Adopting DASH and Multi-DRM for Video Delivery

An Obscure Change in Browser Architecture Presents a Great Opportunity for Change

A Viaccess-Orca White Paper

viaccess·orca

Copyright

The information in this document is subject to change without notice. Viaccess S.A nor Orca Interactive warrant that this document is error free. If you find any problems with this documentation or wish to make comments, please report them to Viaccess-Orca in writing at documentation@viaccess-orca.com.

Trademarks

Table of Contents

Introduction

> “Unless video providers move quickly, they will lose the ability to serve half of their PC users: anyone using Chrome”

Multiscreen video is a now reality that consumers enjoy every day. While it may not be perfect, today’s online video experience usually ‘simply works,’ and it often attains a level of quality that rivals traditional TV. If we notice video quality at all, it’s more to comment about how good it is, and less to complain about errors and buffering. To get to this point, content owners, service providers, application developers and the underlying enabling technologies have all evolved together, and so far, the evolution toward anytime anywhere video on any device has been relatively smooth. But behind the scenes, it hasn’t been simple.

One of the biggest challenges has been software. Over the years, the developers of Web browsers, video streaming and online video content protection platforms have evolved their proprietary offerings in different directions in an effort to create vendor lock-in and thereby capture market share. As consumer devices proliferate, the problem has only grown: each type of device uses different sets of software to make up the total video experience. Software fragmentation has made it an ongoing challenge for video providers to present a common experience - and virtually impossible to use the same combinations of browser, video player and content protection - across all devices.

To address this situation, several recent technical standards, used together, gives content providers and video distributors a common set of tools to specify the formatting, playback and protection of the video experience without having to address proprietary software directly.

These standards are:

- MPEG-DASH, which provides a standardized alternative to proprietary video formats for adaptive bit-rate streaming,
- HTML5 and its Encrypted Media Extensions (EME) architecture, which specifies a common security framework, and,
- The Common Encryption (CENC) model, which specifies a common set of rules for content protection using Digital Rights Management (DRM).

In recent years, the presentation and streaming aspects of HTML5 and DASH have been in the industry spotlight, but their security aspects have seemingly taken a back seat. As a result, many video providers have taken the stance that there’s no rush to transition to HTML5 and DASH.

In 2013, this situation quietly changed, when Google announced that it would be deprecating the existing plug-in architecture of its Chrome browser and enforcing HTML5 EME. In September 2015, the transition will be complete and the old architecture will be discontinued altogether. This seemingly obscure change will have a huge impact: more than half of all video consumers on PCs use Chrome. Support for HTML5 has gone from a “nice to have” to a video provider imperative.

Because of the ways that different software vendors are addressing this situation, there's a genuine possibility that in September, video providers who don't pay careful attention and migrate accordingly will lose the ability to serve significant percentages of their end users. This can damage the video provider's reputation.

The good news is that although HTML5 EME, CENC and DASH represent significant breaks from the past, we believe strongly that these standards also present video providers with an uncommonly good opportunity. Implementing them will help video providers reduce time-to-market and create consistent video experiences across devices in the long term.

This paper details the situation and offers specific recommendations to help video providers manage their way through the transition to DASH and multi-DRM smoothly and proactively as they set their service road maps toward the future.

> “ Support for HTML5 has gone from a “nice to have” to a video provider imperative. Standards such as HTML5 present video providers with an uncommonly good opportunity ”

Online Video Delivery and Fragmentation

> “Content owners and distributors know that the theft of their intellectual property may be all that stands between profitability and business failure, making them highly motivated to protect themselves from piracy”

Together, four key categories of technology work together to enable the secure delivery and playback of video delivered over the Internet: adaptive bit-rate streaming, client software, content security, and device operating systems. Multiple proprietary approaches compete within each of these categories.

Adaptive Bit-rate Streaming

The first enabler of video streaming is the technique of streaming itself. Adaptive bit-rate (ABR) streaming has become the preferred method to distribute video over unmanaged networks, utilizing HTTP, the Internet's Hypertext Transfer Protocol. ABR enables a video provider to publish multiple versions of a particular video together, each version having a different resolution. Lower resolution versions take less bandwidth to distribute.

Adaptive streaming is designed to compensate for changes in available bandwidth, and its advantages are particularly evident with wireless access, in which physical obstructions (such as walls in a home) and changes of surroundings (such as happen in a moving vehicle) can result in unpredictable changes in bandwidth. ABR detects these changes and swaps between lower and higher resolution versions of the video without interrupting the overall experience.

