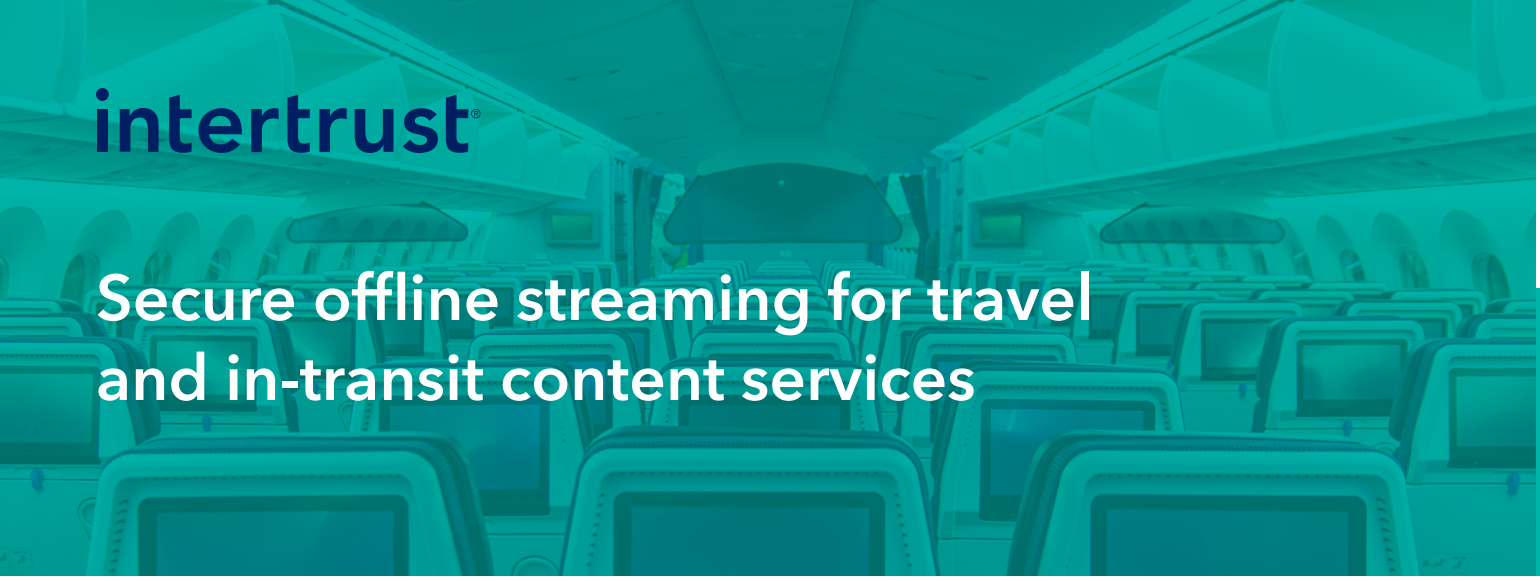
intertrust®

Solution Brief

ExpressPlay



Secure offline streaming for travel and in-transit content services

The challenge

Travelers and commuters making use of public transportation such as airplanes, trains, and buses (a.k.a. common carriers), every so often encounter challenging environments with limited internet connectivity that prevents them from accessing their favorite streaming subscription. Even in cases where internet access is provided, whether against a fee or as a perk, it is often not possible to stream online video due to bandwidth restrictions imposed by the carrier or internet service provider. This is especially true for the current generation of In-Flight Entertainment (IFE) systems, which are constrained by limited satellite bandwidth and hence do not accommodate streaming video from ground-based systems.

To provide passengers with video entertainment without internet access, the common solution is to install onboard systems for on-demand video distribution. These onboard content distribution systems remain offline except for during pre-defined stop-overs when the programming is refreshed, either via a temporary online connection or encrypted high-capacity memory devices. An exception is live services transmission via satellite, where all passengers get a limited number of linear channels to choose from. Carriers must also decide whether to install a dedicated in-seat entertainment system, or to take a "bring your own device" (BYOD) approach. Airlines have invested large sums in IFE systems for many years, while other types of carriers mostly prefer the BYOD approach. Common to both approaches is the need to obtain premium programming to offer onboard video entertainment services. To license premium programming from studios and other content providers, carriers must commit to implementing strong content protection while limiting access to authorized users. The content licensing terms typically include a requirement to utilize a modern digital rights management (DRM) system.

