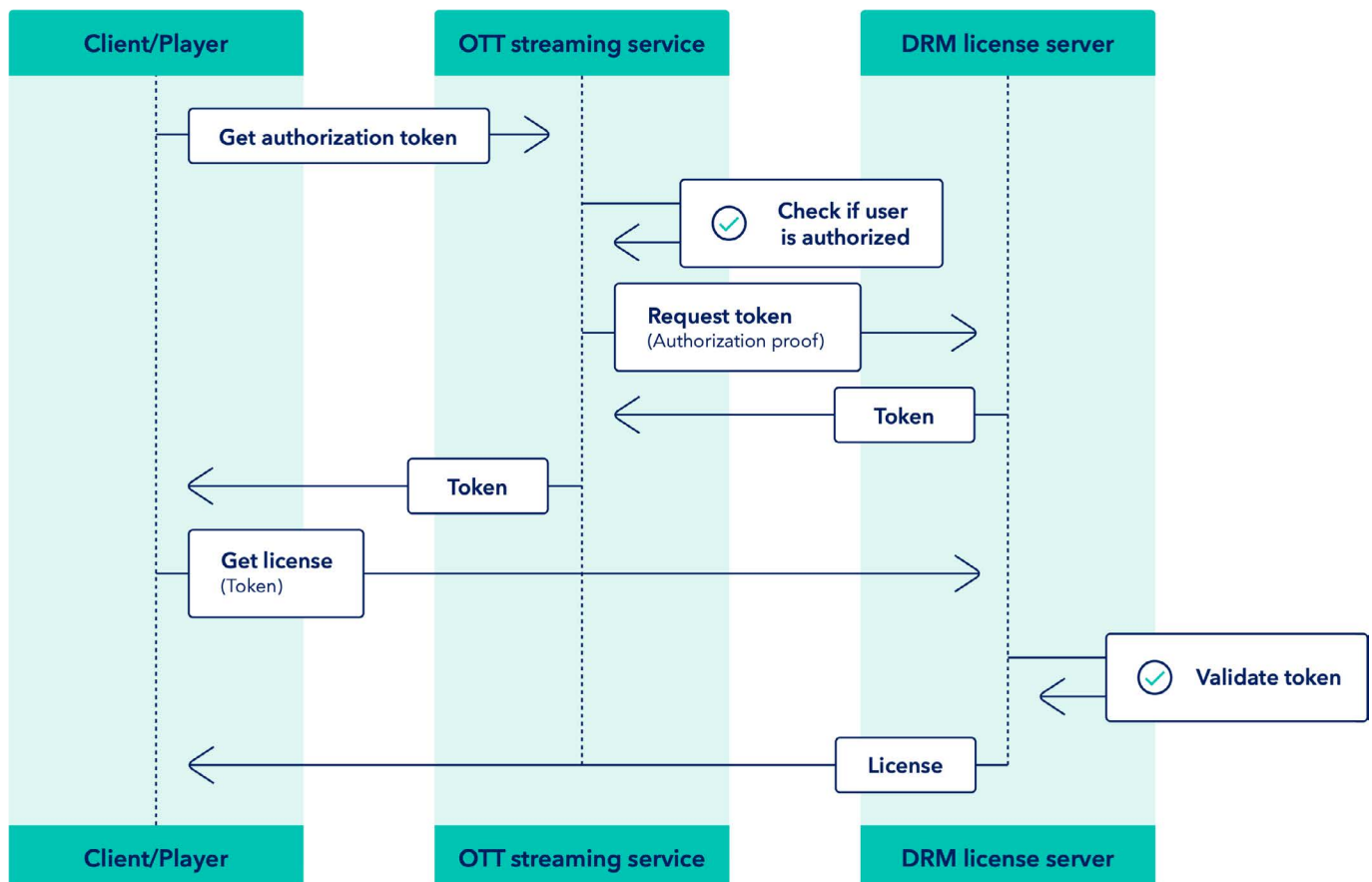
- **Direct license acquisition model:** In this workflow, the subscriber's device or player application communicates directly with the multi-DRM service (e.g. ExpressPlay DRM)
- **Proxy license acquisition model:** In this workflow, the subscriber's device and player application communicates with a proxy service managed by the OTT service provider, which redirects the requests back to the multi-DRM service (e.g. ExpressPlay DRM)

Moreover, similar to other professional cloud services, a typical multi-DRM workflow requires some form of authorization, which can be implemented by leveraging a secure token. A secure token enables a robust and secure mechanism to deliver several settings and parameters to the multi-DRM service. Secure token is encrypted to ensure confidentiality and includes digital signature to ensure integrity.

### Direct License Acquisition Model

This approach is also commonly referred to as an upfront token authentication workflow. Typically, a secure token is then used by the video player in the target device to perform a DRM license acquisition from the DRM license server. Once the DRM license server receives such a request, it can provide a DRM license that is bound to the requesting client device.

#### Workflow of the Direct License Acquisition Model



The workflow of this direct license acquisition model involves the following steps:

1. The OTT service provider receives a request for content, authorizes the user session, then triggers the generation of a secure token. This process is achieved by calling some ExpressPlay multi-DRM APIs and passing all the required parameters to create a DRM license, which includes an identifier of the CEK(s), and desired DRM license policies.
2. The ExpressPlay multi-DRM service returns a secure token, which is an encrypted, opaque data blob that contains all the information from the previous request.
3. The OTT service provider inserts the secure token in a DRM license acquisition URL, that is returned to the client application.
4. The client application initializes the media player with the DRM license acquisition URL, which triggers a DRM license acquisition call to the ExpressPlay multi-DRM service endpoint.
5. The ExpressPlay multi-DRM validates the secure token, then returns a DRM license with the requested settings.
6. The video player can start the playback of the encrypted video using the retrieved DRM license.

### Benefits and challenges of direct license acquisition model

The main benefits of the direct license acquisition model are:

- Using tokens for authorization of the client device is a simple method that is easy to deploy.
- The multi-DRM service provider (e.g. cloud-based ExpressPlay DRM service) will manage the authorization steps with the different DRM servers.
- The client devices only need to connect directly to the multi-DRM provider license servers and avoid connection with multiple DRM servers.

