INTEROPERABILITY, DIGITAL RIGHTS MANAGEMENT AND THE WEB

JOHN C. SIMMONS, MICROSOFT CORPORATION
DR. STEFAN ARBANOWSKI, FRAUNHOFER FOKUS RESEARCH INSTITUTE

SEPTEMBER 13, 2013

We are on the verge of an important inflection point for the Web. In the next few years commercial web video delivery utilizing new, international standards (DASH Media Ecosystem) will become commonplace. These standards will enable cross-platform, interoperable media applications and will transform the media entertainment industry, delight consumers and expand the nature of the Web.

Although all of the standards outlined below are necessary, the most significant change was the introduction of interoperable digital rights management technologies which enable the distribution of digital media on the open web while respecting the rights of content producers.

THE DASH MEDIA FRAMEWORK

The principle standards which will enable commercial web media receivers are: ISO MPEG Live Dynamic Adaptive Streaming over HTTP (DASH), ISO MPEG DRM-interoperable Common Encryption (CENC), fragmented MP4 encoded media which utilizes CENC – such as the UltraViolet Common File Format (CFF) or the Common Streaming Format (CSF), HTML5 Media Extensions under development in the W3C - Media Source Extensions (MSE), Encrypted Media Extensions (EME) and Web Crypto Extensions – and OAuth 2.0-based authentication (AuthN) and authorization (AuthZ) protocols such as the Online Multimedia Authorization Protocol (OMAP).

These standards have emerged rapidly, all appearing in the last three years, and they are being adopted by multiple ecosystem participants. They will redefine the way commercial media is delivered on the Web, and in doing so they will transform the Web itself.

We refer to this as the “DASH Media Framework” because, for many in the industry, the term “DASH” has become a catchall phrase for the entire new media stack, gathering to it not just the DASH specification itself, but all of the new web media standards which in principle can enable on-demand and live DRM-protected media consumption by standards-based browsers without the need for plugins.

Although the development of the DASH specification began as an effort to standardize adaptive bitrate streaming, the companies who contributed to this international specification effort evolved DASH into a generalized media presentation description language – including support for alternate audio language tracks, advertising avail signaling, closed caption tracks, content protection mechanisms, alternate audio codecs, second screen capabilities, etc. – aiming to include all the features broadcasters use today for cable and satellite television networks.

Today the 67 member companies in the international DASH Industry Forum are grooming "DASH" to become a general purpose live and on-demand media delivery stack. This is a revolutionary transition from a fragmented to an integrated media ecosystem; from service and device specific media encoding to generalized encoding common across services and devices; from service and device specific applications to Web-based media playback.

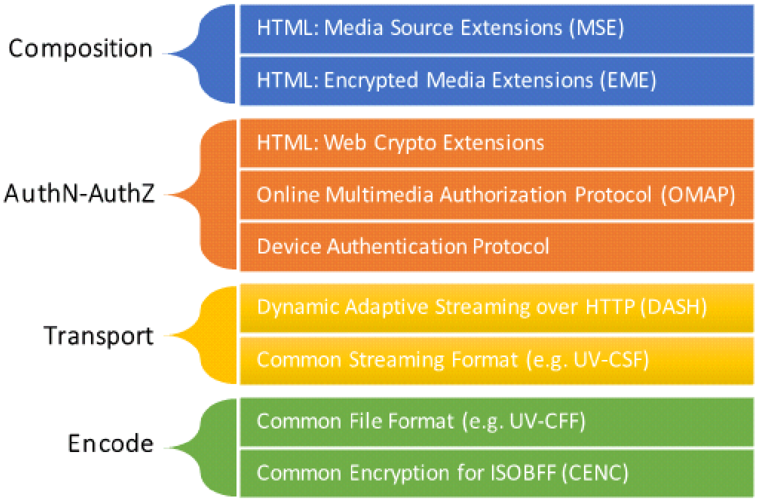
Composition
HTML: Media Source Extensions (MSE)
HTML: Encrypted Media Extensions (EME)
AuthN-AuthZ
HTML: Web Crypto Extensions
Online Multimedia Authorization Protocol (OMAP)
Device Authentication Protocol
Transport
Dynamic Adaptive Streaming over HTTP (DASH)
Common Streaming Format (e.g. UV-CSF)
Encode
Common File Format (e.g. UV-CFF)
Common Encryption for ISOBFF (CENC)

Figure 1 the DASH Media Stack

Interoperability, Digital Rights Management and the Web

DRM interoperability can be solved by utilization of the common encryption standard[1] (CENC) and the application of common encryption to the proposed HTML5 Encrypted Media Extensions (EME).

