intertrust®
ExpressPlay®

WHITE PAPER

Combating the latest threats to live streaming

Part 2:
Deploying advanced solutions to fight against live-streaming piracy

Building trust for a connected world.

Contents

Executive summary

The OTT market's landmark shift to live-streamed sports and other linear content calls for a new, comprehensive approach to battling piracy that can support actionable results against illegal access involving vast numbers of simultaneous viewers.

Given the far-reaching complexities of these issues, identifying an effective approach to protecting live-streamed content is a challenge. Speed of execution is an obvious priority since the sooner piracy can be disrupted, the more significant the impact on pirated live streams can be.

Many other aspects of live streaming complicate content security strategies compared to those with time-shifted content. With live streaming, there are typically:

- More variations in licensing policies, especially when cross-border distribution is involved
- Requirements to reduce latency to accommodate a live viewing experience
- Scalability that requires vastly more streams to be parsed all at once in the search for illegal flows
- More illicit sources to identify and disrupt

Fortunately, these challenges are not insurmountable. The key to success is to choose a tightly integrated platform that combines best-of-breed tools to ensure the streamlined, rapid, and highly scalable execution of everything required to respond effectively to piracy.

The second part of this white paper series explains how advanced multi-DRM and anti-piracy services can deliver the results license holders are looking for at the lowest possible costs. These solutions include ExpressPlay Multi-DRM service, ExpressPlay Anti-Piracy, and ExpressPlay XCA - all developed by Intertrust and its partners to offer a proven, effective response to illicit distribution of live-streamed content.

Part 2 begins with an overview of the requirements needed to mount an effective defense against the highly effective means pirates now employ to capture audiences and deter detection. These requirements include support for:

- Robust execution of the multi-DRM protection suited for high-value content, meeting all licensing policies for each engagement
- Techniques to ensure DRM protection will not add latency to live video streams
- Approaches to forensic watermarking that can address different types of linear content
- Effective means of immediately identifying stolen content as a first step to tracking sources through watermark detection
- Additional requirements contained in the MovieLabs' Enhanced Content Protection specifications for 4K UHD and HDR-enhanced content

Once these requirements have been met, losses can be cut in amounts far exceeding the costs of curtailing theft. Through implementing Intertrust ExpressPlay solutions, producers and distributors of high-value sports and other live-streamed content will have the tools they need to combat the ongoing challenge of live-streaming piracy.

Defining content protection for the live-streaming era

As noted in the first paper in this series, a piracy ecosystem has emerged utilizing new approaches to marketing, monetizing, and facilitating consumers' access to illegally streamed sports and live TV channels. This sophisticated approach is driving legitimate providers' losses to what were once unimaginable heights. But, with the proper tools, this is no longer an inevitable outcome.

Multi-DRM support at low latency with unlimited scalability

As in many other aspects of OTT operations, advances in cloud technology have greatly facilitated the ability to set up and manage comprehensive anti-piracy initiatives cost-effectively. Large-scale processing and multi-faceted workflows can now be activated with far greater technical and financial agility than the on-premises server installations of the past.

Implementing a cloud-based next-generation security solution optimized for live streaming starts with a multi-DRM operations platform. Given the realities of device fragmentation, such a platform must work seamlessly with the four major DRM systems, including Apple FairPlay, Google Widevine, Microsoft PlayReady, and the widely used Marlin DRM. Intertrust and others developed the latter, and it is natively supported in chipsets running on millions of devices worldwide.

Keys used by end devices to unlock encrypted content must be provisioned on a per-session basis for all of the types of encryption methods and file formats these DRMs use to convey licenses and policy information. All provisioning and upgrade processes associated with these interactions must be rigorously secured. The same is true of the keys themselves, which must always be protected.

With linear OTT content, licensors typically require that keys be refreshed multiple times during a viewing session. The multi-DRM platform also must support instant delivery of keys and licensing enforcement policies whenever a user accesses a new program in the OTT service lineup. This is essential to allow users to switch from one live channel stream to another just as easily as they do with legacy TV services.

It's important to note that additional usage rights policies can come into play when live streams provide automated support for time shifting. These include catch-up viewing in limited-time windows and cloud-based DVR options utilizing long-term storage. Distributors must be sure their system recognizes whether their licenses cover such use cases and that appropriate protections are provided when they do.

