2 HOW TO TRUST ▷ YOUR PLAYER

Presented by BITMOVIN Friend MTS intertrust

BUILDING AN OTT SERVICE FOR TODAY'S WORLD

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/packagers 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, packagers, 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:

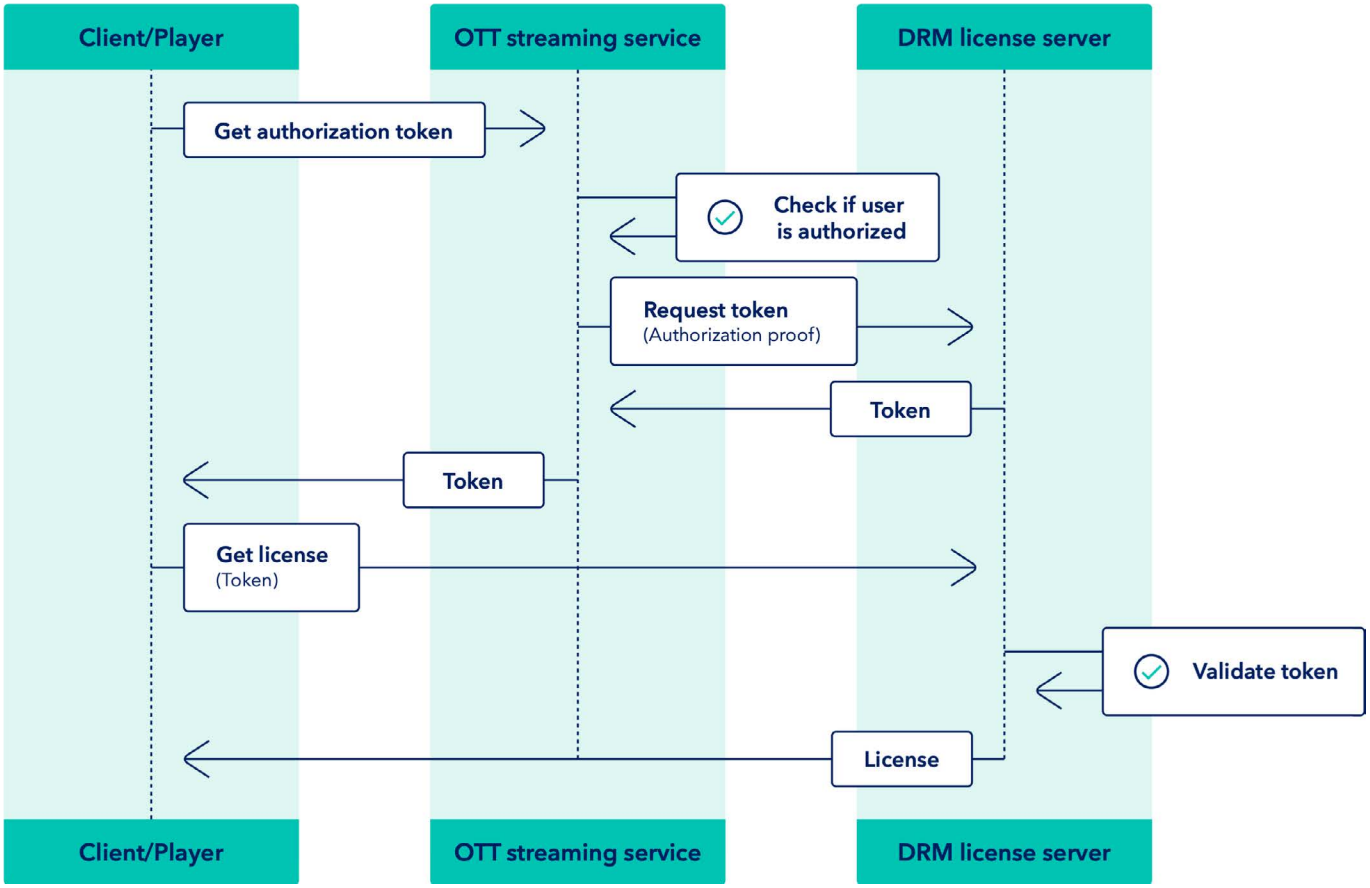
- **Direct license acquisition model:** In this workflow, the subscriber's device or player application communicates directly with the multi-DRM service (e.g. ExpressPlay DRM)
- **Proxy license acquisition model:** In this workflow, the subscriber's device and player application communicates with a proxy 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.