It happens that the vendor landscape for ABR is dominated by a small number of powerful companies. Despite the common HTTP delivery protocol, Adobe's Flash-based HTTP Dynamic Streaming, Apple's HTTP Live Streaming (HLS), and Microsoft's Smooth Steaming formats are proprietary, and therefore are different and incompatible with one another. Furthermore, Microsoft's Silverlight player and Adobe's AIR and Flash players only work with Microsoft and Adobe encoding, respectively.

Browsers and the Forced Migration to HTML5

When they were invented in the 1990s, Web browsers were very limited in functionality. For that reason, early browsers offered frameworks that allowed software developers to extend the functionality of browsers by using ‘plug-ins,’ eliminating any need to modify the browser itself. Plug-ins exist for many purposes, including the playback of multimedia and video content. One of the original Web browsers, Netscape Navigator, enabled extensions via an architecture called the Netscape Plug-in Application Programming Interface (NPAPI).

In 1998, Netscape's developer established the Mozilla Project, and made a version of the Netscape browser freely available as open source software. As a result, Mozilla became the basis of a variety of other browsers - including Google's Chrome and the open-source Firefox browsers – all of which continued to use the NPAPI. According to statcounter.com, Chrome had more than 50% market share for desktops as of May 2015.[1]

The other powerful PC browser suppliers are Microsoft, with Internet Explorer, and Apple, with Safari. Browsers also exist on devices other than PCs, where Chrome is also dominant. Chrome and Android together had about 43% share for mobile and tablet devices.

Although plug-ins have been the accepted way to extend the functionality of Web browsers, they have never been an ideal solution. Every type of device is unique, and poor integration may sometimes cause them to be unstable or to function as an entry points for hackers. In addition, plug-ins have been frustrating for consumers that don't care about technology and often are not in a position to understand why their videos suddenly will no longer play.

Believing that plug-ins placed an unnecessary burden on device memory and processing resources, Apple objected to the plug-in approach altogether. Instead, Apple began to champion the HTML5 standard from the World Wide Web Consortium (W3C), which defines video as an object that can be played natively in browsers, without the need for plug-ins.

In 2010, Apple announced that its mobile devices would no longer support Adobe Flash, which represented a turning point that essentially forced HTML5 onto the roadmap for any category of video consumer electronics device where Apple offers a product. But for Web browsers other than those from Apple and Microsoft, the NPAPI remained.

But it wasn't until late in 2013, when Google, the developer of the Chrome Web browser, announced [2] that it would be transitioning Chrome from NPAPI to HTML5's Encrypted Media Extensions, and will disable NPAPI altogether in September of 2015. Suddenly, HTML5 isn't just a technology of casual interest. Unless video providers implement video players that support HTML5 EME, they will lose the ability to serve half of their PC users: anyone using Chrome.

Security

The third enabling category is security. Security for adaptive streaming to unmanaged devices is implemented through digital rights management (DRM) rather than by using the Conditional Access systems traditionally used by TV service providers. In DRM, encryption is applied to the content itself, rather than to the connection. Video player software incorporates the technology that decrypts the content, once the user is authenticated.

Predictably, Apple, Microsoft and Adobe each have their own proprietary DRM to complement their browsers: FairPlay, PlayReady and Primetime, respectively. Again, their architectures differ from one another and are therefore not directly interchangeable. To complicate matters further, each of these software companies implement their DRM with their own video players.

To secure streaming video content in pay TV applications, Microsoft PlayReady has become the most widely-used of the three. A fourth security technology in widespread use is Google's Widevine Technologies DRM platform, which offers two security options. Widevine Classic is meant for downloaded and on-demand video, while Widevine Modular is designed for live streaming of MPEG-DASH. This paper discusses DASH in the next section.

Operating Systems

A fourth source of fragmentation is the fact that different types of devices run different operating systems. One might hope that the same software can be implemented across all devices of the same type, but in some cases, the opposite is true. Google's Android platform is notorious for fragmentation. OpenSignal reported 18,769 distinct Android devices as of August 2014,[3] which makes it extremely difficult to rely on the native Android API to deploy a premium video service. A similar case can be made for Linux.

The Impact of Fragmentation

> “When one considers all of the permutations and combinations of devices, operating systems, streaming techniques, security, and video player software, the challenge facing video providers becomes clear”

When one considers all of the permutations and combinations of devices, operating systems, streaming techniques, security, and video player software, the challenge facing video providers becomes clear.