In cases involving MVPD services, operators also need to rely on the multi-DRM platform to serve as aggregators of OTT providers' services. Given the hassles subscribers face in dealing with the fragmented OTT ecosystem, such service aggregations have been widely adopted by MVPDs looking to leverage convenience as a retention tool.

These strategies are best accommodated through a uniform approach to content protection that marries the rights policies the MVPD must adhere to with the rights policies governing their OTT partners. An integrated approach to content protection on live-streamed services allows MVPDs to adhere to all policies without re-encrypting content under separate protection regimes.

All the steps in managing the execution of rights policies tied to multi-DRMs, whether under the control of an OTT provider or an MVPD, pose a serious latency challenge for live sports and other time-sensitive linear content. As discussed in Part 1, with distributors going to extraordinary lengths to cut streaming lag times to broadcast-level latencies, there's no room for adding a second or two of latency in live-streaming situations.

As the number of simultaneous users viewing a live-streamed program increases, which can reach tens of millions with major sports championships, completing all the processes involved in multi-DRM protection at low latency is even more challenging. Whether a few hundred or millions are watching, the multi-DRM platform must be able to ensure consistent user experiences across all devices with delay-free acquisition of keys from DRM servers run by multiple licensing authorities.

This applies to key refreshment and key provisioning with each session. Of course, preventing delays caused by the end-user players' acquisition of licenses in the initial authorization process is also vital to maintaining low latency. This is an incredibly daunting challenge when the multi-DRM platform must issue tens or even hundreds of thousands of licenses per second.

Effective support for flagging stolen content

A basic principle in the battle against consumption of purloined sports and other live-streamed content is that the quicker a fast response is, the more effective it is. Disruptions to illicit viewing early in a game cause more pain to pirate audiences than later disruptions, and failure to act before the game ends renders any action useless.

Timely counteraction begins with determining which live content streams emanate from unlicensed sources. Insofar as other sources might have licenses to distribute the content, it is essential to ensure that follow-up source tracing using forensic deciphering of watermarks is strictly focused on illegitimate sources.

Many legacy approaches to identifying stolen streams commonly used with stored content offered on demand either need to be faster or have been compromised by pirate countermeasures to the point where they can no longer be relied on. One that has been used with live streaming but is now more or less useless involves monitoring for branding labels and other visible "hash codes" on streams that aren't from licensed sources. Pirates regularly employ widely available, low-cost hash-code removal tools, which work in near real-time to strip away any kind of visual marks from a video feed in ways that avoid any noticeable disturbance to the picture.

A more effective approach to identifying illicitly distributed licensed content involves using web crawling tools in conjunction with forensic fingerprinting technology, a mainstay in automatic content recognition (ACR) applications. Digital fingerprinting, as the term is used in media, entails storing key video and/or audio descriptors that uniquely define a piece of content licensed to a specific distributor. Suppose an automated reference to server-stored listings shows the content isn't coming from one of the listed licensees. The content can then be immediately flagged for follow-up in the watermark detection process.

The fingerprinting technology used in theft detection must be undetectable by pirates. It must also be robust enough to remain intact across all video formats and survive any aspect ratio change, bitrate reduction, and downscaling during playout processing. Moreover, speed and scalability of detection at 100% accuracy is essential.

Watermarking designed for live streaming

The motion picture studios' MovieLabs issued Enhanced Content Protection (ECP) specifications in 2013. This ignited industry expectations that watermarking could be used to identify end-user premises-based sources of piracy and become an essential security component in high-value video distribution. But, with the slow ramp-up to distribution of movies earmarked for ECP, including 4K UHD-formatted releases and movies distributed in early-release windows, the studios have been slow to implement ECP requirements. Recently, they've picked up the pace amid growing alarm over losses to piracy.

A much stronger push for watermarking is coming from the live-streaming side of the market, especially for sports streaming. The scale of losses to theft is prompting more sports producers to include requirements for an effective approach to watermarking in their licensing terms. At the same time, now that 4K UHD and HDR formatting are becoming more commonplace, watermarking requirements are taking hold in licensing for other types of live-streamed content.