Since the secure token, also known as the DRM authorization token, is critical for generating and delivering the DRM license to the video player in the target device, a multi-DRM service should prevent attackers from reusing the DRM authorization token when they are not authorized to watch the content. Techniques available to achieving this goal include:

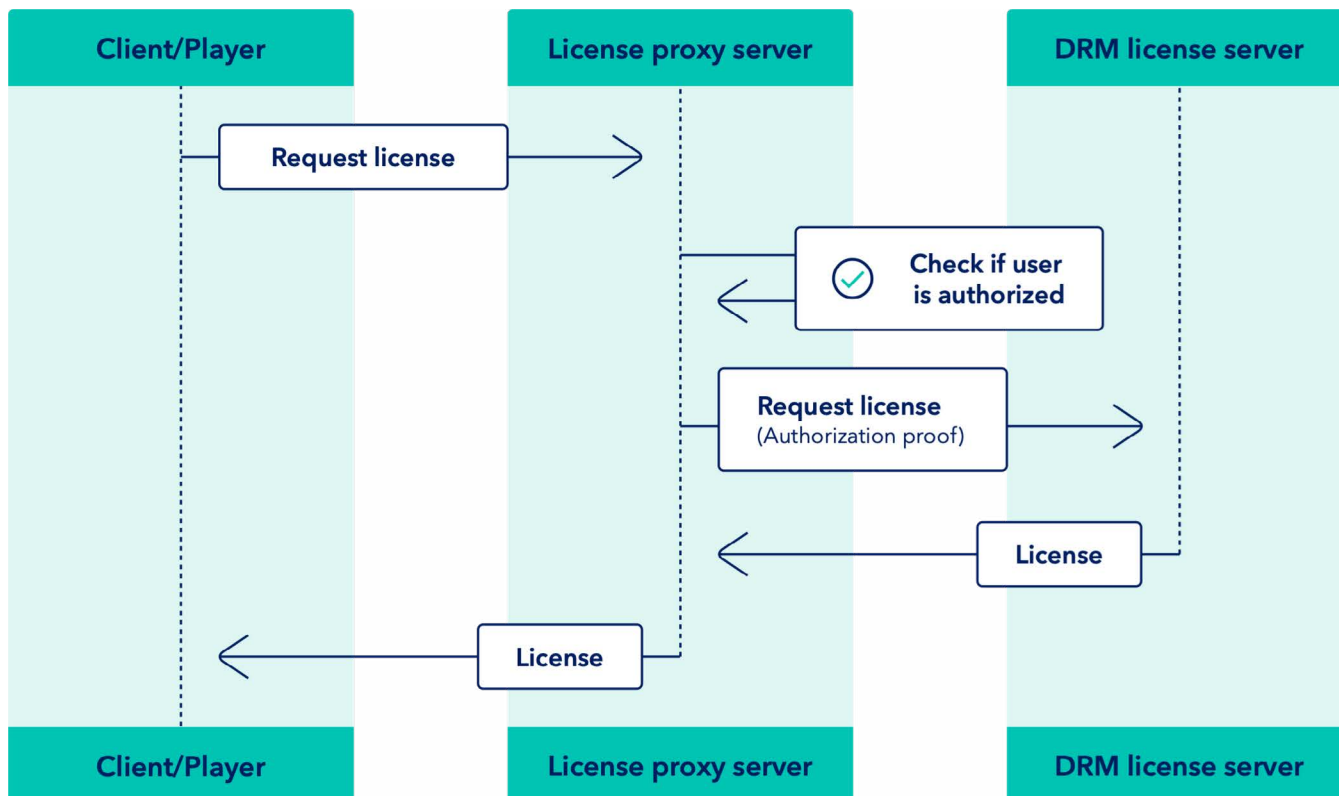
1. **Limit the lifespan of the DRM authorization token to a short specific duration.** In this approach the OTT service provider can define the lifespan of the token (e.g., 10 seconds) as one of the parameters sent to the ExpressPlay DRM service. Therefore, the client application will need to retrieve the DRM license before the token expires. This approach prevents an attacker from retrieving the DRM license from the multi-DRM service because the token is not valid after the set time period.
2. **Bind the DRM authorization token to some form of device identifier that will enable only the authorized device to retrieve the DRM license from the multi-DRM service.** In this approach, the OTT service provider will pass the device identifier to the ExpressPlay multi-DRM service as one of the parameters, and the token generated by ExpressPlay will include the device identifier. In the case of browser-based playback, this approach is not feasible because browsers do not expose a persistent unique identifier. Both of these methods are supported by ExpressPlay multi-DRM service.



### Proxy License Acquisition Model

A more advanced deployment DRM license acquisition can be accomplished through a DRM license proxy service, which enables the video player to directly communicate with an endpoint managed by the OTT streaming service provider (DRM license proxy). In this case, the streaming service provider retrieves a DRM license from the multi-DRM cloud service (e.g. ExpressPlay multi-DRM service) and there is no need for the video player to send a token directly to the multi-DRM cloud service for retrieving the license.

#### Workflow of Proxy License Acquisition Model



The workflow of this proxy license acquisition model involves the following steps:

1. The OTT service provider receives a request for content as a DRM license request, authorizes the user session, then forwards the license request to the ExpressPlay multi-DRM service along with the authorization proof. This request is managed by the license proxy server.
2. The ExpressPlay multi-DRM service validates the authorization proof and generates the DRM license using the requested settings. It returns the DRM license along with the requested policies to the license proxy server.
3. The license proxy server which is managed by the OTT service provider, will deliver the DRM license to the client device.
4. The video player can start the playback of the encrypted video using the retrieved DRM license.

### Benefits and Challenges of Proxy License Acquisition Model

The main benefits of the proxy license acquisition model are:

- DRM license server APIs are not directly exposed to client devices and media players; therefore, they are less prone to direct attacks.
- Help in reducing latency, because this approach requires only one API call (on average) by the video player to retrieve the DRM license. In contrast, the direct token-based license acquisition model requires at least two round-trip API calls between the device and multi-DRM service.
- OTT service providers can build additional authorization logic to control DRM license requests from the video player such as session bound license. For example:
  - » Binding DRM license, provided by ExpressPlay DRM service, to that particular user or viewing session
  - » Enforcing additional restrictions on the client requesting the DRM license, such as geographic location (geo-blocking), or that the request originates only from a legitimate client application (e.g. using the client's Origin header in case of browsers)
- Leveraging a simpler client-side logic that enables:
  - » Streamlining the DRM license acquisition workflow from the client-side application
  - » Ability to catch errors in retrieving the DRM license early on the DRM license proxy side
- Provides a robust framework to deploy scalable rotation of CEKs for live streaming.

When using the proxy license acquisition model, the OTT service provider is responsible for both scaling up the DRM proxy endpoint as the number of video player and device client requests increase, and for designing and implementing such DRM proxy service according to online services security best practices.

### Digital Rights Management Best Practices

On top of the deployment model considerations mentioned above, modern DRM schemes offer a wide range of content protection configurations, policies and restrictions applied to content, whether it is played on devices' internal screen or on external screens such as through an HDMI cable.

#### Multiple Content Encryption Keys

Best practices involve setting different CEKs for audio track as well as for each video resolution (e.g. SD, HD, UHD). This approach enables OTT streaming service providers to grant access to content distributed to different customers/different devices by delivering only the DRM licenses with CEKs for the authorized resolutions based on the consumer's subscription package.