Careful readers may have noticed that this paper is focusing on video playback on devices other than TV set-top boxes. The historical focus for pay TV operators, broadcasters and Telco's has been to provide their service on their own set-top boxes. Although any given video provider might have several models in service at a particular moment, the number of models is limited and the service provider can specify the technology inside. Also, software integrations for set-top boxes go through extensive validation. Hence, services to set-top boxes are not particularly at risk.

Addressing Fragmentation through Standards

Together, three recent technical standards provide a clear roadmap toward overcoming the fragmentation we've described:

- The MPEG-DASH video standard, which provides an alternative to proprietary streaming video formats,
- The W3C Encrypted Media Extensions (EME) architecture within HTML5, which specifies a common framework for secure video plug-ins, and,
- The Common Encryption (CENC) standard, which allows content companies to specify security using a common set of rules

Together, these standards allow application developers to implement media presentation, playback and content protection use cases without having to specify how they are accomplished. This section reviews these standards in order.

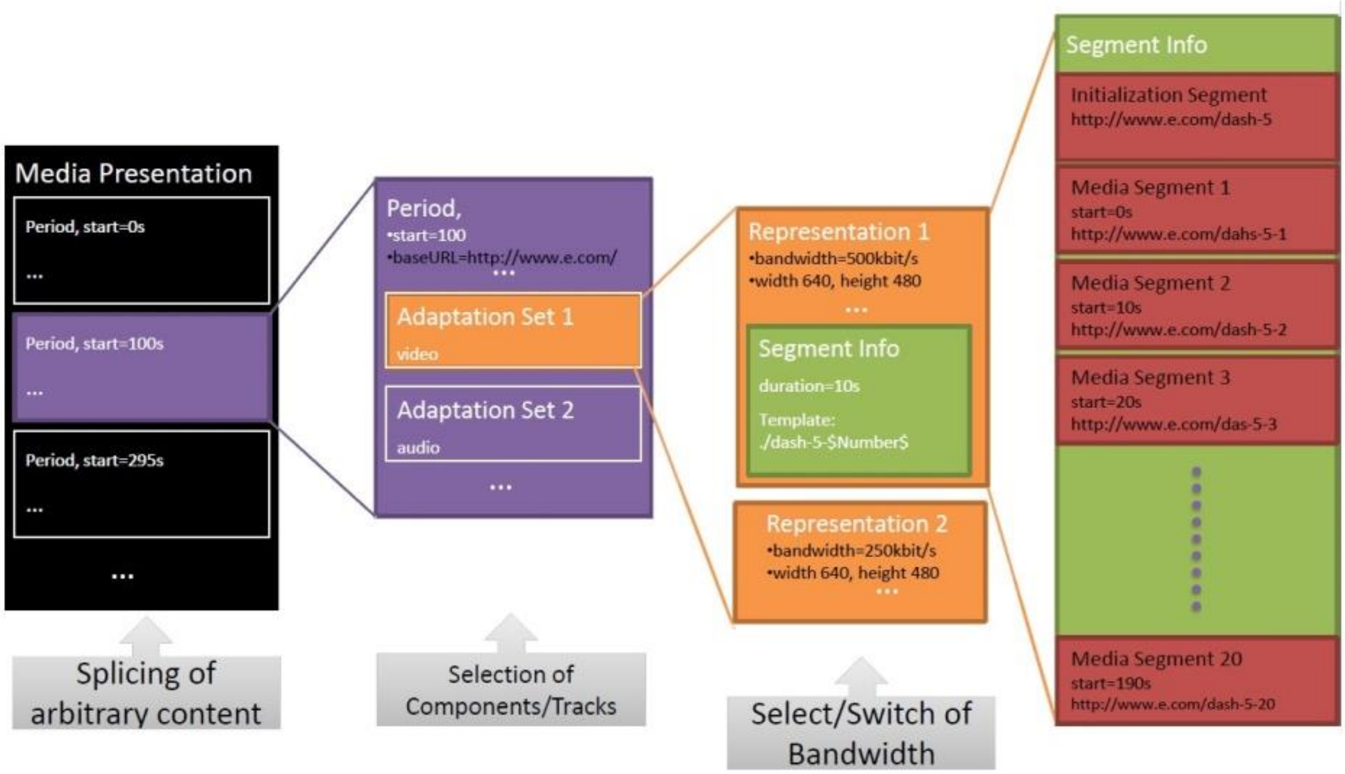
MPEG-DASH

To provide a standards-based alternative to the various available proprietary adaptive bit-rate streaming formats, a streaming technique called MPEG Dynamic Adaptive Streaming over HTTP (MPEG-DASH) was ratified as an international technical standard in 2012. DASH can be used to stream any video content format, including MPEG-2 transport streams (which contain usage rules in transport stream headers), and content packaged within ISO-BMFF (Base Media File Format) containers, which include data (e.g. video and audio elementary streams) and metadata (such as protection rules, timing information and codec).