To be effective for live streaming, watermarking solutions, working in tandem with fingerprinting or other means of detecting pirated content, must:

- Support extraction and analysis fast enough to allow disruption of illicit viewing shortly after streaming starts. Critically, this includes extracting the marks directly from the video for immediate identification of pirate sources. This eliminates traditional "non-blind" approaches to detection that require comparison with the original unmarked video
- Be rigorous enough to withstand detection by pirates and the many means outlined in Part 1 that pirates have devised to render watermarks useless.
- Survive content degradation in both the legitimate and piracy phases of distribution, including processes such as transcoding, recompression, and camcording.
- Avoid adding noise or artifacts that could contribute to content degradation.
- Work with persistently encrypted content, eliminating the need to decrypt and re-encrypt during content preparation and delivery.
- Integrate watermarking tightly into a comprehensive security solution that orchestrates all aspects of protection to achieve the best possible results.
- Ensure a legal framework exists for service providers to actively pursue copyright infringers.

There are two approaches to executing watermarking in live-streaming scenarios. One uses server-side per-session injection of watermarks. This is often done at network edge points anchored by CDN facilities that have been enhanced to execute watermarking through integrations with solutions from one or more suppliers. The other relies on client-side solutions that are securely integrated with media players or embedded in lightweight and versatile hardware to work with any device.

A rule of thumb for distributors selecting a watermarking solution for live streaming is that the optimum results are likely achieved with a market-validated client-side solution approved by studios. The exception will be if the rights holder has stipulated conditions necessitating a market-proven server-side solution.

Fundamentally, the intrinsic advantage of a client-side over a server-side solution stems from the fact that, in live streaming scenarios, the watermark extraction process leading to the identity of the source can be performed in a minute or so. Server-side applications have much longer identification processes that can take up to 15 minutes. Watermark identifiers in client-side applications are encapsulated in shorter video segments. This is possible in live scenarios because pirates don't have time to execute the countermeasures that could be taken against this somewhat less secure approach to watermarking.

Accordingly, license holders have adjusted their requirements to enable rapid action against the theft of live content. However, for linear streams delivering episodic programming that will also be available on-demand, watermarking high-value linear streams formatted in 4K UHD and HDR will likely require a server-side watermarking approach.

The studios have made clear that they will continue to require more stringent watermarking requirements in licensing 4K-formatted movies for network distribution, as set by the MovieLabs ECP specifications. In these cases, the accessibility of client code to every end user, which is theoretically possible in client-side applications, no matter how vigorously protected, is perceived as too great a vulnerability.

Many server-side solutions designed for live streaming rely on the CDN "A/B" switching approach to marking. This avoids delays in the watermarking process that are untenable with live content. In these cases, each of two versions of the same live video sequence created in the encoding process has been injected with one of two different invisible digital codes that remain the same for all viewing sessions. The system assigns a unique sequence of watermarked chunks from the two streams. These are delivered either at the point of unicast streaming from an edge server or with client player-directed rendering of the sequence on the device.

Choosing the right watermarking approach: Server-side vs. client-side solutions for live streaming.

This solves the problem of executing on-the-fly injection of the watermarks into each unicast stream. But proponents of other purportedly superior approaches say that the A/B method adds to the workloads on encoders, increases storage requirements in conjunction with temporarily queueing up A/B chunks in the delivery network, and consumes more bandwidth over distribution links to the points where the A/B switching occurs.

Since other solutions have appeared that claim advantages over the A/B approach with no loss and, in some cases, gains in speed both at the injection and extraction steps in watermark processing, the A/B choice for live streaming can no longer be taken for granted. This adds to the factors that distributors need to consider when choosing a solution.

A well-designed comprehensive security platform suited to protecting live-streamed content should allow distributors to use client- or server-side approaches.

Other requirements impacting live content licensing

Security mechanisms incorporated into solutions integrated with the comprehensive content protection platform should also provide protection against app attacks where sources of pirated content substitute a phony ID for the real source's ID. Attacks on apps, which, as mentioned in Part 1, are a growing source of industry concern. They can be thwarted with advanced shielding that hardens apps against static and dynamic analysis, hacking, and reverse engineering.

Beyond watermarking, license holders are including other elements of MovieLabs' ECP specifications in their requirements for rights to stream live content. Although these requirements were proposed in the motion picture context, they, like watermarking, have moved into the broader realm of protection for multiple content categories.

