

Commercial Video Provider HTML5 DRM Requirements

Bob Lund – CableLabs (b.lund@cablelabs.com), August 10 2011

1. Abstract

Commercial Video Providers (CVP) want to deliver high value content to devices that use HTML5-based user agents for presentation of user interface and media playback. This necessitates a content protection scheme. This document describes high-value media delivery use cases and identifies new HTML5 requirements to support the use cases.

2. CVP Use-Cases

The following use-cases are important to CVPs.

2.1 *Delivery in Distribution Windows*

Commercial video providers deliver content to their users in a variety of, and potentially new, distribution windows. To do so, they must provide delivery solutions that enforce content owner security and usage rights requirements for those delivery windows.

2.2 *Support of Content Owner Property Rights*

Commercial video providers would like to deliver Ultraviolet, a.k.a. Digital Entertainment Content Ecosystem (DECE), content to their users. To do so, they must provide delivery solutions that conform to DECE security and usage rights solutions.

2.3 *Delivery to Personal Computer Platforms*

High-value content is delivered to personal computers. The HTML5 user agent may be:

1. An off-the-shelf browser such as Chrome, Firefox, Internet Explorer, Opera or Safari.
2. An application incorporating a browser downloaded from a service provider.

2.4 *Delivery to Retail CE Devices*

High-value content is delivered to a retail consumer electronics device with an embedded application. Several embedded application environments might exist:

1. Closed with no ability to change the application in the field.
2. May or may not have hardware support for security.
3. Field-upgradeable with or without hardware support for firmware or application secure download.

3. Use-case requirements

This section describes requirements derived from the use-cases.

3.1 *General Web Delivery Requirements*

1. If Web users are to have access to a wide range of content, the Web delivery platform must provide support for the property rights of content owners.

3.2 *User-agent Requirements*

1. The HTML5 user-agent needs to support one or more digital rights management (DRM) systems¹.
2. If the user-agent doesn't have support for a DRM required by the content it should be able to download an available module that supports playback of content using that DRM.
3. The device platform may provide hardware-based root-of-trust which should be available for use by the DRM module.
4. Web content and DRM modules should be able to determine the level of trust of the device.

3.3 *HTML5 Media Element Requirements*

1. Web content should use the video and audio element interfaces to playback DRM protected content. All of the features that exist for the video and audio element should be available when playing protected content, e.g. have child track elements, be assignable to a media controller object.
2. The HTML media resource selection algorithm should include resource selection based on user agent DRM support.
3. Web content should be able to determine certain DRM-related playback events and errors.
4. Web content should be able to determine which DRMs are supported by the user-agent.
5. The DRM solution needs to work for content accessed directly by a URL or via a URL to a media presentation description (a.k.a. manifest file).

¹ In this paper DRM is used to refer to a more general class of content protection, which includes link protection schemes. This recognizes the transition from link protection to more expressive DRM systems while acknowledging that link protection schemes are considered as viable content protection schemes for certain content.