DASH supports all of the functionality normally associated with pay TV video delivery, including live, on-demand, time-shifted and cloud-based delivery, interactivity, ad-insertion, multiscreen delivery, multiple language support and the delivery of graphics, animations, subtitles, and other data that compliments the audio-visual content.

DASH streams are associated with a manifest or index file called the MPEG-DASH Media Presentation Description (MPD), which is defined in the ISO/IEC 23009-1 technical specification.

Figure 1 – MPEG-DASH Media Presentation Description (MPD)



Source: Thomas Stockhammer (Qualcomm)

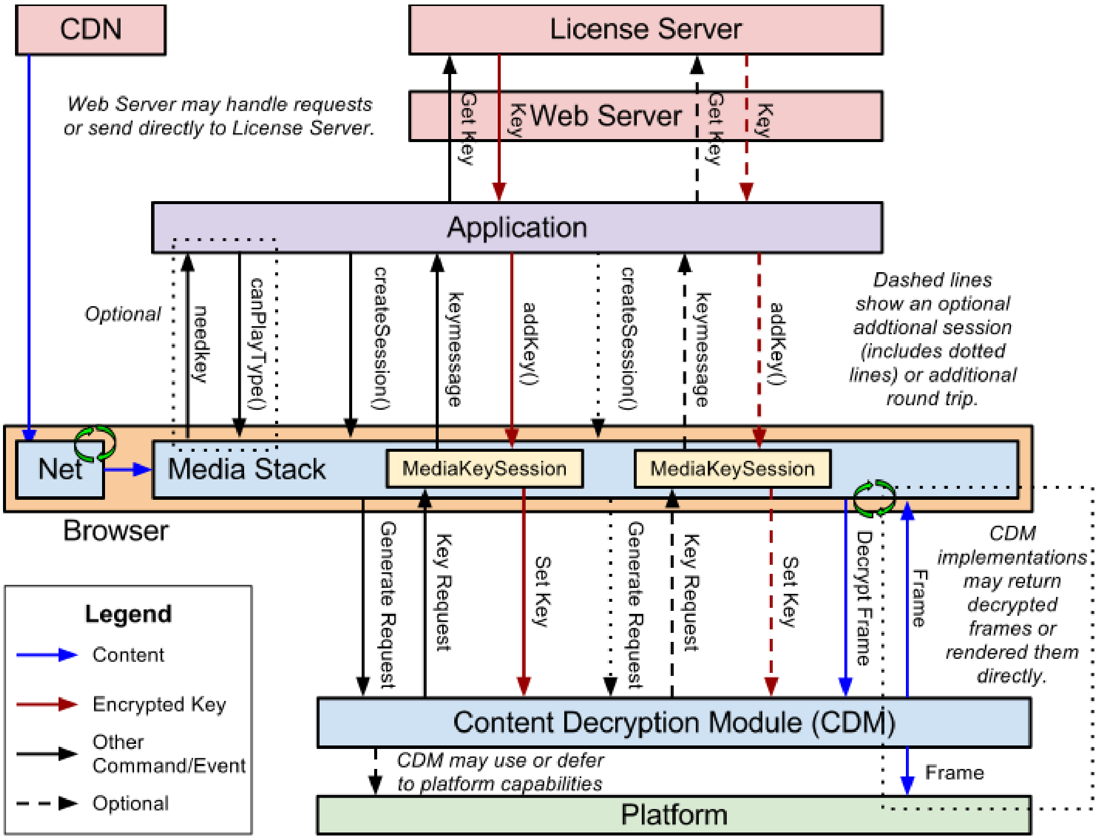
W3C Encrypted Media Extensions (EME)

To address the fragmentation of browser platforms, the World Wide Web Consortium (W3C) introduced HTML5. HTML5's Extended Media Extensions (EME), give HTML5 browsers a standardized framework to recognize encrypted media, and an API to control the playback of encrypted content. The API enables applications to identify, select and implement systems that interact with encryption, including DRM; although DRM is not mandatory.

Rather than implementing security specifically for each individual browser and its plug-ins, the EME standard provides an architecture that handles playback of encrypted video in the same way for all browsers. The module that handles the decryption and playback itself is called a Content Decryption Module (CDM). The details of key exchange and authentication are managed by the CDM. In order to support the W3C EME architecture, each individual DRM supplier must update its plug-ins so that they function as CDMs within the overall EME architecture.