BYOD vs. dedicated IFE systems

A dedicated IFE system requires investments in in-seat video screens and passenger control units (PCUs, i.e., remote controls), headsets, and wiring to each seat. Dedicated IFE systems are costly to purchase and install, and also require extensive and expensive certifications with the governing aviation authority. Another drawback is that such systems also require extensive training of cabin staff to manage and, when problems arise, troubleshoot. Those duties come on top of an already resource-constrained environment.

Dedicated IFE systems have another aspect deeply disliked by passengers apart from malfunctioning: in each seat row there is the equivalent of a bulky set-top box installed under one of the seats, which restricts the ability of a passenger to stretch the legs or to store carry-on items under the seat in front. In the BYOD approach, onboard servers stream content over Wi-Fi to passengers. There are no "seat-top boxes" or other in-seat devices that can malfunction or obstruct, and the demands on personnel is far less. The BYOD approach is by far the most cost-effective and manageable solution compared to dedicated IFE systems while also increasing passengers' flexibility to choose their viewing devices.

The BYOD challenge

The key BYOD challenge centers on how to cope with client device fragmentation; in other words, how to support an array of tablets, phones, and laptops equipped with different operating systems (OS), media players, and DRMs. Offering a branded and downloadable app for iOS and Android devices, as part of the onboard service, is the most cost-effective solution for such offline environments. The app basically consists of a media player with an integrated DRM client. After users download and install the app on their own devices, they will be able to watch content streamed by the onboard server, subject to content usage rules as defined by the rights holders and carriers, and enforced by the DRM system.

The solution

There are several ways to introduce secure streaming for offline environments and this document will describe the Intertrust ExpressPlay solutions that progressively add support for offline entertainment:

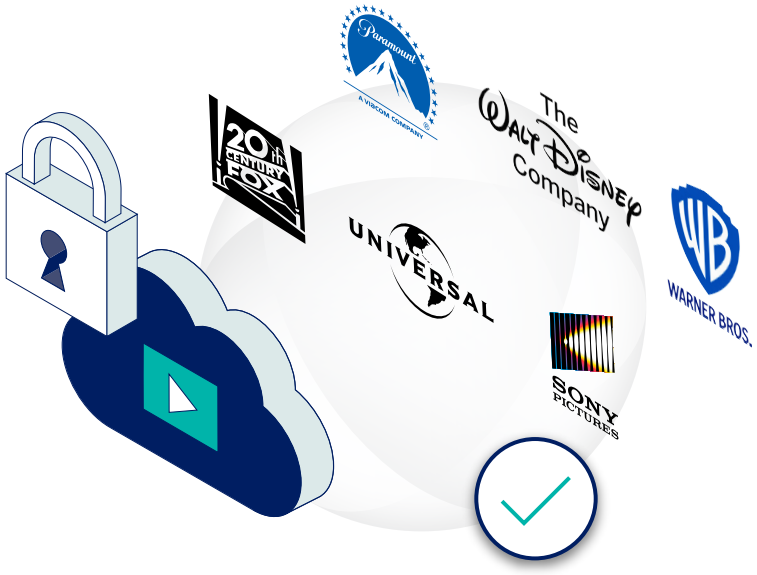
- Marlin DRM
- Intertrust ExpressPlay DRM Offline
- Secure offline streaming workflow and architecture