Also, this allows the streaming service operator to fine-tune the DRM policies for each given resolution or track. For example, audio and SD content may not require enforcement of HDCP over an HDMI connection. However, an HD resolution may require HDCP 1.4 to be enforced, and 4K/UHD may require HDCP 2.2 to be enforced in the DRM license. We will cover additional considerations related to the use of HDCP in article four of the How to Trust Your Player series.

### Digital Rights Management Security Levels

DRM security level is a concept that defines the security tier of the DRM stack that is supported by the target device. Although different DRM schemes have different definitions of their security levels, there are two relevant distinctions in the security levels:

- **Software-based DRM client.** The DRM client implementation stack is mostly in software, usually protected with white-box cryptography solutions like whiteCryption for code protection and application shielding. The main examples of such security levels are PlayReady Security Level 2000 (SL2000) and Widevine Level 3 (L3).
- **Hardware-based DRM client.** The DRM client implementation stack leverages a Trusted Execution Environment (TEE) on the target device. Such implementations involve the decrypted media to be processed through a Secure Video Path (SVP) without it leaving the secure environment provided by the device hardware and TEE. The main examples of such security levels are PlayReady Security Level 3000 (SL3000) and Widevine Level 1 (L1).

Using the right DRM security level allows OTT streaming service providers to map the required security level for each given resolution or track. For example, audio and SD content may only require a “software-based DRM client,” whereas HD and 4K/UHD may require a “hardware-based DRM client” to be enforced.

In the case of 4K/UHD, there will be additional requirements from the Enhanced Content Protection (ECP) specification by Movielabs (an entity owned by several Hollywood studios). Leveraging the right DRM security level is particularly important because audio codecs are usually implemented in software, and cannot be enforced through “hardware-based DRM clients.”

### Widevine Verified Media Path (VMP)

Another important digital rights management best practice is related to the Verified Media Path (VMP) requirement enforced by Google Widevine DRM. This process is specifically relevant when a browser-based video player is used to decrypt Widevine protected content. The W3C Encrypted Media Extension (EME) specification defines the interfaces that web applications can use for provisioning the browser’s media stack with the DRM license required to play protected content.

A critical module of the EME specification is a trusted component that evaluates the rules specified in the DRM license and ensures the content key is handled securely. This component is known as the Content Decryption Module (CDM). Once the media is decrypted by the CDM, it is essential that the browser securely processes the decrypted media.

When the browser uses a native DRM client, at the start of video playback, decrypting media will be through a Secure Video Path (SVP), and it can enforce “Hardware-based DRM client.” When the browser is not using the native DRM client, the CDM is mostly using “Software-based DRM client.” This is the typical situation for Chrome or Firefox browsers running on desktops computers. In these cases, the Widevine desktop browser CDM includes support for VMP, a feature that ensures Widevine has sanctioned the browser media processing implementation.

In the past few years, Google has deprecated all CDM versions that do not contain VMP functionality and is now mandating VMP for all browser CDM implementations to stay current with the stable Chrome releases. This action ensures that the latest updates are applied and that they support the latest APIs. More recently, Google also adopted a policy of strictly enforcing the VMP requirement which means Widevine license servers by default can only issue licenses for CDMs that support the VMP feature.

## Securing Content Access with Digital Rights Management Best Practices

---

These best practices are crucial when using Widevine DRM:

- OTT streaming service operators need to instruct the subscribers to update their browser and related components (e.g., CDM) to the latest version. This is usually done seamlessly for browsers on Mac OS X and Windows. However, this automatic update is not always successful. Consequently, some users are unwittingly using a Chrome browser version with a deprecated CDM that does not support the VMP feature. They will not be able to play Widevine-protected content.
- For desktop Linux browsers that do not support VMP, it is possible to override the default Widevine license server behavior by specifying a dedicated flag, and still issue a license to grant playback. ExpressPlay DRM service will provide a mechanism to override the default Widevine license server if needed.

## Combating Online Piracy with Digital Rights Management

Pirates have continued to evolve their technical skills to develop new methods and are now leveraging the same advances in streaming technology used by legitimate OTT service providers. To combat the increasing number of piracy attacks, streaming service operators must follow DRM best practices to block the loopholes that hackers otherwise may use to defeat the purpose of DRM technology.

When leveraging a cloud-based DRM service, it is essential to follow the correct DRM license acquisition workflow, maintain a secure interface for delivery of content keys, and take advantage of DRM security levels and multiple content encryption keys.

---

To learn more, view the associated fireside chat.

[Video 2 - Securing Content Access with Digital Rights Management Best Practices](#)

# 3

## HOW TO TRUST ▶ YOUR PLAYER

Presented by

▶▶ BITMOVIN

FriendMTS

intertrust

### Article 3 – Tips and Tricks: How to Secure Your Content in Challenging Streaming Environments

Published Date: October 6, 2020

*Joshua Shulman, Digital Marketing Specialist, Bitmovin*

Piracy occurs at all levels of video streaming, from illegal downloads to screen captures. How can an OTT provider overcome these issues? Fortunately, there's a good answer: with a mixed balance of back-end solutions including digital rights management (DRM), watermarking, and/or client-hardening. As a part of a multi-post series between partners Bitmovin, FriendMTS, and Intertrust Technologies, Bitmovin is here to define some of the top tips and tricks to implementing these solutions into your web-based player.

By the time content arrives at a web-based player, a majority of protection measures should already be in place. Although it's possible to arrive at the player without a concrete DRM, watermarking, and/or client-hardening solution, this is ill-advised, as not all consumer players can be trustworthy enough to simply view content without engaging in some kind of piracy measures.

#### How to Secure Video Streaming Content in Web-Based Environments

The browser environment, open by default, is a challenging environment to secure. Delivering high-value premium content to a web browser can be a risky venture, but one that is critical to reach your audience. To reach a maximum audience, the recommendation is to implement a player in as many devices as possible, including app-first or native solutions. Browser environments are amongst the farthest reaching, but least secure, due to their open nature, and will require some extra attention when implementing content protection systems.

Content licensors (or content owners) are increasingly wary of the impact of content theft at user playback, and will often mandate use of certain obfuscation techniques as part of authentication and authorization flows. **As the second article in our "How To Trust Your Player" series highlights**, ensuring that session authorization tokens are securely ciphered, and can prevent attacks against DRM license acquisition servers is critical to developing a truly end-to-end security chain.

For the browser playback environment where website code (JavaScript) is interpreted and executed, masking how to interact with security systems in place is a critical step. This typically takes place through the use of a code obfuscation tool. The goal of this type of tool is to render the source code unintelligible to prying eyes without fundamentally altering how it functions.