The following diagram presents an abstract view of EME. The diagram is read from left to right.

Figure 2 – Generic EME Architecture



Source: W3C

Information about the characteristics of the video content carried with the content indicates, among other things, whether or not the content is encrypted. If it is encrypted, the browser establishes a session with a license (key) server through the application.

Once the browser's request has been authenticated and authorized to view the content, keys are delivered through the application and back to the CDM, which then decrypts and plays back the content. Content packaging, authentication, and key delivery are all separate processes that do not directly involve the CDM.

To date, only Google's Chrome browser and Microsoft's Internet Explorer for Windows 8.1 comply with the EME/CDM architecture. However, the Microsoft Silverlight player for Smooth Streaming, which is widely used in pay TV "TV Everywhere" and premium OTT video applications, is not being migrated to EME. So in effect, Chrome customers are being disrupted for all legacy content packaging/delivery in Microsoft Smooth Streaming (PIFF) format. Video providers distributing their content in Microsoft Smooth Streaming using PlayReady DRM, with the expectation that the Silverlight player will be invoked as a plug-in will therefore lose their ability to reach Chrome users.

A second issue is that EME can't enforce vendor neutrality. Even though Chrome is built on the open source Chromium code-base, and a PlayReady CDM for Chromium has been developed for Chrome, Google still publishes and controls all of the "libraries" associated with their version of Chromium. Therefore, PlayReady support in Chrome is a political issue not a technical one.

> “ PlayReady support in Chrome is a political issue not a technical one ”

Common Encryption

Instead of calling for specific DRMs for content protection, MPEG-DASH endorses a Common Encryption model (abbreviated CENC), which allows content publishers to specify the encryption algorithm and DRM with which they prefer to protect their content.

In other words, even though there is no single type of video encryption, there is a common model for implementing it. By defining a Protection System Specific Header as the single location to store private DRM information in the content, CENC provides a common online video encryption model that supports Adobe, Microsoft, OMA, Marlin and Google/Widevine DRM platforms.

This allows the publisher to publish content from different sources, in the formats that are appropriate to individual consumer end-devices. The DASH Industry Forum publishes generic and protection-specific identifiers [4] for content publishers, so the publisher can choose the protection system and encryption for a given distribution of content that the publisher determines to be most appropriate for the content and the player devices being targeted.

Over the past several years, video processing vendors have implemented support for DASH and CENC in their products, but by adhering to the principle of "if it's not broken, don't fix it," the momentum of content publishers to fully embrace and transition to these standards for video distribution has been weak. As a result, multiple streaming formats and encryption schemes have remained in widespread use.

Other Relevant Standards

Although it is not directly related to the discontinuation of NPAPI or the transition to MPEG-DASH, a new video compression technology happens to be transitioning into commercial availability at this time: High Efficiency Video Coding (HEVC, defined as the ITU-T H.265 standard). Compared with H.264, HEVC takes about half the bandwidth to deliver to a consumer device. Because of this, an operator can deliver twice the content using the same network capacity or the same amount of content to twice as many devices – or some mix in between.

If any aspect of video delivery does not accommodate HEVC, an operator's ability to maximize subscriber reach is hampered. It would make sense for operators to opt for online video players that support HEVC, but not all of them do. For example, the Widevine video player used with Google's Chrome browser uses only the H.264 baseline profile. One reason may be that Google offers an alternative codec to HEVC, called VP9, which is not expected to be used in pay TV set-top box applications.

Not a Perfect Solution

> “ The new standards replace many vendor-specific approaches to implementing security for ABR video with a single architectural approach ”

Even though HTML5, EME, CDMs and DASH were intended to reduce fragmentation by offering a common architecture and a common approach to authentication and delivery, different browsers will continue to use different streaming and encryption solutions, as shown in the following table.

Figure 1: Content Decryption Modules, by Browser

Browser Platform	CDM Provider
Google Chrome v35+	Google Widevine
MSIE 11+ (Windows 8.1+ only)	Microsoft PlayReady
Apple Safari v8+	Apple FairPlay
Firefox	Adobe Primetime DRM
Android 4.4+	Google Widevine modular
iOS 6+	Apple FairPlay
Windows Phone 8.1+	Microsoft PlayReady
ACCESS Netfront	Marlin / Intertrust

Source: Streaming Media 5

This situation creates challenges for video security vendors in the short term, as they migrate their products to the CENC model. A cynic might say that these new standards are replacing one type of fragmentation with another.