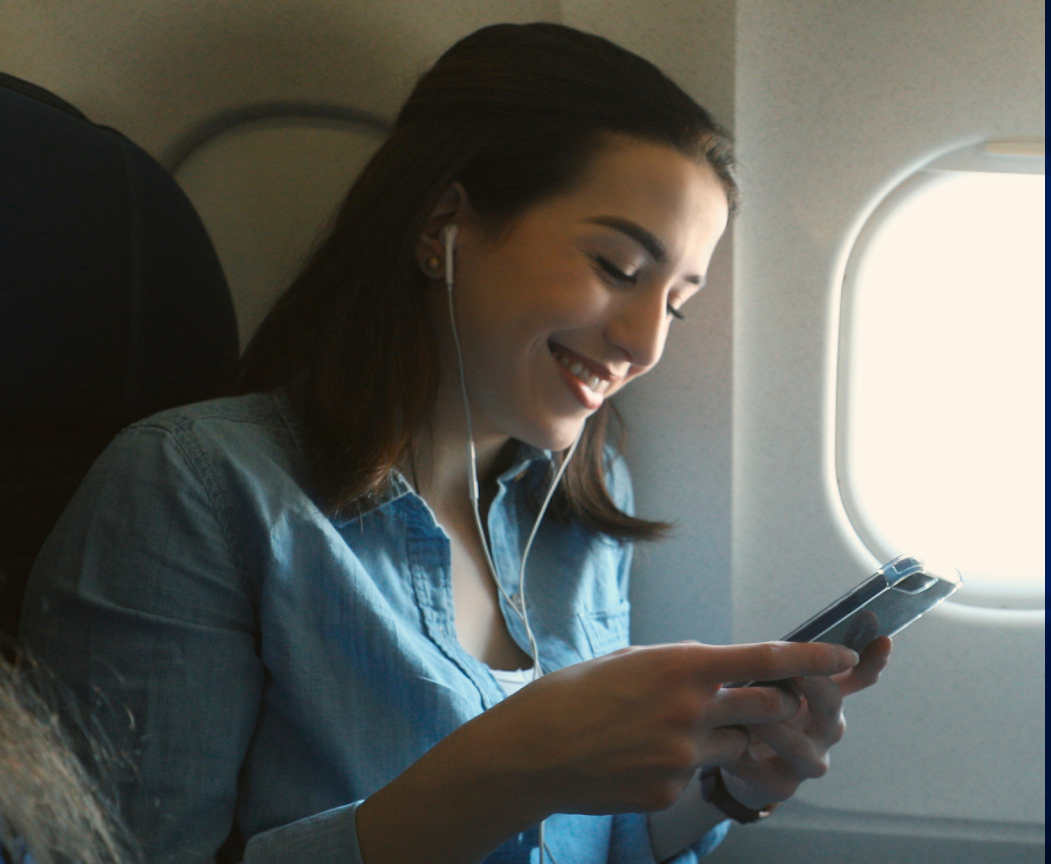
These solutions will be described further in the following.

Marlin DRM

Marlin DRM is a long established content protection specification that is applicable to a variety of use cases across content types, content formats, delivery mechanisms and platforms. It offers sophisticated copyrights management for playing entertainment and media content (including audio, video, eBooks, and games) distributed over mobile, broadband, and broadcast networks. Marlin supports various content distribution models like download, streaming, multicast, and broadcast. Unique to Marlin is its general-purpose rights management architecture that allows for substantial flexibility and control in how it is implemented. Marlin DRM offers sophisticated offline capabilities that are mission critical to transport systems with limited or no internet access.

Marlin complies with requirements defined in MovieLabs' Enhanced Content Protection specification for premium UHD 4K content for limited access and offline environments. The solution is ideal for applications such as travel and hospitality with a BYOD policy to enable secure offline streaming when using branded operator apps on smartphones and tablets. To enable secure streaming to web browsers in Win/Mac OS platforms, advanced multi-DRM support is required, which is where ExpressPlay DRM Offline enters the picture.





Intertrust, Panasonic, Philips, Samsung, and Sony co-founded the Marlin DRM specifications, which were introduced in 2006. The technology specifications and test tools that were jointly developed are freely accessible for evaluation on the Marlin DRM website. Marlin is the DRM of choice in high volume transport settings with large in-train deployments in Brazil and India, and major IFE systems in Japan. Monetization opportunities include advertising, subscriptions and e-commerce/ partnership services.

Marlin provides maximum flexibility to meet the demands of consumers, device manufacturers and service providers. Entities interested in adopting Marlin may do so via the Marlin Trust Management Organization (MTMO), which is the operational entity that grants commercial licenses for Marlin technology.

Intertrust ExpressPlay is a provider of Marlin-based DRM solutions through the ExpressPlay Media Security Suite. Intertrust ExpressPlay is presently the only DRM provider in the world that delivers a complete Marlin stack with these functions as part of the Suite's ExpressPlay multi-DRM service with support for Microsoft PlayReady, Apple FairPlay, and Google Widevine.