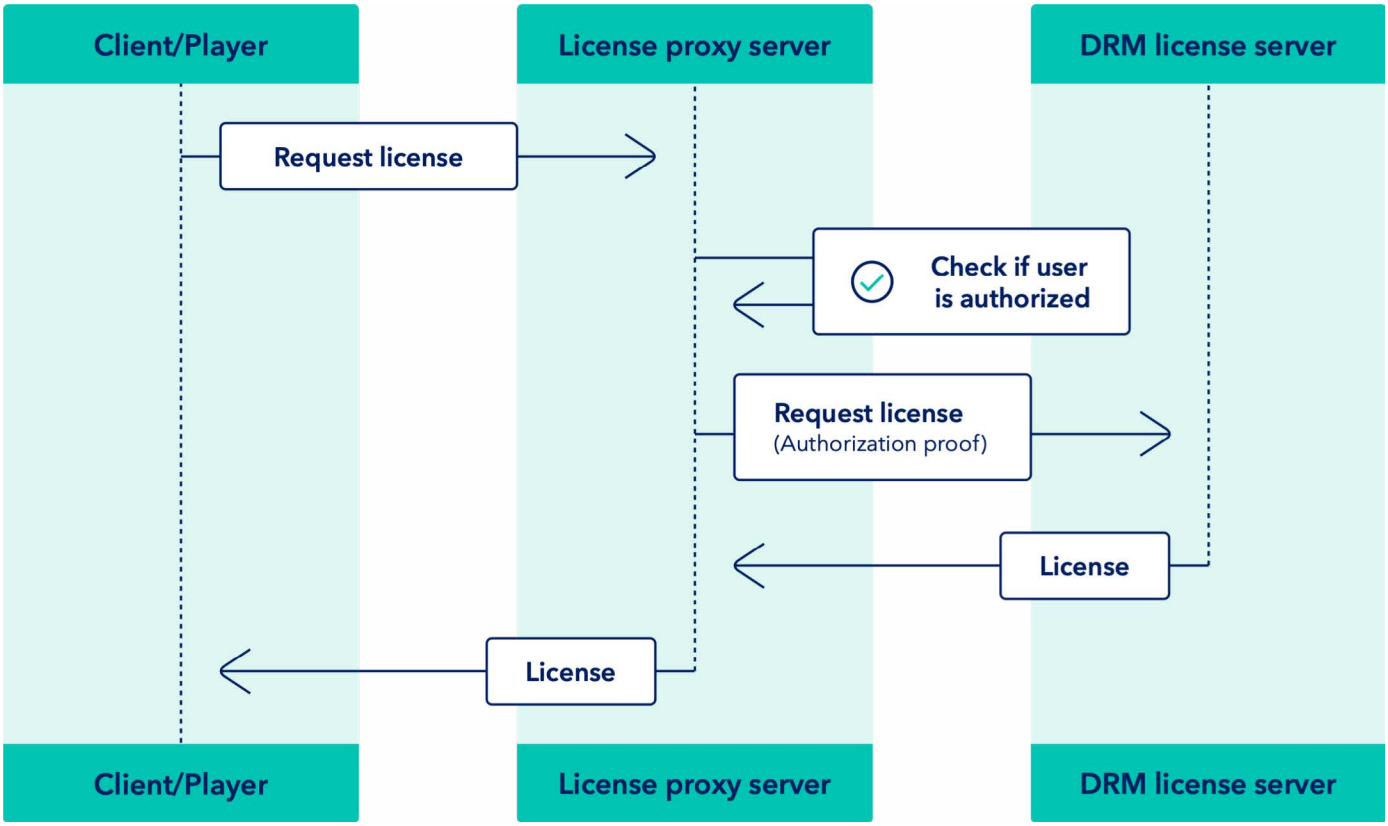
Since the secure token, also known as the DRM authorization token, is critical for generating and delivering the DRM license to the video player in the target device, a multi-DRM service should prevent attackers from reusing the DRM authorization token when they are not authorized to watch the content.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

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 about "How to Trust Your Player," check out the other articles in our series:

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

Still want to learn more? View our associated Fireside Chat sessions:

- **Video 1 – Tips from the Top: Secure Content Delivery and Playback**
- **Video 2 – Securing Content Access with Digital Rights Management Best Practices**
- **Video 3 – Tips and Tricks: How to Secure Your Content in Challenging Streaming Environments**
- **Video 4 – Beyond Digital Rights Management: Video Watermarking Weighs In**

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**.

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.