However, it’s more accurate to say that the new standards replace many vendor-specific approaches to implementing security for ABR video with a single architectural approach. Ultimately, this new approach will take significant time out of the video provider’s innovation process.

Time-Sensitive Issues: What to Do Next?

This discussion of standards might distract some readers from the fact that this situation is time-sensitive, as Google follows through on its commitment to discontinue Chrome's NPAPI. Beginning in November 2014, NPAPI plug-ins were disabled by default.[6] In April 2015, NPAPI was 'unpublished' by Google in Chrome version 42, but was still available on an exception basis. This exception is to be removed in September 2015 with Chrome version 45.[7]

Any video provider that hasn't dealt with this situation by then runs the real risk of losing consumers.

Roadmap Alternatives

Although the deprecation of NPAPI forces a software migration in the browser, it's also a catalyst to update other aspects of their video delivery process.

Video providers have a range of choices:

- Choose not to support HTML5's Encrypted Media Extensions, and inform their consumers to change to different browsers. Consumers establish their usage habits and software preferences over time, and those habits are difficult to change. Any video provider that asks users to change browsers may lose some consumers
- A second choice is to identify temporary workarounds (for example, to temporarily re-enable the NPAPI on an exception basis). This alternative will be gone in September.
- A third is to move premium video playback to a software player that is not associated with the browser. This is Microsoft's approach.[8]
- The fourth - and preferable - long-term approach is to move to MPEG-DASH and multi-DRM support.

In reality, video providers should be prepared to do all of these things.

Viaccess-Orca's Connected Sentinel

To facilitate this transition, Viaccess-Orca (VO) provides the Connected Sentinel multi-DRM platform, which enables video providers to deploy premium video services across the entire diversity of targeted devices.

With Connected Sentinel, a single platform enables multiple choices for the packaging and encryption of video content. Video providers can use VO's own content packager, or use VO key management servers in conjunction with third-party content packagers; including transcoders and video/origin servers from leading vendors like Anevia, Envivio, Harmonic, and others.

The Viaccess-Orca solution incorporates a multi-DRM license server that enables video providers to deliver a single set of MPEG-DASH video content to multiple consumer devices, regardless of whether the device is using Microsoft PlayReady, Widevine Modular DRM, VO proprietary DRM, or another DRM solution; and it's designed to easily integrate with new ones.

Connected Sentinel manages the complexity of security as it evolves, while helping to reduce the overall cost of providing premium online video services. VO upgrades its platform on a continuous basis, both to take the evolving requirements of content owners into account, and to accommodate new features and new security requirements from DRM technologies providers. This approach allows video providers to focus more on differentiating their services and satisfying their end users.

Conclusions

> “We believe that EME, CDMs, DASH and CENC are good for video providers in the long term, and good for the online video industry”

The current fragmentation of Internet video delivery has been two decades in the making. It's the result of vendors ranging from Adobe and Apple to Microsoft, Google and others, to capture market share by using proprietary encryption and digital rights management, and to control the media flow to their devices. All of this took place under the guise of providing better security.

Fragmentation has placed real hardships on publishers, content providers and service providers, who must reach their entire audience, regardless of the devices that they use. Google's discontinuation of the NPAPI in Chrome is an important move toward having a consistent and standards-based delivery framework that helps video providers overcome the hardships of fragmentation.

Google's move also forces video providers to make some critical technology decisions, and these decisions are time sensitive. One choice is to do nothing: to not support the W3C's Encrypted Media Extensions architecture, at the risk of losing consumer-facing and advertising revenue from Chrome users that can no longer play content.

At the other extreme, a second choice might be to support *only* browsers that have migrated to EME, which would create the same problem in reverse: cut off all users *except* for those using EME-capable browsers. At the time of this writing, only Chrome and Microsoft Internet Explorer for Windows 8.1 comply. A third approach is to ask Chrome users to switch browsers. Because all of these choices are disruptive, none of them are satisfying.

We believe that the right way forward is to innovate, by migrating incrementally toward the standards-based approach; to support EME and Content Decryption Modules as they become available, while maintaining support for existing plug-in approaches until they make the transition.

The migration to EME, CDMs, MPEG-DASH and CENC will not take place overnight. For example, just as the past decade has seen a transition from MPEG-2 to MPEG-4 and H.264, there will now be a transition from H.264 to HEVC. One case in which video distributors will need to support content in both formats is with advertising, where the primary video programming might be available in HEVC while the ads are H.264. To address this situation, video providers can adopt players that support both.