Obfuscation entails parsing JavaScript (JS) source code, rearranging the code, and at some points, transforming it by renaming variables and data structures, and refactoring logic structures to mask algorithms. This makes it nearly impossible to understand the code and how data is parsed by it. The result is code that is extremely difficult to read and reverse-engineer, either by a tinker or a more determined actor...such as a content pirate.

### How to Bolster Your Video Streaming Defenses

Techniques such as uglify-ing or minify-ing JS code provide some minimal defenses, but can be reverse-engineered themselves through automated tooling. While it may not be possible to get back to the original source, it is possible to generate much more intelligible code from tools such as a JS beautifier, from which a hacker could discern information beneficial to attacking your code or services.

#### Improving on Obfuscation

JavaScript protection solutions, such as **Jscrambler**, provide significant robustness by generating code with polymorphic obfuscation techniques. On top of this obfuscation, code locks are added to restrict the browsers and platforms on which the code can be executed, providing the ability to restrict the code use to a specific user session. They also aid in the generation of self-defending code, where anti-tampering techniques protect functions and objects. These anti-tampering techniques can trigger defenses (such as halting execution and throwing fatal errors), or generate session invalidation events that trigger a service block for future HTTP requests to your security services.

As your code has to execute on a web browser, following open JS standards, it just is not possible to completely secure playback. Obfuscation products are not a foolproof mechanism to create a secure execution environment. Someone with enough motivation, and time to spend gathering intelligence and doing research, will eventually be able to reverse engineer your playback code. However, putting in place multiple layers of JavaScript code obfuscation as part of a complete defense strategy will deter attacks from content pirates.

#### Concurrency Management

Many content owners require OTT service providers to limit account oversharing – the number of simultaneous video views that can take place from a single authenticated and authorised user account. While this is primarily to ensure that a household's stream concurrency or device limits are not exceeded, this has the effect of limiting the impact of credential sharing outside of the user's household. Concurrency management typically takes place by keeping a tally of the number of play/pause/stop events that the player framework's analytics data generates.

Below is a standard tally-event measurement system that measures users "Alice" and "Bob" based on overlapping timestamps of video views in similar geographic locations. ("P" indicates a video pause.) Although this helps monitor general concurrent usage across shared accounts, this method has its limitations.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Alice			1	1	1	1	P	P	P	1	1	1	1	1	
Bob					1	1	1	1	1	1	1				
Concurrent	0	0	1	1	2	2	1	1	1	2	2	1	1	1	0

*Concurrent management tally sample*

One is that this method often is not robust enough to limit concurrency. This is because the analytics events can be intercepted and blocked – and are not explicitly tied to a service’s DRM license issuance, and the user’s entitlement store or rights locker. A better practice is to include heartbeat messaging, driven from the player’s message bus with the playhead timeline position (or an offset for VoD), that ties to a specific user’s session. When a stream entitlement check takes place as part of DRM license issuance, a heartbeat identifier should be set, tied to the user’s session, cryptographically signed, and then passed to the player as the heartbeat token.

On playback start, and until the end of the session, the player should communicate with the heartbeat service at a predetermined interval to exchange the heartbeat token. At exchange of a valid heartbeat token, the heartbeat service would respond with the next/refresh token, and the user’s stream entitlement within the user store would be tallied. If the heartbeat token is not validated within the predetermined interval (+/- n seconds), then the heartbeat service would remove the user’s entitlement to play back the content. This, in effect, would remove the ability for the user’s session to obtain further DRM licenses until the session had been reset.

When receiving an error from the heartbeat service, the player (through the heartbeat customisation) should invoke the player “stop” functions to tear down the session.

### Domain Locking

Whereas concurrency management is a method of monitoring how many users are viewing the same account, domain locking is essentially a technique to white or blacklist certain websites. It will prevent a player from being embedded on a non-approved site, such as one on which an aggregator might want it to look like they have content available – but in reality are embedding another service’s player.

Bitmovin’s web-based player, as part of the standard security controls, uses an allowlist for player licensing to prevent misuse. The top-level domain name or host for which the player can be used must be added within the “Player – Licenses” section of the **dashboard** by selecting “+ Domain” before deploying a player.

The screenshot displays the Bitmovin player dashboard. On the left is a navigation sidebar with the following items: Dashboard, ENCODING, PLAYER, Licenses (highlighted with a red box), Billing Statistics, ANALYTICS, Discover, Organization Settings, Contact Support (with a 'New' badge), Getting Started, and SDKs. The main content area is titled 'PLAYER / LICENSES / License default-license'. It shows details for a license named 'default-license', including a Player Key, Impressions (18/5000), and Analytics (Enabled). Below this is a section titled 'Domains / Package Names / Bundle Identifiers' (also highlighted with a red box). This section contains a table with two entries: 'example.com' and a blurred entry, each with a trash icon. At the bottom of this section is a form to 'Add Domains / Package Names / Bundle Identifiers' with a text input field containing 'example.com(, exa...)' and a '+ Add' button. A note below the form states: 'It can take several minutes for license changes to take effect.'

*Bitmovin player dashboard*



From this page, it is also possible to add IP address ranges to indicate where the player can be licensed, which can be useful during testing. Localhost is allowed by default. For the mobile/device software development kits (SDKs), the allowlist may also contain the package name and/or bundle ID. In the case of the Roku device, the dev.roku domain is mandatory, along with the Roku channel ID.

Once you've secured your **distribution chain from source to the playback environment**, and have followed best practices to secure the playback experience as much as possible (as above), it's imperative that you follow these rules to boost your users' experience – and ultimately, your brand.

## Rules to Gaining and Retaining Trustworthy Video Players

### 1. Make your content available where your users want to watch it

Combining Bitmovin's encoding and packaging solution to prepare the content for delivery, the robust ExpressPlay DRM system provided by Intertrust to protect delivery, and Bitmovin's Player, it is possible to support a wide range of browser versions and devices to reach your audience.

Bitmovin's multiplayer SDKs streamline the development by bringing your apps to all of the platforms your users would be willing to pay to watch it on – e.g., Smart TV, tablet or mobile device (iOS, Android, etc.). You can find information on the Bitmovin SDK and how to implement it in its **documentation**.

You can also view **all devices and apps supported by the web player**.