Intertrust ExpressPlay DRM Offline™

Intertrust's ExpressPlay DRM Offline

Intertrust's ExpressPlay DRM Offline, a component of the ExpressPlay Media Security Suite, enables secure streaming through a multi-DRM solution designed to protect premium content delivery and playback in environments with limited internet access. The solution features support for Google Widevine Modular and Apple FairPlay Streaming DRMs in addition to Marlin DRM. It allows authenticated and authorized users to gain secure access to premium and rights managed content using Windows and Mac OS browsers, in addition to smartphone and tablets equipped with native DRM clients although the latter can also be served by Marlin SDKs as described next.

marlin WIDEVINE FairPlay

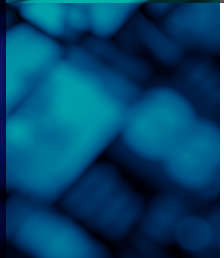
Choice of DRM clients – Broadest client device coverage

Depending on the operating system (OS) of the client devices, there is a choice of using ExpressPlay SDKs or the native DRM clients that many devices come equipped with. This choice enables the broadest possible client device coverage and provides a means to overcome the increasing end-user device fragmentation.

ExpressPlay Binary SDK for Android
- Playback of protected HLS and MPEG-DASH content on devices without native DRM support

ExpressPlay Binary SDK for iOS
- Playback of protected HLS and MPEG-DASH content on iOS devices

Native DRM clients
- Android
- iOS



Secure offline streaming workflow

The overall offline streaming architecture with key components and secure workflow are shown in the diagram below.