Despite this sometimes confusing situation, we believe that EME, CDMs, DASH and CENC are good for video providers in the long term, and good for the online video industry, because it will enable content and service providers to reach all audiences, regardless of device, video format, or method of content protection.

Recommendations

Viaccess-Orca has several specific recommendations for video providers, regarding their roadmap for browsers, content production, and client-side software

Browser Recommendations

- Continue to support existing streaming formats and DRM. Have a plan to migrate each type of client, to coincide with the timeline of deprecation,
- Consider alternatives to NPAPI that exist in Chrome. In cases where standard web technologies are not yet sufficient, developers and administrators can use NaCl, Apps, Native Messaging API, and Legacy Browser Support to transition from NPAPI. Moving forward, our goal would be to evolve the standards-based web platform to cover the use cases once served by NPAPI)

Content Production Recommendations

To reduce the cost of content packaging, we recommend the following:

- Rely on HLS for iOS devices, since Apple does not allow the publication of application that will streams over 3G/4G network with another technology
- Add MPEG-DASH output capability at the headend, using encryption based on Common Encryption and a multi-DRM scheme. This enables video providers to support Microsoft PlayReady and Widevine Modular DRM immediately
- Because some service providers have deployed set-top boxes that make use of the Microsoft Smooth Streaming to enable VOD or catch-up content, one sensible approach might be to deliver live content as MPEG-DASH, and on-demand content in Smooth Streaming. Video providers will realize a savings by not having to cache both MPEG-DASH and Microsoft Smooth Streaming streams in distribution
- To minimize the number of video profiles stored in the origin servers, we recommend on-the-fly video packaging (depending on encoder capabilities and the amount of available storage)

Client Side

- Relying on an SDK that provides a video player with an integrated DRM agent is still the best option in term of cost of operation in order to provide a premium video service that can scale on all devices (Android but also iOS) with the operator selected look and feel
- Deploy only the CDM that is the “most native” to the browser of the device that the video provider wants to support

Additional Strategic Recommendations

- Adopt a rights management platform that accommodates key management communications from any type of client and allows the video provider to add or change DRM as necessary
- Understand the other benefits, and why. Clearly identify how the use of DASH and multi-DRM reduces expenses and time-to-market

- Working with a partner such as VO that has validated end-to-end workflow on multiple DRM technology, will benefit to service provider since they will be able to rely on the cross platform testing performed by the partner thus reducing testing time, avoiding known pitfall, so overall better quality product, reduce in cost and time to market

Download the complete guide to Connected Sentinel – VO's multi-DRM platform

Glossary

- **ABR**: Adaptive Bit-rate Streaming. A generic name for a type of technique used to distribute video over unmanaged IP networks. Several proprietary approaches exist, as does a technical standard
- **Adobe HDS (HTTP Dynamic Streaming)**:[9] A proprietary ABR technology from Adobe Systems
- **API**: Application Programming Interface. A point of contact designed to enable different computer-based processes to interact with one another
- **Apple HLS (HTTP Live Streaming)**:[10] A proprietary ABR technology from Apple
- **ISO-BMFF**: A specification for the structure and content of a stream of content
- **CDM**: Content Decryption Module. The client-side software module within the W3C EME specification
- **CENC**: Common Encryption, a technical standard that specifies standard encryption and key mapping methods, maintained by the International Organization for Standardization as ISO/IEC 23001
- **DASH:** Dynamic Adaptive Streaming over HTTP
- **DRM**: Digital Rights Management. A generic name for frameworks used to encrypt, authenticate, and decrypt digital content
- **EME**: Encrypted Media Extensions. [11] A standardized API within the HTML5 standard to accommodate decryption of protected content, from the W3C Consortium
- **HEVC**: High Efficiency Video Coding. A technical standard published by the International Telecommunications Union, Telecommunications branch (ITU-T) as the H.265 specification
- **ISO**: The International Organization for Standardization, a technical standards organization
- **IEC**: The International Engineering Consortium, a technical standards organization
- **Microsoft Smooth Streaming**:[12] A proprietary extension to Microsoft's Internet Information Server (IIS) that streams ABR video to Microsoft Silverlight online media player software
- **Microsoft Silverlight**:[13] A developer tool set from Microsoft, used to create online video and interactive digital media experiences which are played by using the Microsoft Silverlight media player
- **Media Presentation Description (MPD)**: [14] A file distributed with MPEG-DASH streams which contains metadata about the stream. Defined in ISO/IEC 23009-1
- **MPEG-DASH**:[15] Motion Picture Experts Group Dynamic Adaptive Streaming over HTTP, a technical standard for adaptive bit-rate streaming maintained by the International Organization for Standardization as ISO/IEC 23009
- **DASH-IF Industry Forum (DASH-IF)**: An industry association that publishes guidelines [16] for the implementation of MPEG-DASH
- **NPAPI**: Netscape Plug-in Application Programming Interface. An architecture for adding new functions to Web browsers