### (Web SDK) DRM Support on Desktop Devices

Browser	Minimum OS Version	DASH ClearKey	DASH Widevine	DASH/SMOOTH/HLS PlayReady	HLS AES128	HLS Widevine	HLS FairPlay
Chrome (last 3 major versions)	OS versions supported by Chrome	✓	✓	-	✓	✓	-
Firefox (last 3 major versions)	OS versions supported by Firefox	✓	✓	-	✓	✓	-
Opera (last 3 major versions)	OS versions supported by Opera	✓	✓	-	✓	✓	-
Safari 10+	macOS Sierra	✗	-	-	✓	-	✓
MS Edge (last 3 major versions)	Windows 10	✓	-	✓	✓	-	-
MS Edge (Chromium) (last 3 major versions)	Windows 7 / macOS 10.12	✓	✓	-	✓	✓	-
MS Edge (Chromium) (last 3 major versions)	Windows 8.1	✓	✓	✓	✓	✓	-
Internet Explorer 11	Windows 8.1	✓	-	✓	✓	-	-
Internet Explorer 11	Windows 7 (Adobe Flash required)	✓	-	-	✓	-	-

*DRM Systems supported by the Bitmovin Web Player*

### **2. Feature parity with piracy**

Create an impactful and feature-rich player that improves the viewer's quality of experience. Don't punish legit users by restricting how they view their content, such as with **offline play**, time to release and overall quality. In some cases, legitimate content just is not available in high enough resolution, whereas pirated content might offer 4K quality.

### **3. Provide your content at a reasonable price point**

Bitmovin's player SDK enables an OTT provider to spend less time developing workflows for each potential player implementation by reducing workflow cost with easy-to-use configurations.

## **Summary: How to Secure Video Streaming**

The combination of these three rules creates a more favorable user experience than what content pirates can provide. Yet, there is one last problem to overcome once your player is ready: re-streamed content. This is where an effective watermarking service comes in. Not only will it detect, deter and disable leaks, it will work to create a frustrating experience for illegitimate viewers and encourage them to use more legitimate means of consuming content.

***Make it harder to pirate content, but easier to pay for content***

---

To learn more, view the associated fireside chat.

**Video 3 – Tips and Tricks: How to Secure Your Content in Challenging Streaming Environments**

# 4 HOW TO TRUST ▶ YOUR PLAYER

Presented by



Friend MTS

intertrust

## Article 4 – Beyond Digital Rights Management: Video Watermarking Weighs In

Published Date: October 23, 2020

*Alan Ogilvie, Lead Product Manager, Friend MTS*

*Andy Wilson, Senior Product Architect, Friend MTS*

*Chris O'Brien, Engineering Manager, Friend MTS*

In the continually evolving OTT world, we've established that savvy pirates are implementing new and advanced methods to steal valuable content – to the tune of **more than \$67 billion** (USD) in value by 2023. Another report from **ABI Research** estimates that more than 17% of worldwide video streaming users access content illegally.

We also know that launching an OTT service is costly, resource-intensive and complicated. Getting it right is critical. Beyond building the video consumption environment and content acquisition, companies must incorporate up-to-date content protection methods. In this “How to Trust Your Player” series, we've learned about **Digital Rights Management (DRM) from Intertrust Technologies**, and about content packaging, license acquisition models – and **best practices for implementation within the video player environment from Bitmovin**.

### Understanding Content Protection

But what about the other players? They are the users, the consumers of all this valuable content. To ensure content protection among these players, we have to look at watermarking. Working together with OTT services throughout the world, we have seen how companies are working hard to protect their content at the front end with DRM, but are not commonly implementing readily accessible, advanced watermarking techniques to protect the content once it reaches the end user.

As a result, they are risking subscriber loyalty, growth, and revenue by not covering the last hole in the content delivery system. This scenario is one case where the overused “end-to-end” term is applicable: OTT companies must protect their content end to end in order to truly protect their content and revenue.

### Protection Beyond DRM

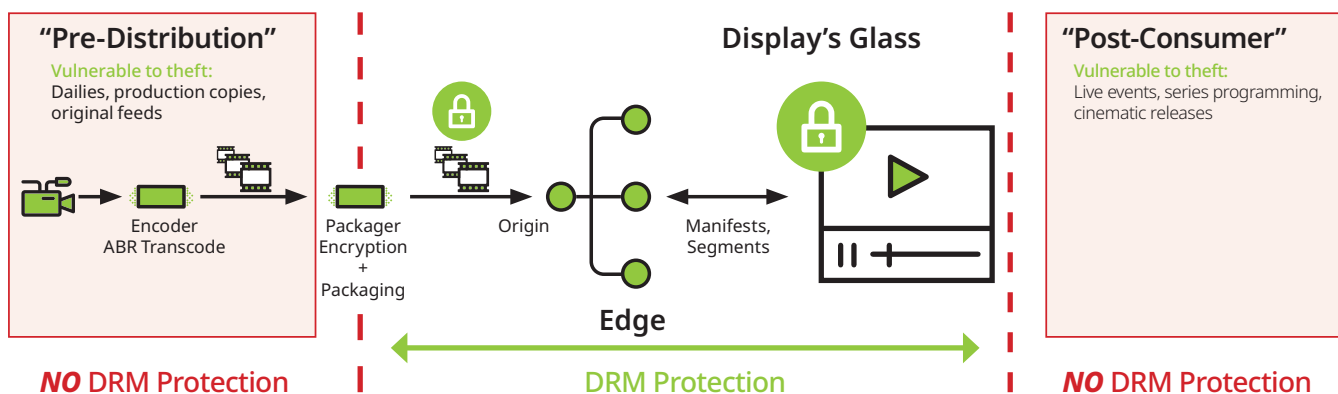
So what's an OTT service provider to do?

We know that DRM is absolutely necessary in this journey, and needs careful, considered implementation. As Intertrust pointed out in its article, "[Securing Content Access with Digital Rights Management Best Practices](#)", recommended DRM best practices are essential to:

- Maintain a secure interface for delivery of content keys to the encoder and packagers;
- Secure session tokens for authentication and authorisation;
- Prevent attacks against the DRM license acquisition servers;
- Make sure only verified browsers and players can access the media and DRM license in different devices.

A default option for any premium content service provider, DRM is designed to protect audio/video content during transit to the consumer's player. As discussed in the above-mentioned article, DRM manages the robust content encryption key exchange between the secured playback device (the player) and the license service. DRM is also responsible for setting usage policies for the content, and for enforcing this within the playback environment. However, once the material has started playing, a new threat emerges – the consumer. A common misconception is that playback devices are secure.

DRM can do little to isolate pirated content, or identify the wrongdoers, when content is stolen and made freely available. Once content arrives at its intended legitimate destination, DRM can do nothing to stop it from being redistributed by those who have no rights to do so. The crux of the problem is that DRM protects only the legitimate path from origination to the point of consumption.



See "[Beyond DRM: The Complete Content Protection Story](#)," for further details.

It's also important to understand that practices to curb sharing and theft of credentials (such as passwords) do not help reduce the distribution of content once it has escaped the boundaries of a video service.

In short, DRM is a key part of any rigorous approach to piracy defence. But if we want to talk about end-to-end protection, there's more.