While extended ECP requirements aren't universally required yet, distributors must be sure the security platform they choose is equipped to meet these stipulations as they gain more traction. These requirements include:

- Expanded hardware-level protection that entails implementing hardware roots of trust at the factory or through firmware reconfiguration to, as MovieLabs puts it, "provide a secure mechanism for DRM systems to store secrets in local, persistent storage in a form encrypted uniquely for the device."
- Maintaining a secure video path (SVP) and leveraging Trusted Execution Environment (TEE) for separate protection-related processing, including encryption, decryption, and device authentication
- Extending ECP protections beyond streaming to include content downloads, offline playbacks, device-to-device side loading, and time shifting.
- Protection for all in-the-clear content transitions
- Rigorous enforcement of device certification requirements through "trusted implementers" instead of relying on device OEMs to provide security compliance
- Implementing robust server-side security measures, such as strong user authentication and meticulous session management, to ensure only authorized access and control.

Robust protection of Intertrust anti-piracy solutions

Comprehensive protection services provided by Intertrust's ExpressPlay Media Security Suite are optimized to provide license holders and distributors of live-streamed content with all the mechanisms they need to meet the requirements described above.

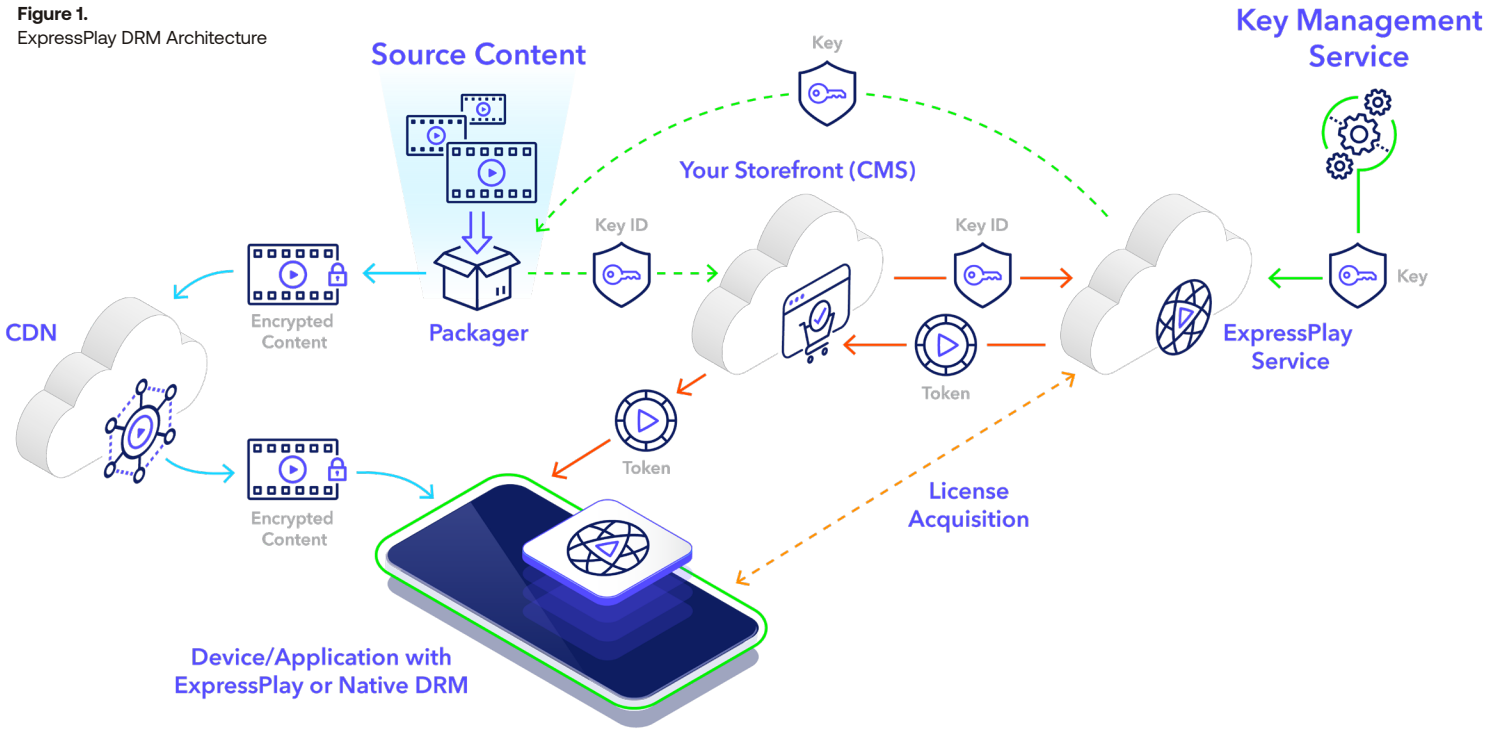
These live-optimized features exist within the Intertrust framework to protect all types of content delivered in OTT and MVPD managed-network environments.