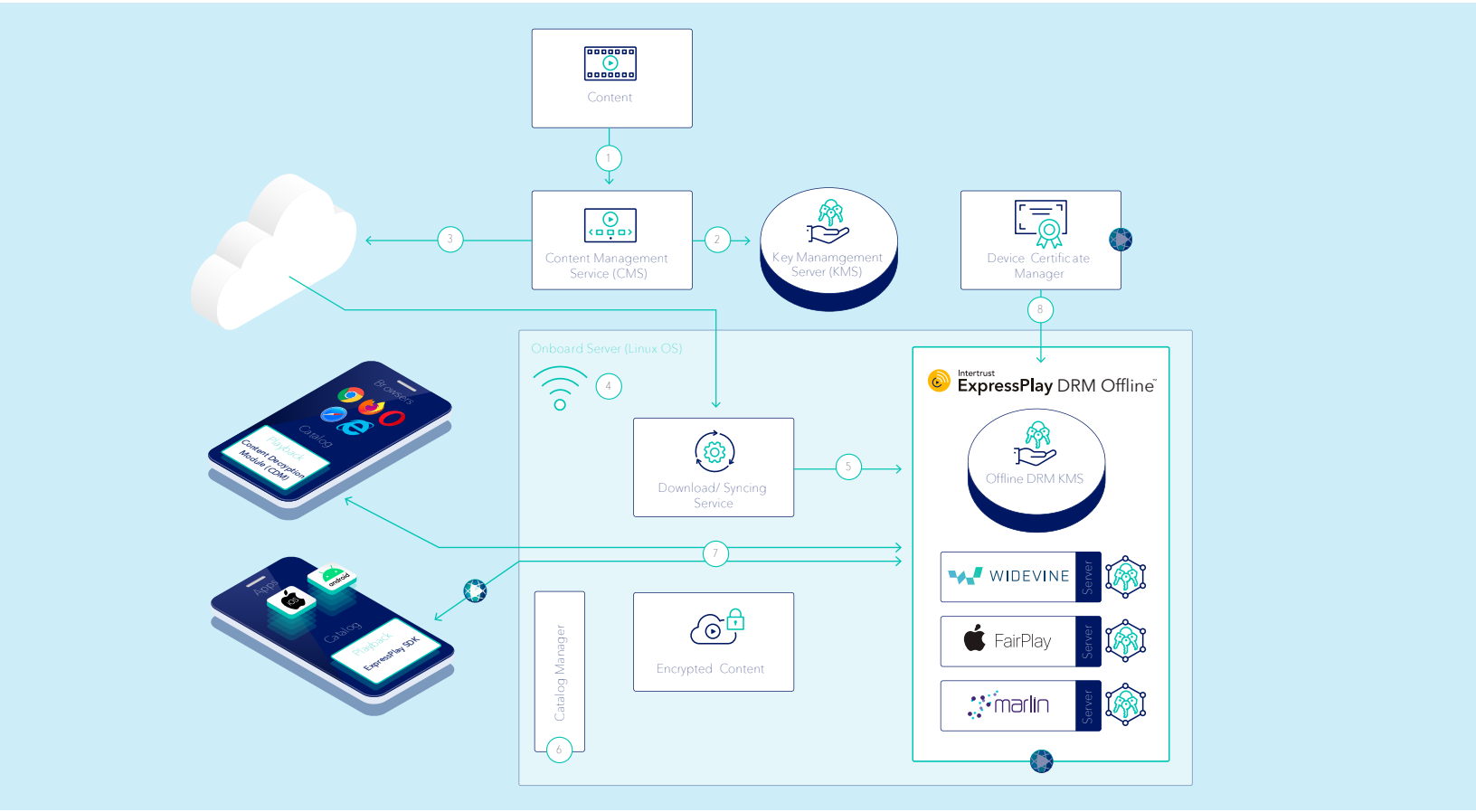


Fig. 1
The secure offline streaming architecturewith key components and secure workflow

The following key components implement the secure workflow as described further here:

1 **Content Management Service (CMS):** A cloud management portal, managed by the service operator or third-party, for publishing and managing content on remote streaming servers. Content is packaged and encrypted with Widevine, Fairplay, and Marlin signaling.

2 **Key Management Server (KMS):** Key management server that handles all the encryption keys during content packaging.

3 **Cloud Storage:** Cloud content storage (s3 or CDN) that keeps all the encrypted content after content packaging.

4 **On-board Server:** Performs downloading/syncing services to refresh server storage with newer content when available from cloud storage. Encrypted content is stored on the server and encrypted keys are kept in the local KMS database.

5 **ExpressPlay™ DRM Offline:** Contains the offline DRM implementation for Widevine, Fairplay, and Marlin DRM.

6 **Catalog Manager:** End-users are able to browse available content via apps or browsers over the local Wi-Fi network.

7 **Content Playback:** Secure offline playback is enabled across all the major browsers, OS, and BYOD devices, in two different processes:

- If the content is played using a browser, the video player and the Content Decryption Module (CDM) communicate with ExpressPlay™ DRM Offline service to authenticate devices and generate/serve native Widevine and Fairplay DRM licenses.
- If the content playback uses native apps, ExpressPlay SDK communicates with ExpressPlay™ DRM Offline service to authenticate devices and generate/serve Marlin DRM licenses.

These processes ensure that secure offline playback is accomplished across all the major browsers, OS, and devices.

8 **Device Certificate Manager:** The ExpressPlay DRM Offline service regularly refreshes all device certificates required by the different DRMs to authenticate end-user's devices.

Entertainment on-the-go use cases

In-flight entertainment (IFE)

The IFE market is undergoing massive change resulting from the pandemic, requiring direct delivery of entertainment content to users' BYOD devices. The ExpressPlay DRM Offline enables IFE solutions to create a secure cloud to distribute content in-flight via Wi-Fi, with no requirement for upstream connectivity. It is a unique and comprehensive solution for passengers, providing a smooth travel experience. For airlines, it is also a potential incremental revenue generator, or an added perk in times of intense competition. Providing the flexibility to allow users to bring their preferred viewing devices is appreciated by passengers while airlines save large CAPEX amounts by not having to install complex in-seat video systems.

In-vehicle entertainment

Similar to the IFE market, the use case for in-vehicle entertainment entails providing both streaming and offline playback of content on user's own devices, secured and protected with ExpressPlay DRM Offline. Users can benefit from a complete entertainment everywhere service for in-car, in-bus and in-train environments with no requirement for upstream connectivity.

Hospitality and public hotspots

Content hotspots are Wi-Fi zones, where users can enjoy protected content securely, by providing an offloading solution that is a lower-cost alternative to expensive broadband infrastructure. These hotspots form the access end-points for mobile devices and enable secure video streaming, protected by ExpressPlay DRM Offline. Hotspots are especially useful for hospitals, hotels, army bases, and more.

intertrust®

Building trust for the connected world.

Learn more at: expressplay.com/products
Contact us at: +1 408 616 1600 | onestopshop@expressplay.com

Intertrust Technologies Corporation
400 N McCarthy Blvd, Suite 220, Milpitas, CA 95035