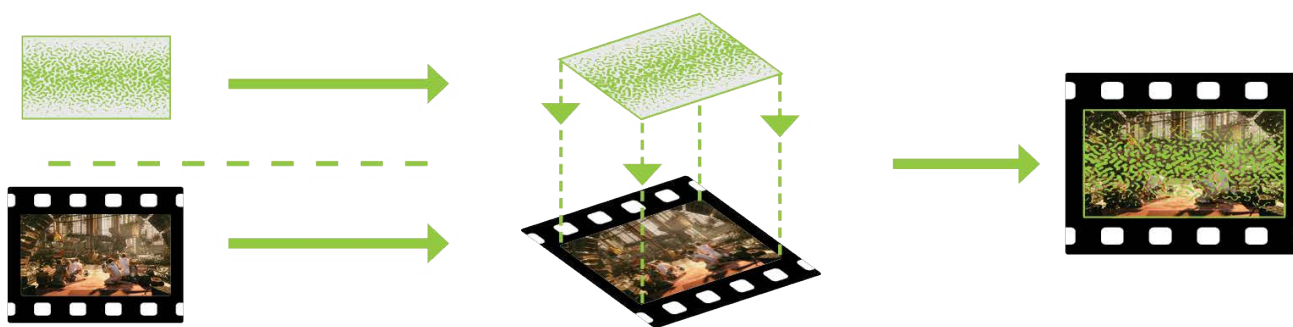
### Enter Video Watermarking

To protect the value of video content – whether original or rights-managed – outside of these legitimate service boundaries, you'll need to identify the video itself. Specifically, you'll need information to confirm its outermost point of legitimate use. With that, you can identify the “bad actors”: the infringing users and industrial-scale pirates.

To accomplish this, video providers can embed information into the video itself, at the point of origin, in the Content Distribution Network (CDN) during distribution, or within the player device. Information might include the device IP address, session details, and subscriber identifier.

The most effective way to do it? Client-composited (client-side) watermarking. It's clever, as consumers can't see the watermarks. Only automated analysis can.

Client-composited watermarking occurs within the consumer device. The embedded player accesses a software library database that replies with a unique identifier. The watermark information is converted into a pattern, similar in concept to a QR code, and then is “composited” with the video via an overlay.



Source: Friend MTS. Image source: frames from (CC) [Blender Foundation](#)

Client-composited watermarking is fast. Time to detection of content theft can be as little as a few seconds – important for any service, but particularly so for live sporting events. It's also lower in cost than other watermarking options, such as A/B watermarking.

For a more thorough discussion of watermarking methods, their advantages and disadvantages, see our [“Subscriber Watermarking Technologies – White Paper Quick Facts.”](#)

### Best Practices in Video Watermarking: Detect, Deter, Disable

No matter which way you go with watermarking, you must keep the end goals in mind: to deter piracy, detect it when it occurs, and disable the source of the pirated content. The truth is that embedding watermarks alone is not very helpful unless there is a way to use the watermarks to find stolen video content, identify its source, and take appropriate action. Herein lies the hallmark of a robust watermarking solution.

*Detecting* involves monitoring suspected pirate outlets, and then matching the digital “fingerprint” of a suspected piece of content with a reference fingerprint that generates during the production process. Then, advanced watermarking analysis can see the identifying watermark and extract the information that it contains.

*Determent* is about defending against pirate “attacks.” To reduce the chances that an instance of stolen content could be traced back to its last legitimate distribution end point (or to the pirates themselves), content thieves may try to make the watermark unreadable by applying “transformations” to the content. These “attacks” make the watermark no longer available or readable. However, a strong, advanced watermarking program has a far better chance of surviving these attacks and remaining readable.

*Disabling* is about treating the incident after determining the identity of a pirated video stream. This can include direct actions against the pirate, ranging from take-down notices to reporting to law enforcement. Typically, video providers take actions against subscribers whose accounts they detect to be re-streaming. Those actions might be interrupting the session, requiring the user to re-enter access credentials, suspending the end user's account, disallowing the use of the device on the account, or even initiating legal action.

### Choosing a Watermarking Service

What do you want from your watermarking service? What *should* you want from your watermarking service?

#### Deployment

How widely deployed is the service? How many set-top boxes and OTT players is it securing around the globe? In the OTT world, and in the content protection world, experience does count. Make sure you are getting a system with a proven, demonstrable track record in detecting, deterring and disabling piracy across multiple illegal redistribution channels.

#### Strength Against Attacks

OTT players need to choose a watermarking service that is effective. How effective? Ask the provider for details. At Friend MTS, we know that our Advanced Subscriber Identification (**ASiD**) service has remained secure against every attack made to date in both broadcast and OTT environments.

Keep in mind that staying abreast of attacks is a constantly changing process. Your watermarking provider has to not only keep up with the latest pirate schemes, but stay ahead of them. Those bad actors are clever, and don't always appear "bad" on the surface. In general, they use a legitimate subscription and easily available screen recording software for screen scraping – or even \$10 (USD) switches that can remove HDCP. Commercial pirate distributors can easily capture video output, then re-encode and redistribute the premium video using their own infrastructure to monetise stolen content.

Fragmentation of content – which happens when consumers need to subscribe to more than one streaming service to get access to all the content they want to watch – makes it even harder for legitimate content owners and providers to compete with illegal subscription services. These pirate content aggregators, not restricted by licensing agreements, monetise stolen content by offering the end user a one-stop shop for the best sports and entertainment programming.

Be sure the service you are considering is highly adaptable to ever-evolving pirate attacks.

#### Speed

As explained, client-composited watermarking will provide the fastest identification of piracy. If you're dealing with live sports and entertainment, pay-per-view, and on-demand content, this factor should play an important part in your decision on the type of watermarking system to deploy. Think about it in these terms: Several years ago, a major broadcaster – the original source for 60% of the sports channel piracy in its market – introduced ASiD. OTT piracy reduced to less than 1% within weeks.

#### Global Reach

With today's technology and the speed of the Internet, OTT players will need to protect content in markets throughout the world. Even if you are servicing customers in one country or on one continent, remember that content thieves can and do act without physical borders.

### Multi-CDN Service

Some watermarking mechanisms may incur additional charges to support multi-CDN usage. Since OTT services have enough expense and complexity, know that it is possible to find a robust service that incurs no additional expenses for multi-CDN content delivery.

Every OTT operator will have its own criteria, but the bottom line is to carefully select a watermarking service that is cost-effective and results-driven.

### Understanding the Human Factor

One of the most challenging aspects in securing an OTT service is the understanding of the human factor in content protection: the end users who are consuming content.