On the OTT side, Intertrust's ExpressPlay DRM, a cloud-based multi-DRM service, is the foundation for that framework. One of the world's most widely deployed multi-DRM technologies, ExpressPlay DRM, provides full turnkey support for OTT video service providers that reach more than a quarter of the world's population.

As depicted in Figure 1, ExpressPlay DRM delivers the functionalities essential to cover all bases of any OTT video service strategy. Critically, it is the only multi-DRM service that supports all major DRMs, including Apple FairPlay, Google Widevine, Microsoft PlayReady, and Marlin DRM.

Deployed on Amazon Web Services (AWS) facilities worldwide, ExpressPlay DRM allows distributors to implement robust rights management on a usage-driven cost basis without adding new infrastructure or incurring extraneous

Figure 1.
ExpressPlay DRM Architecture



Proven scalability: ExpressPlay DRM efficiently managed 85 million licenses during a major event, showcasing unmatched reliability and performance in live-streaming content delivery.

setup costs. The service operates in all live and on-demand OTT streaming scenarios to provide device credentials, content key storage, content encryption, secure playback with multi-DRM license delivery, and real-time generation of audit reports to adhere to licensing terms.

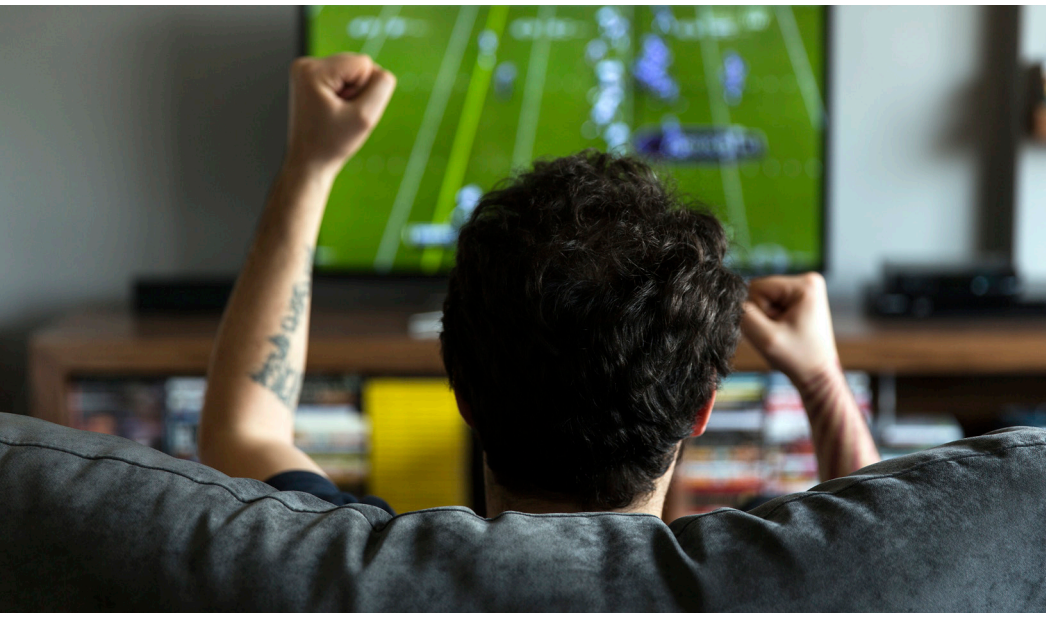
Since any solution must maintain a large amount of capacity sufficient to accommodate the heaviest use-case scenarios, ExpressPlay DRM also delivers a major cost advantage over fixed-priced solutions and build-it-yourself approaches.

