Content Protection Doc

Release 1.0

AS

March 21, 2016

Contents

We design for DRM & Content Protection (DRMCP) plug-in free playback solutions using desktop and mobile HTML5 rendered multi-DRM encrypted video.

Our DRMCP content authoring workflow approach is tailored to use encrypt-once common encryption (CENC) using HTML5 EME and CDM to manage end-user playback.

1 DRM

Depending on the appropriate playback protection device use-case, integrate with Intertrust's ExpressPlay and Secure Key Manager or AWS Cloudfront content protection mechanisms.

For Adobe Primetime DRM (Firefox 43+ CDM support), the Bento4 CENC packager supports Primetime encryption for DASH, however neither the Bitdash player nor ExpressPlay support Primetime DRM at this time.

1.1 1.1 ExpressPlay Cloud DRM

Secure, cloud-based content protection system from the inventor of DRM. Provide single API access for multi-DRM support. ExpressPlay is a cloud-based DRM service provider for content protection across most consumer-used devices. Enable your online media service with robust rights management without the need for any new infrastructure or setup cost.

The following adaptive bit rate streams are supported by a single HTML5 Javascript player installation, Bitdash 4.0+.

Note: MPEG-DASH.

- DESKTOP MPEG-DASH
  - Protected with Widevine Modular, Microsoft PlayReady, Fairplay, and Marlin DRM
  - Native Google Widevine HTML5 MSE Browser Support
    - Google Chrome 35+
    - Opera (31+)
    - Android 4.3+
  - Native Microsoft PlayReady HTML5 MSE Browser Support
    - Internet Explorer (11+ on Windows 8.1+)
    - Microsoft Edge (Windows 10+)
  - Native Apple FairPlay HTML5 MSE Browser Support
    - Safari 8+ on Mac OSX.
  - Native Adobe Primetime HTML5 MSE Browser Support [Coming Soon]
    - Firefox (38+) on Windows
- DESKTOP HLS

  - Protected with AES-128 encryption and Widevine DRM
  - Native AES HTML5 Browser Support
    * Microsoft Edge (Windows 10+)
  - Native Widevine HTML5 Browser Support
    * Android 4.3+

1.1.1 1.1.1 MPEG-DASH

- Create a PlayReady, Widevine, Primetime and Marlin CENC encrypted MPEG-DASH manifest and files using Bento4 packager.

1.1.2 1.1.2 Apple HLS

- Create FairPlay (SAMPLE-AES) encrypted HLS manifest and files using Bento4 for playback with Safari HTML5 on Mac OSX, iOS apps, and Apple TV apps.

1.1.3 1.1.3 ExpressPlay Cloud Simple Key Manager (SKM)

ExpressPlay provides secure online storage service for your content cryptographic keys * at no additional charge *. The ExpressPlay Key Storage Service uses the Simple Key Management (SKM) REST API, that allows the packager and adaptive player to push/pull content keys to/from ExpressPlay.

Each DASH or HLS packaging process requests the creation of new SKM Key Object prior to multi-DRM CENC encryption. The cloud stored keys are used as inputs to provide encryption data to the manifests.

1.1.4 1.1.4 Amazon AWS Cloudfront Private Distributions

- Once DRM-enabled DASH and HLS packages are complete, upload to Amazon S3 for AWS CloudFront distribution.
  - The S3 bucket is configured with restricted access, limited to CloudFront Origin Access Identity and Authorized AWS User.
  - CORS is configured restricting access to your player's domain.
  - AWS CloudFront (CF) is configured for Web delivery, (optional) CNAME and SSL SNI, S3 bucket restrictions and Origin Access Identity, Cache Behaviour policies and Geo restriction policies.

2 Ingest and DRM packaging process

We use Bento4, a C++ class library and tools designed to read and write ISO-MP4 files. This format is defined in international specifications ISO/IEC 14496-12, 14496-14 and 14496-15. The format is a derivative of the Apple Quicktime file format.