It is essential to start at a level of zero trust, assuming that some users of your service will attempt to circumvent security controls or use your service in a way you didn't intend. This could mean something as simple as sharing their credentials with family or friends, or a more direct attack against your content security systems by bypassing/overcoming licensing restrictions.

To overcome this challenge, understand that the point of zero trust begins as early as sign-up to your service. Protection steps include validation of the presented user profile, location checks, payment fraud detection (such as comparison with other existing users), and enforcement of a suitably complex password with multi-factor authentication to prevent brute force attacks.

### Video Viewer Personas

Errant or undesired behavior within your service can typically be broken down into the following personas.

#### The Over-Consumer

Running an OTT service is expensive. The cost of delivering compressed video to your consumers is one of the most costly aspects, even with high competition driving CDN pricing down. Your service pricing and tiers model against costs, and per-user delivery/CDN cost – driven by view time per user session – is a major factor. Is a user's consumption patterns far more than your predicted model suggests? That could indicate the "over-consumer".

#### The Frequent Mover

Here, an authenticated and authorised user's sessions change IP addresses frequently in a short period of time, spanning multiple geographies. This is a good indication of a compromised account, with multiple users accessing the service unbeknown to the legitimate account holder.

#### The Account Sharer

The Account Sharer is characterised by multiple authentication authorisations over time, with different IP addresses/ISPs, and possibly different geographies. As with the Frequent Mover, this pattern could indicate a compromised account. But, it is also possible that a legitimate user has shared their credentials with friends and family – or worse, with a much wider group.

#### The Out-of-Bounds Viewer

In this case, the user viewing the content is outside of a designated geographic area. Initial authorisation attempts may have been genuine, but other data sources may reveal the user's true location.

#### The Anonymous IP Viewer

The Anonymous IP Viewer's traffic comes from a suspected, or known, proxy/VPN, or a suspect network source (i.e. cloud infrastructure vendor, rather than ISP).

### **The Long Viewer**

This user watches only live channels, for very long periods in one session.

### **The Tamperer**

The Tamperer's session data indicates tampering with the playback environment. Tamper warnings from the code obfuscation solution may have fired. Session token data mismatches may have been logged. You may also see multiple authorisation attempts, and multiple content license request attempts for a single use token.

From sign-up forward, every component within your service should provide user behaviour monitoring to aid in identification of patterns that could indicate fraudulent or suspicious activity. This analysis is important to protect your interests under the terms of your content licensing deals – and critically important for revenue protection.

## **Using Watermarks for End-to-End Protection**

To combat the increasing number of piracy attacks, OTT services must implement solid watermarking and detection as well as DRM. There's a lot at stake: content, revenue and brand – and even investment in delivery infrastructure of systems, software, operations, and technical support.

Start by developing and enhancing understanding of the full content protection strategy, and continue with following the considerations and best practices we've outlined to choose and implement a watermarking service. Only then can you make sure that your players – from one end to the other – are as trustworthy as the technology you've implemented.

---

To learn more, view the associated fireside chat.

[Video 4 – Beyond Digital Rights Management: Video Watermarking Weighs In](#)



# HOW TO TRUST ▶ YOUR PLAYER

Presented by

▶▶ BITMOVIN

Friend MTS

intertrust

## Article 5 – From One End to the Other: Protecting Content From Origination to Playback, Once and for All

Published Date: November 12, 2020

*Joshua Shulman, Digital Marketing Specialist, Bitmovin*

*Alan Ogilvie, Lead Product Manager, Friend MTS*

*Ali Hodjat, Product Marketing Director, Intertrust Technologies*

Any player in the OTT world would have a hard time keeping up with the myriad of changes we have seen over the past several months: COVID-19. The dramatic increase in video consumption. The exponential rise in subscriptions to established OTT streaming services. New OTT streaming services. PVOD. Fragmentation of content. But enter the other player – the content pirate – and things become even more complicated.

As we reviewed in our [first article](#), the stakes are high – very high. A recent report from [Parks Associates](#) finds that the value of pirate video services accessed by pay-TV and non-pay TV consumers will exceed \$67 billion (USD) worldwide by 2023. Another report from [ABI Research](#) estimates that more than 17% of worldwide video streaming users access content illegally. The impact on OTT streaming services is a direct and significant blow to the bottom line.

### Securing OTT Content

To stay alive in this environment, OTT companies have no choice but to secure content delivery and playback at a multiplayer level, which includes:

- Protecting content with technology *within and around* the video player: the consumer playback experience.
- Protecting content *from* “players”: the pirates – the potential bad actors looking to compromise your service, and steal content. This is the human factor.

If you're an OTT service launching premium exclusive content, don't be the one that suddenly discovers your content appearing, and then being distributed through pirate services, within minutes of launch.

### Digital Rights Management (DRM)

Often considered the cornerstone of content and revenue protection strategy, [digital rights management \(DRM\)](#) remains a critical part of an effective multi-prong system. In [Article 2](#), [Intertrust Technologies](#) discussed the pros and cons of two DRM license acquisition models (direct acquisition model, from a license server, and proxy license acquisition model, from a proxy server).

---

*Linked content is protected under the individual Privacy Policies and Terms & Conditions of the companies listed.*

©December 2020 Bitmovin Inc. All rights reserved. ©December 2020 Friend MTS Limited. All rights reserved. ©December 2020 Intertrust Technologies Corporation. All rights reserved.

Intertrust also discussed DRM best practices for leveraging a cloud-based DRM service to protect high-value streaming content. OTT operators must follow these to block the loopholes that hackers otherwise may use to defeat the purpose of DRM technology.

- **Multiple content encryption keys (CEK)** – Setting different CEKs for audio track, as well as for each video resolution, enables OTT streaming service providers to grant access to content distributed to different customers/different devices. They can do this by delivering only the DRM licenses with CEKs for the authorized resolutions based on the consumer's subscription package.
- **DRM security levels** – Defining the security tier of the DRM stack that is supported by the target device, with two relevant distinctions: software-based DRM client and hardware-based DRM client. Using the right DRM security level allows OTT streaming service providers to map the required security level for each given resolution or track.
- **Widevine Verified Media Path (VMP)** – The requirement enforced by Google Widevine DRM is specifically relevant when a browser-based video player is used to decrypt Widevine-protected content. Given Google's recent policy to strictly enforce the VMP requirement, Widevine license servers can only issue licenses for content decryption modules that support the VMP feature.

### Securing the Playback Experience

Delivering high-value premium content to a web browser can be a risky venture, but one that is critical to reaching audiences today. Browser environments are amongst the farthest-reaching, but least secure, due to their open nature, and require some extra attention when implementing content protection systems.

Bitmovin highlighted in [Article 3](#) how code obfuscation tools and techniques work in browser playback environments where website code (JavaScript) is interpreted and executed. The result is code that is extremely difficult to read and reverse-engineer, either by tinkerers or a more determined actor...such as a content pirate.