Achieving multi-DRM scalability

Intertrust's emphasis on a service architecture optimized for instantaneous scaling is paramount in achieving multi-DRM scalability. This capacity is particularly crucial when accommodating the unpredictable spikes in user activity during live-streaming events.

ExpressPlay's service structure is adept at combining a high transaction rate with low latency, which is instrumental in enabling simultaneous access for a large number of users. ExpressPlay's resilience and scalability have been consistently tested and validated in high-demand situations where more rigid platforms might have shown limitations.

Intertrust's track record solidifies this claim. Over the last three years, the platform has efficiently distributed over 50 billion DRM licenses, managing peak rates that soared to 10,000 DRM licenses each second. A standout instance of this capability was evident during one of the biggest sporting events in the world in November 2023, wherein ExpressPlay effortlessly handled the delivery of 85 million DRM licenses throughout just 7 hours. These statistics exemplify the system's reliability and efficiency and reinforce the critical advantage of using ExpressPlay when unparalleled scalability is required to meet the burgeoning demands of live-stream content delivery.



A key aspect of Intertrust's optimization of ExpressPlay DRM for live streaming involves mitigating latencies frequently incurred in multi-DRM scenarios.

Support for new advances that accelerate DRM operations

A key aspect of Intertrust's optimization of ExpressPlay DRM for live streaming involves mitigating latencies frequently incurred in multi-DRM scenarios. That mitigation starts with eliminating encryption-related delays through tight integration of ExpressPlay DRM with third-party encoders and packagers. This is done via robust APIs tuned to leading encoders/packagers used by content distributors.

This integration aligns with ExpressPlay DRM's ability to execute the fast, efficient Content Encryption Key (CEK) acquisition process defined by the MPEG-DASH Industry Forum's Content Protection Information Exchange (CPIX) standard. This facilitates the packaging of protected content while eliminating the need to rely on proprietary DRM APIs to handle information exchanges.

These efficiencies are also important to save time when specifying multi-key encryption processes, where different key values are associated with different content resolutions or other distinctions assigned to a given content stream. CPIX supports per-track encryption and key rotation.

The widespread adoption of the Secure Packager and Encoder Key Exchange (SPEKE) protocol, developed by AWS as a CPIX subset to define a standard API that streamlines communications between DRM systems, packagers employed in encoders, and origin servers, augments efficiency tied to the use of CPIX.

Intertrust leverages SPEKE to facilitate streamlined integration of customers' DRM operations with AWS Media Services. Communications between Media Services and the ExpressPlay Key Management Service (KMS) through AWS API Gateway endpoints support DRM signaling and the delivery of encryption keys for live and VOD content processed by the AWD MediaPackage,