- **W3C**: World Wide Web Consortium. A technical standards organization
- **Widevine**: A developer of DRM software now owned by Google. Widevine DRM is Google's default DRM for online video solutions offered by Google

About Viaccess-Orca

As a leading global provider of content protection, delivery, and discovery solutions, Viaccess-Orca is shaping the ultimate content experience. Through its integrated range of business-savvy products and solutions, Viaccess-Orca helps service providers in the cable, DTT, satellite, IPTV, and OTT industries gain a competitive edge in today's rapidly evolving multiscreen environment. By enabling service providers to securely deliver an engaging user experience on any device, Viaccess-Orca is reinventing the entertainment landscape. Viaccess-Orca is part of the Orange Group.

For more information, visit www.viaccess-orca.com, follow us on Twitter @ViaccessOrca and Linkedin.

[1] *StatCounter Global Stats*. Web page. StatCounter. Accessed May 1, 2015. See: http://gs.statcounter.com/#desktop-browser-ww-monthly-201405-201505-bar

[2] *Saying Goodbye to Our Old Friend NPAPI*. Article. Chromium Blog. Google. Accessed May 2015. See: http://blog.chromium.org/2013/09/saying-goodbye-to-our-old-friend-npapi.html

[3] *Android Fragmentation Report, August 2014*. Market research report. OpenSignal. Accessed February 2, 2015. See: http://opensignal.com/reports/2014/android-fragmentation/

[4] *Content Protection*. Web page listing of content protection identifiers for generic and protection-specific content protection schemes. DASH Industry Forum. Accessed January 30, 2015. See: http://dashif.org/identifiers/protection/ and http://dashif.org/identifiers

[5] *The Changing Face of DRM: Where Do We Stand?* Article. Jan Ozer. February 2015. Streaming Media Magazine. See: http://www.streamingmedia.com/Articles/ReadArticle.aspx?ArticleID=101319&PageNum=2

[6] *The Final Countdown for NPAPI*. Article. Chromium Blog. November 24, 2014. Google. Accessed May 2015. See: http://blog.chromium.org/2014/11/the-final-countdown-for-npapi.html

[7] *NPAPI Deprection Developers Guide*. Timeline and discussion of Google’s discontinuation of the NPAPI from Chrome. Web page. Google. Accessed May 2015. See: http://www.chromium.org/developers/npapi-deprecation

[8] *Out of Browser*. Web page. Microsoft Silverlight. Microsoft Corporation. See: http://www.microsoft.com/silverlight/out-of-browser/

[9] *HTTP Dynamic Streaming*. Informational Web page. Adobe Systems Inc. Accessed May 2015. See: http://www.adobe.com/products/hds-dynamic-streaming.html

[10] *HTTP Live Streaming*. Informational Web page. Apple Inc. Accessed May 2015. See: https://developer.apple.com/streaming/

[11] *Encrypted Media Extensions*. Technical specification for proposed EME API in HTML5. Edited by Dorwin (Google), Smith (Microsoft), Watson (Netflix) and Bateman. Editors Draft of 29 January 2015 accessed on January 30 2015. World Wide Web Consortium. See: https://w3c.github.io/encrypted-media/

[12] *Microsoft Smooth Streaming*. Informational Web page. Microsoft Corporation. Accessed May 2015. See: http://www.iis.net/downloads/microsoft/smooth-streaming

[13] *Microsoft Silverlight*. Informational Web page. Microsoft Corporation. Accessed May 2015. See: https://www.microsoft.com/silverlight/

[14] *MPEG’s Dynamic Adaptive Streaming over HTTP (DASH)*. Presentation to the European Broadcast Union (EBU). November 22, 2011. Thomas Stockhammer, Qualcomm. See: https://tech.ebu.ch/docs/events/webinar043-mpeg-dash/presentations/ebu_mpeg-dash_webinar043.pdf

[15] *MPEG-DASH*. Information Web page. Moving Picture Experts Group (MPEG). Accessed May 2015. See: http://mpeg.chiariglione.org/standards/mpeg-dash

[16] *Guidelines*. A Web page that links to completed and draft interoperability documents for MPEG-DASH. DASH Industry Forum. Accessed May 2015. See: http://dashif.org/guidelines/