DRM-Interoperable Encoding

The key consumer experience challenge with DRM is the lack of interoperability – that the content is tied to a particular application on a particular device with a particular DRM technology. The state of the world in 2009 when common encryption was invented was that encoding formats themselves were DRM-specific. The problem then was, 'how to make encoded content work across DRMs?'

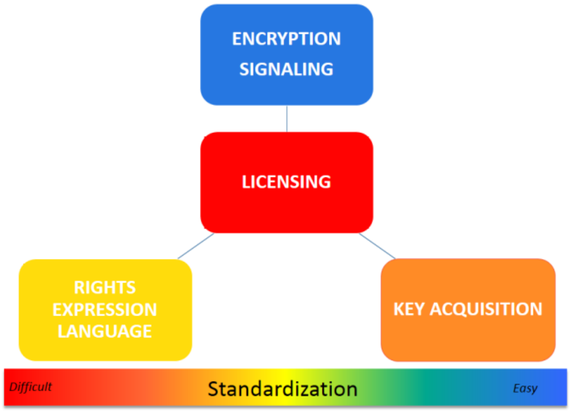

Figure 2 DRM Component Standardization

Without a **licensing** regime with compliance rules and robustness rules, there is no way to ensure that a DRM client will actually follow the rights expressed for the commercial content. Such licensing schemes are inherently difficult to standardize.

The decryption **key acquisition** mechanism invariably involves the client proving to a server that it was built by a company in good standing with the DRM provider, and as such the key acquisition protocol is also difficult to standardize.

[1] ISO/IEC 23001-7: 2011, "Information technology – MPEG systems technologies – Part 7: Common encryption in ISO base media file format files"

The **rights expression language** has an intimate relationship to the licensing compliance rules, so it is also difficult to standardize, although less so.

The **encryption** algorithm and the manner of **signaling** what DRMs can be used to decrypt the content is easy to standardize, which is precisely what is specified in the ISO MPEG Common Encryption standard.

The CENC specification standardizes encryption and the signaling of protection schemes while leaving rights expression languages and key acquisition protocols proprietary. It is transparent to the end user that the key acquisition requires a different backend server. With common encryption the content plays regardless of the application, the device or the underlying DRM.

Common encryption takes us one third of the way to solving DRM interoperability. The next step is to remove the need for service-specific applications on the target device – to provide a Web-interoperable DRM solution.

HTML5 Encrypted Media Extensions

Common encryption provides interoperable media content, but in order to have truly interoperable media playback, there would need to be a way to play back DRM-protected media in standard browsers without the use of proprietary plug-ins.

In 2011 both Microsoft and Netflix gave presentations at a W3C Web and TV Interest group meeting, hosted in Berlin by Fraunhofer FOKUS.[2] These presentations dealt with the need to support DRM-protected media in browsers. By 2012 Microsoft, Google and Netflix had submitted a joint proposal to the W3C HTML Working Group that would enable browsers to consume DRM-protected content without the use of plug-ins – the Encrypted Media Extensions (EME).

EME enables a JavaScript app to select a content protect mechanism and facilitate key acquisition. When combined with CENC, EME enable a web page to support multiple DRM systems without customization or the use of plug-ins, enabling interoperable commercial media consumption.

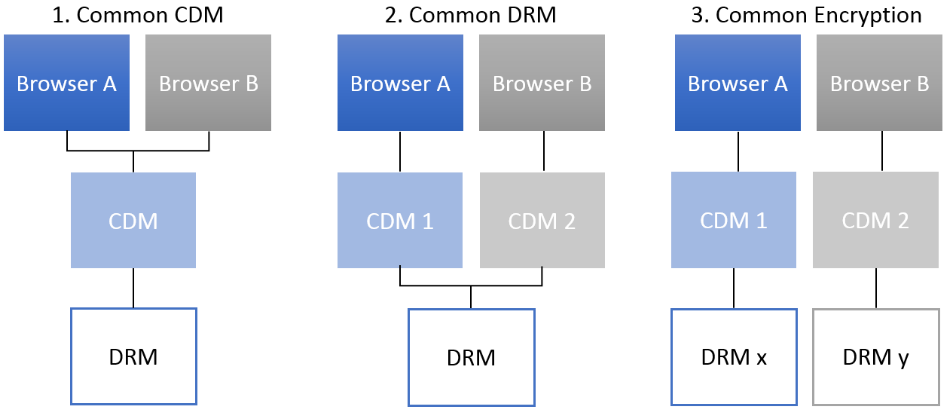

Figure 3 Content Decryption Module Interoperability

In EME, the portion of the browser which provides the EME functionality is the Content Decryption Module (CDM). CDM interoperability can take three forms – browsers can use a **Common CDM**, or they can implement separate CDM modules tied to a **Common DRM**, or they can use separate CDM modules and separate DRMs and rely upon **Common Encryption** for interoperability.