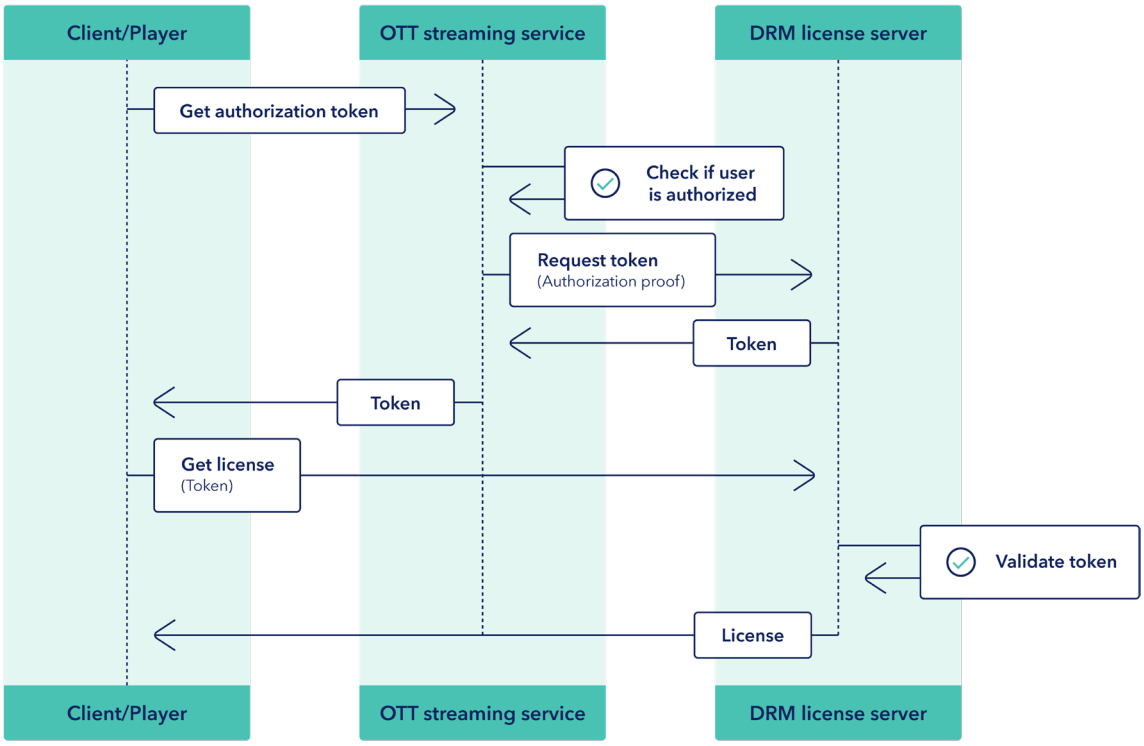


Figure 2
Direct DRM license acquisition model

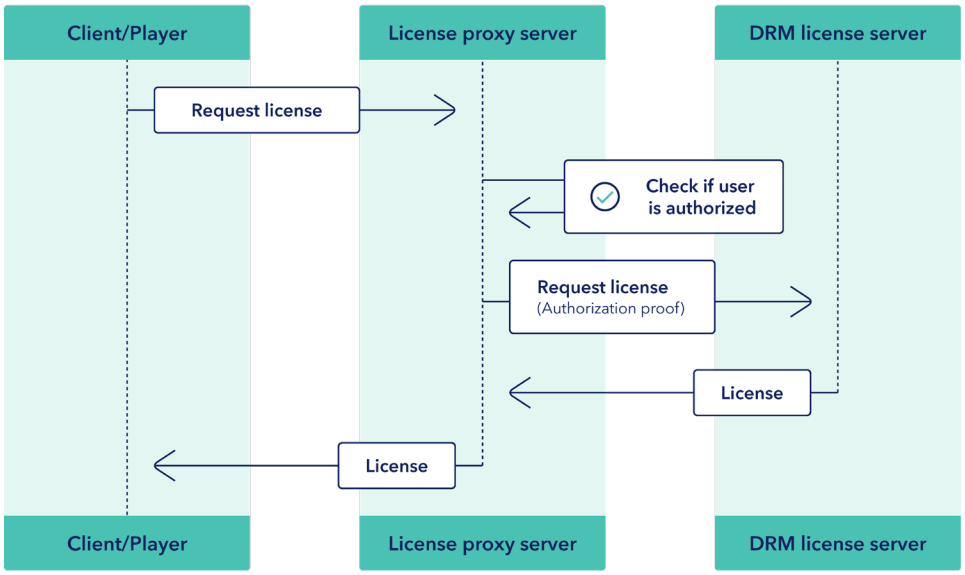


Figure 3
Proxy DRM license acquisition model

MediaConvert, and Media Live modules. ExpressPlay DRM enhances the operator's capability to distribute DRM licenses directly to user devices via a proxy service. This approach grants operators greater control over license delivery status, thereby minimizing potential delays in the event of a failure.

In addition, License Proxy licensing authorization is performed as part of the license acquisition process triggered by the player when it detects a content key is needed. This greatly simplifies support for complex use cases such as key rotation and/or multi-party packaging workflows.

Other important benefits can be realized with proxy-based license delivery. As the licenses are bound to the specific session they were requested for, using a replay attack will not be effective. Viewers cannot process pirated licenses because using them for another session/device is impossible.

Proxy Licensing also simplifies client-side logic, making setting up players easier. Because the player will always retrieve the license from a known endpoint, there's no need to configure the player to prefetch tokens.

Support for live-optimized watermarking systems

ExpressPlay also offers two types of watermarking solutions, providing distributors with a choice of client-side or server-side solutions; however, as noted earlier, a client-side solution is the preferred choice for live content distribution.

Intertrust has partnered with best-of-breed suppliers in both categories. Notably, each approach uses watermarking injection more efficiently than CDN A/B switching. In either case, ExpressPlay Watermarking enables a holistic live content protection environment.