Yet executing code on a web browser, following open JavaScript standards, remains impossible to completely secure playback. Someone with enough motivation, and time to spend gathering intelligence and doing research, will eventually be able to reverse-engineer your playback code. In reviewing its web player, Bitmovin detailed how concurrent management and domain locking work as part of a complete defense strategy to deter attacks from content pirates.

Finally, once an OTT provider has secured its **distribution chain from source to the playback environment**, and has followed best practices to secure the playback experience as much as possible, Bitmovin summarized three golden rules to boost users' experience – and ultimately, your brand.

### Watermarking and Monitoring

For all of its merits, the reality is that DRM only protects the delivery and distribution of content to the point of consumption. In [Article 4](#), [Friend MTS](#) showed that beyond DRM there is a need to detect pirated content, deter wrongdoers by identifying them in stolen content, and take action to stop further loss of revenue by disabling access to the service.

Although DRM protects the content until it arrives at its intended legitimate destination, additional precautions should be made to stop content from being redistributed by those who have no rights to do so.

Commonly pirates will capture content directly from the screen (with the use of screen recording software) or a device's digital output with rights management removed. They're able to rip the stream once the content is decrypted by the authorized devices.

So, if DRM protects only the legitimate path from origination to the point of consumption, the OTT operator must protect the value of video content – whether original or rights-managed – outside of these service boundaries.

**How?** Forensic subscriber-level watermarking can be employed on any delivered video in the service. Doing so affords the ability to identify the ‘subscriber’, your legitimate user. Using a combination of active monitoring of piracy groups and sites – suspected pirate materials are identified through known reference fingerprints, and an extraction process can take place to obtain the subscriber identifying data within the watermark. This can rapidly signpost the “bad actors”, low volume content sharers, and industrial-scale pirates. Action can then be taken to stop the content from being accessed and used for piracy.

With an effective subscriber-level watermarking solution, you can close the loop and start to lock down piracy at its source.

Friend MTS reviewed the pros and cons of A/B variant (server-side) and client-composited (client-side) watermarking and looked at how they are deployed and function. Client-composited is the clear winner with its rapid detection of content theft, lower overall cost, reduced deployment complexity, faster time-to-market, and higher adaptability to attacks on watermarks.

In looking at the characteristics of an effective client-composited watermarking service, Friend MTS outlined its Advanced Subscriber Identification (**ASiD**) service, which has retained its agility to fend off attacks and has proven robustness in both broadcast and OTT environments. They highlighted the importance of a watermarking provider not only keeping up with the latest pirate schemes but staying ahead of them. They also detailed the key watermarking features of speed, global reach and ability to deliver through a multi-CDN service – all within the context of live sports and entertainment, pay-per-view and on-demand content.

Article 4 also highlights the need to understand the ‘human factor’ in your OTT service – the end-users who are consuming content. Friend MTS advised starting with a position of ‘zero trust’ for your users – assume some users of your service will attempt to circumvent security controls or use your service in a way you didn’t intend. Errant or undesired behavior within your service can be broken down into various ‘personas’ and the article takes you through several of these.

Once user behaviours are understood, you can plan your monitoring architecture, and how your business support systems should respond to service misuse.

## Conclusion

Today’s OTT world is radically different than it was in early 2020. Bad actors abound. Content and revenue are at risk literally every minute of every day around the world. But you do not need to be a victim.

It’s possible to take steps upfront to secure content, working with a multi-pronged strategy that integrates DRM, client-composited forensic watermarking, player security, and robust monitoring to produce a real solution to the problem of content piracy. In today’s world, “end-to-end” is not just an IT buzzword. It’s a way of delivering streaming media to a playback client in the most secure and protective environment that we can achieve.

---

Check out the recording of our How To Trust Your Player Webinar: [View Recording](#).

For information on redistributing this content, please reach out to [pr@friendmts.com](mailto:pr@friendmts.com).

**How To Trust Your Player** is a collaborative effort between Bitmovin, Friend MTS and Intertrust. Our goal is to educate media and content providers on the importance of delivering streaming content in the most secure ways possible from the video player to the end-consumer while protecting both their content and revenue.

## Bitmovin

Bitmovin is a developer of video streaming technology. Built for technical professionals in the OTT video market, the company's software solutions work to provide the best viewer experience imaginable by optimizing customer operations and reducing time to market.

Bitmovin's solution suite – a video encoder, player, and analytics platform – lets content owners redefine the viewer experience through API-based workflow optimization, fast content turnaround, and scalability.

Founded in 2012, the company is based in San Francisco, with offices in major cities in Europe, North America and South America. With more than 250 enterprise customers around the globe, Bitmovin helps power clients like BBC, fuboTV, Hulu Japan, RTL, and iFlix.

## Friend MTS

Friend MTS helps media and entertainment businesses secure content so that revenue can grow and creativity can thrive.

With advanced services that measure, monitor, detect and disable content piracy, Friend MTS provides a 360-degree view of the constantly shifting content piracy protection ecosystem and stays a step ahead of ever-advancing and sophisticated content piracy behavior and technology with a sharp, deliberate, laser-focused commitment to continual monitoring and innovation.

Businesses and nonprofit organizations throughout the world recognize Friend MTS as the leading authority for content and revenue protection. The company also has donated its digital fingerprint technology to the International Center for Missing and Exploited Children to tackle child abuse content online.

Founded in 2000, Friend MTS is headquartered in Birmingham, England, with operations throughout Europe, the Middle East, Africa, Latin America, and North America. Friend MTS is the recipient of an Emmy® Award for Technology and Engineering, presented by the National Academy of Television Arts and Sciences (2018).

## Intertrust Technologies

Intertrust provides the world's leading digital rights management (DRM) cloud service with a complete ecosystem of security and rights management products. We empower businesses to securely manage all of their data and devices, regardless of location, format, or type—enabling innovative multi-party apps and services.

Intertrust Media Solutions provides robust content protection solutions for Media and Entertainment. Intertrust ExpressPlay consists of a cloud-based multi-DRM service, broadcast TV security and anti-piracy services with proven scalability in the largest OTT streaming platforms globally.

ExpressPlay DRM™ is today's most complete multi-DRM monetization service for OTT streaming supporting Apple FairPlay Streaming, Google Widevine, Microsoft PlayReady, Adobe Primetime, and the open-standard Marlin DRM. Intertrust also offers ExpressPlay DRM Offline to enable secure streaming of premium content through an offline multi-DRM platform.

Founded in 1990, Intertrust is headquartered in Sunnyvale, California, with regional offices in London, Tokyo, Mumbai, Bangalore, Beijing, Seoul, Riga, and Tallinn.