[2] Second W3C Web and TV Workshop, 8-9 February 2011, http://www.w3.org/2010/11/web-and-tv

All three approaches can work, but there are problems:

- **Security**: Enhanced content protection requirements make it highly likely that future DRMs will be more closely tied to hardware, with the actual CDM functionality happening outside the browser.
- **State interoperability**: if the CDM associated with a particular DRM is written by different parties, the state transitions of the CDM are likely to be inconsistent, effecting interoperability.
- **Licensing**: Many embedded devices will depend on the use of open source browsers. The open source browser community needs the ability to implement EME functionality without having to license CDM technology.

So CENC and EME only take us two-thirds of the way to solving DRM interoperability. The complete solution requires a means of enabling commercial media content to be played by open source browsers – to enable the DRM to be a platform component – ensuring security and state interoperability.

Open source browsers and digital rights management

All three of the remaining issues with a Web interoperable DRM solution are addressed if the DRM is baked into the platform. The question is how best to accomplish this.

The solution Microsoft has adopted is shown in Figure 4. A thin C++ wrapper is written on top of the PlayReady Device Porting Kit API, creating an object which is "hand in glove" with the EME MediaKeys and MediaKeySession objects. We call this wrapper the **CDMi** or **Content Decryption Module interface**.

This C++ wrapper enables PlayReady to project the W3C HTML5 EME object into the process space of a browser using the operating system's native RPC mechanisms. This is done in a way that ensures (1) the critical DRM decryption functions are not in the browser execution space; (2) the CDMi state transitions are consistent across all PlayReady implementations, and (3) the browser need not incorporate any PlayReady licensed components.

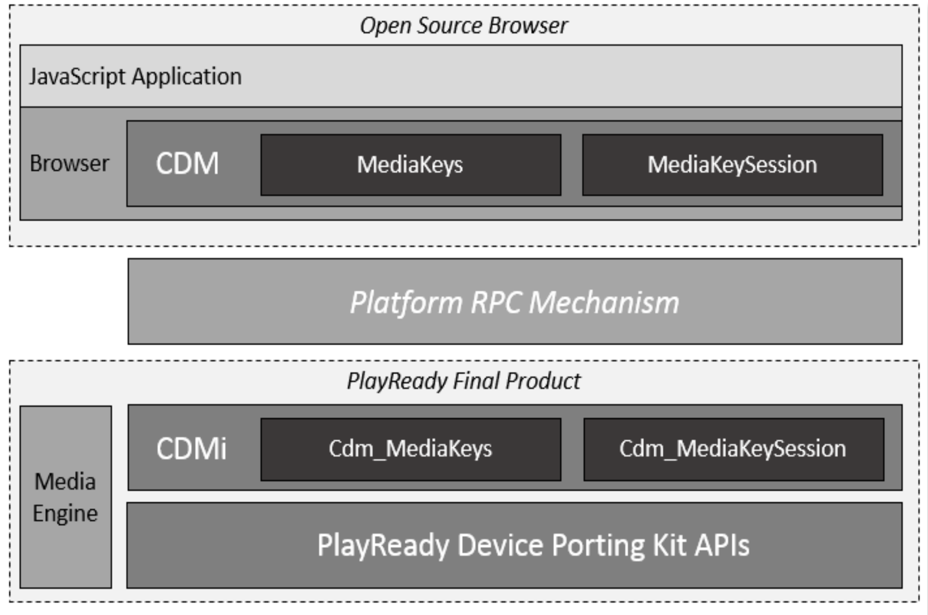

Figure 4 Open Source Access to a Platform DRM

The CDMi specification describes the logical mapping of the EME methods and events to the PlayReady Device Porting Kit APIs. Microsoft will make the CDMi interface public, so that any browser provider may create a PlayReady compliant Content Decryption Module (CDM), providing that the platform where they run supports a PlayReady CDMi. Televisions and set-top-boxes which incorporate the PlayReady

Device Porting Kit will be able to use the PlayReady CDMi to project DRM functionality into the browser of their choosing.

Combining Common Encryption (CENC), HTML5 Encrypted Media Extensions (EME) and a platform Content Decryption Module interface (CDMi) like Microsoft's solves DRM interoperability. It will enable the same media stream to be consumed, for example, on a Windows 8.1 tablet, a set-top-box or a smart TV – protecting the content owner's rights while enabling interoperable media consumption even on open source browsers.

These developments will expand the reach of traditional broadcasters, open the market for new niche online video distributors, revolutionize the consumer electronics industry and expand the utility of the Web well into the twenty-first century.