Advanced DRM integration: Intertrust enhances live streaming with rapid, efficient DRM execution and robust encoder integration, ensuring minimal latency and maximized content security.

Live streaming protection optimized for MVPD operating environments

All of the security elements described here are available to MVPDs as a holistic solution to live-streaming piracy and in conjunction with access to ExpressPlay XCA, Intertrust's SaaS platform for addressing legacy pay TV service protection. XCA is free of the royalty or other fee structures common to legacy conditional access systems (CAS) and is ideally suited to converged content protection for hybrid TV services. Intertrust makes this possible by utilizing the widely embedded Marlin DRM core to enable CAS without hardware tokens.

By leveraging the integration of ExpressPlay DRM with ExpressPlay XCA, TV providers can use ExpressPlay XCA to protect virtually any type of hybrid TV service delivered to any DVB-compatible media gateway, STB, or smart TV, regardless of operating system. By complying with the DVB Simulcrypt standard, ExpressPlay XCA can be deployed alongside legacy CAS on one-way devices as well as in interactive networks to facilitate non-disruptive transitions to hybrid services.

The ExpressPlay XCA SaaS also works in concert with Intertrust's ExpressPlay DRM service to provide robust protection for OTT content. As part of the Intertrust ExpressPlay Media suite, it exists in a cloud-hosted environment that facilitates the choice of best-of-breed watermarking and related solutions in tandem with specific operator needs.

ExpressPlay DRM support for additional ECP requirements

As noted, many ECP recommendations beyond watermarking are gaining traction in licensing policies for high-value live and other content. ExpressPlay DRM supports integration of protection with TEEs and SoCs for UHD and HDR, which complies with rules specifying that hardware roots of trust should be used to associate unmanaged devices with a distributor's service at the chip level. This is done through Widevine Level 1 and PlayReady SL3000, as well as Marlin, designed to support TEE-based security and meet the ECP SVP.

ExpressPlay DRM also protects content beyond streaming. Options include support for secure download, offline playback, device-to-device side loading, and protection for content accessed in catch-up and network DVR applications in the case of live programming.

Holistic live streaming protection: Intertrust ExpressPlay XCA optimizes security for MVPD environments, offering a seamless, royalty-free solution for hybrid TV services.

Conclusion

The emergence of live streaming as a major component of the OTT video services market has spawned a new era in online piracy that requires new approaches to protecting content.

With losses to live content theft, led by sports piracy, accounting for an increasing share of the billions of dollars siphoned off by sophisticated online criminal operations, license holders and distributors need to have a comprehensive approach to fighting the scourge at all points of vulnerability. This means every facet of protection, including multi-DRM operations, locating instances of piracy, identifying pirate sources, and disrupting their operations, must be accomplished at any scale without adding latency to the live viewing experience.

Intertrust meets this challenge with its ExpressPlay Media Security Suite. Anchored by the ExpressPlayDRM cloud service, the solution combines multi-DRM protection, piracy monitoring, watermarking, and other mechanisms associated with MovieLabs ECP specifications. Providers can now cover every tactic in the pirate attack arsenal.

ExpressPlay Media Security suite offers live-streamed video security components, including multi-DRM cloud service and best-of-breed client-side and server-side watermarking solutions. The suite also encompasses the ExpressPlay Anti-Piracy Service (powered by Friend MTS) with a global fingerprinting-based piracy monitoring service.

Reversing the worrisome trend of live streaming piracy requires a new, innovative approach beyond security platforms optimized for an on-demand viewing environment. To ensure robust content protection in this new era, ExpressPlay services create the optimal foundation for mounting a full-scale assault against the theft of live-streamed sports and other high-value content.

Through ExpressPlay services, service providers now have a cost-effective way to identify re-streamers rapidly and eliminate the stream source early during a live event. “Subscribers” to such illicit services will learn that the ability to watch live events is not guaranteed when the illegal re-streaming service is disabled and the screen goes black.

The chilling impact on user behavior with such an experience and exposure has been well documented. When this happens during an important game, viewers are more likely to switch to a legitimate service with superior quality and reliability. After all, a live game is only shown live once.

Learn more at: expressplay.com
Contact us: media@intertrust.com

intertrust® ExpressPlay®

Building trust for a connected world.