MPEG DASH with fragmented MP4 files, as defined in the international specification ISO/IEC 23009-1 MPEG Common Encryption (CENC) as specified in the international specification ISO/IEC 23001-7

Supports multiple DRM systems that are compatible with MP4-formatted content (leveraging CENC Common Encryption), such as Marlin, PlayReady, Widevine and FairPlay. Support for a wide range of codecs, including H.264 (AVC), H.265 (HEVC), AAC, AC3 and eAC3 (Dolby Digital), DTS, ALAC.

alt reStructuredText, the markup syntax

A figure is an image with a caption and/or a legend:

MPEG-DASH	Google Chrome 35+, Opera (31+), Android 4.3+
HLS	Structure-enhanced text, structuredtext.
Text	Well it is, isn't it?

1. We provide SFTP account details to upload source/mezzanine content to our packagers, including your metadata, your transcoding configuration and AWS credentials in a JSON file. This file contains supplied packaging directives (eg resolutions for multi-bitrates, info on multi-language support in audio tracks etc).
2. We transcode source to AVC and HEVC renditions based on the JSON configuration file. MP4 (H.264) files are converted to HEVC (H.265), encoded using MulticoreWare X.265 libraries.
3. The H.264 and H.265 files are then fragmented. For existing Microsoft Smooth ISMV and ISMA input files, these are refragmented into compliant fragmented MP4 files.
4. Packaging

1. Convert MP4 files to an MPEG DASH presentation, consisting of an initial XML manfifest, called the Media Presentation Document (MPD for short), which describes media segments that form a complete presentation. Along with a number of attributes, the MPD allows the MPEG DASH player to compute the URL of each segment, to download it and render it.
2. Convert MP4 files to an HLS (HTTP Live Streaming) presentation, including the generation of the segments and .m3u8 playlist as well as AES-128 and SAMPLE-AES (for Fairplay DRM) encryption.

Prior to adaptive presentation generation, the packager requests a new Key Object from ExpressPlay SKM API that creates unique cryptographic keys in the cloud for use in the packaging for each adaptive asset presentation. The fragmented MP4 files are then converted to DASH and HLS presentations, encrypted with Common Encryption mode

(CENC). Widevine, PlayReady and Marlin encryption keys are embedded in DASH manifests, and FairPlay DRM in HLS manifests.

5. We transfer encrypted packages to your Amazon S3 bucket using AWS Signature Version 4 API signing process, enabling S3's server-side AES256 encryption by default.

2.1 2.1 HTML5 Player

Bitdash HTML5 Javascript Player version 4+.

Bitdash enables HTML5 adaptive streaming with MPEG-DASH native in your browser with no need for plugins like Flash or Silverlight. Due to the native integration with the browser it is possible to play back very high resolutions such as 4K or very high framerates like 60fps.

Encrypted HTML5 based adaptive streaming with MPEG-DASH native in your browser without plugins. Multiple DRM systems, e.g., PlayReady and Widevine can be used in parallel through MPEG Common Encryption (MPEG-CENC). Google Chrome is currently removing Silverlight, so PlayReady will not be supported anymore. bitdash provides a solution with MPEG-CENC your content will be encrypted once and can be used with different DRM systems in parallel.

The following player code snippet is representative of the rights managed data dynamically loaded by the video player.

source: { dash : <MPD URI>,

hls : <m3u8 URI>,

progressive : <MP4 URI>?Policy=eyJTdGF0ZW1lbnQiOlt7IlJlc291cmNlIjoiaHR0cHM6Ly9zZWN1cmUuZGF0YXBsYXN0aW
0-yFCqj2rSi8SXukB3oO5N6WtunUdpqfZlstRTJ9tX6k9xVjGLomjEclIu03wdJ4IrbONkSh9lS~V7QNjtgZtv69tYHvxusrg__&Ke
Pair-Id=9999999999

widevine or playready :

LA_URL : <ExpressPlay Token URI>/?ExpressPlayToken=AQAAAAbTKGIAAABQK2Nll44xo95DwyFp9Rcb1snIRwiJaLINE
Je1MaSMRF6QIx2lV_bPX5qY77Hu2V5xaWYL-SqBuZyR93TKW6tf1piINl2zVryFdAL0ZfJIGjepZb1kTFb6oEB0YDpGgVFC