APPENDIX A

DSTAC REPORT TEXT

A. Proposal 1: DSTAC WG3 HTML5 Security API's Proposal

1. Summary

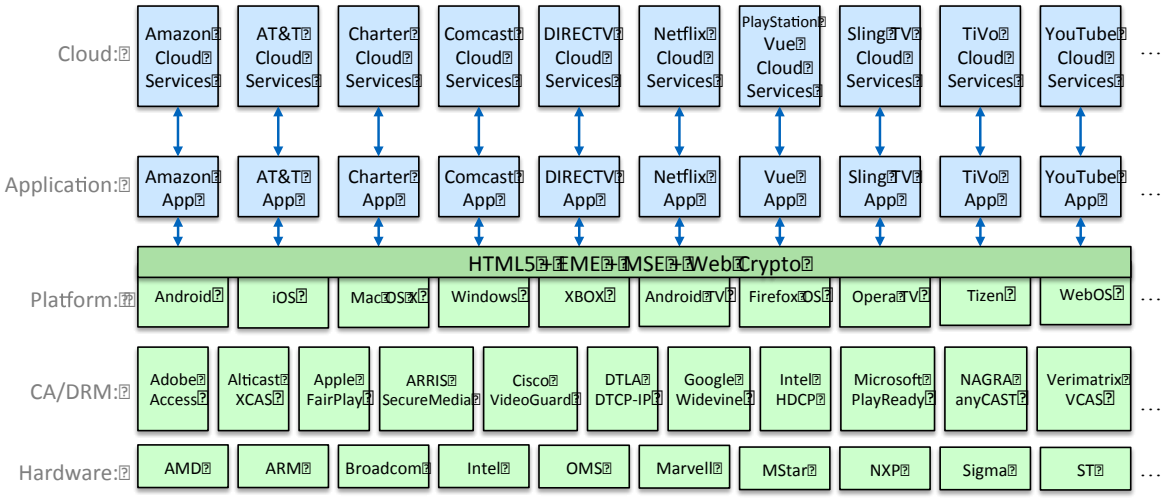

Figure 1 HTML5, EME, MSE & Web Crypto

MVPD/OVDs and CE/CPE companies should adopt the HTML5 media model with Encrypted Media Extensions [EME], Media Source Extensions [MSE] and Web Crypto [WEBCRYPTO] as a non-exclusive, open standard software downloadable security system interface between MVPD/OVD services and consumer electronic devices.

Video providers and distributors have developed a common and open approach to deliver streaming media based on the Internet and the HTTP protocol in particular. HTML has emerged as a strong foundation on which video providers and distributors have based such services. This proposal seeks to leverage these same market forces.

HTML5 is a full application foundation, supporting both security elements (corresponding to DSTAC WG3) and non-security elements (corresponding to DSTAC WG4.) The following proposal will only discuss HTML5 related to the FCC DSTAC WG3 security element requirements.

HTML5 is the open standard defined by the World Wide Web Consortium (W3C) as the cornerstone of the Open Web Platform. Many MVPDs, OVDs, vendors, and members of the DSTAC are members of the W3C, including Adobe, Apple, AT&T, CableLabs, Cisco, Comcast, Cox, EFF, Facebook, Google, HBO, Huawei, IBM, Intel, Microsoft, Mitsubishi, MovieLabs, Mozilla, NAB, Netflix, Opera, Samsung, Sony, Verimatrix, Viacom and Yahoo [W3CMEMBERS].

HTML5 is supported by all major browsers (both on PCs and embedded devices) including Apple Safari, Google Chrome, Microsoft Edge, Mozilla Firefox and Opera.

HTML5, EME, MSE and Web Crypto are being deployed across the Web today by multiple vendors on hundreds of millions of devices, including mobile, PCs, TVs, set-tops and game machines. HTML5 is a software system portable across content protection systems, device hardware and CPU architectures (including AMD, ARM, Broadcom, Intel, OMS, Marvell, MStar, NXP, Sigma and ST).

HTML5, EME and MSE are already being used for multiplatform commercial services such as Netflix, YouTube movies, Google Play, and Apple movies. It is also the basis for multiplatform DLNA VidiPath cloud services.

W3C HTML5 provides a uniform architectural framework for access to media streams. HTML5 uses IETF MIME types for identifying media formats. HTML5 is sufficient to play unencrypted media and link level protected media (e.g. DTCP-IP or HDCP).

EME extends HTML5 to support common-encrypted media decryption by one or more DRM. MSE extends HTML5 to support adaptive video. MSE and EME are designed to work closely together. Almost all content protection companies surveyed and discussed in WG3 now support or plan to support EME, including Adobe Access, Alticast XCAS, Apple FairPlay, ARRIS SecureMedia, Broadcom, Cisco VideoGuard, Google Widevine, Intel SGX, Microsoft PlayReady, NAGRA anyCAST and Verimatrix VCAS.

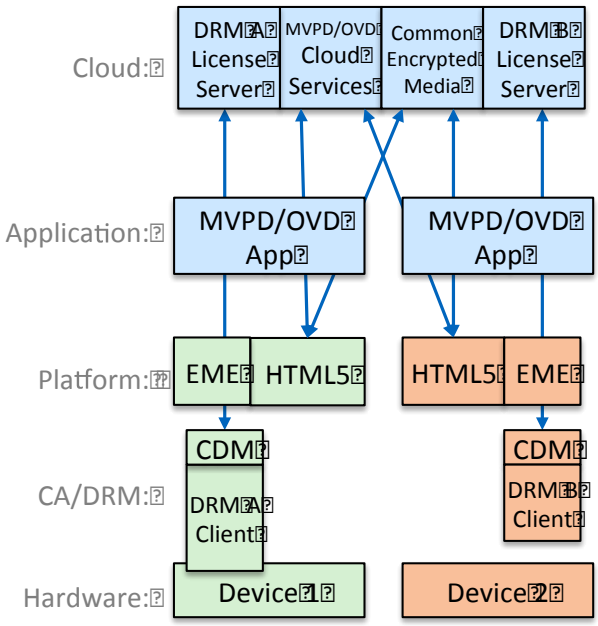

Figure 2 HTML5 EME Common Encryption

Common Encryption (AKA key-sharing or simulcrypt) allows multiple security systems of potentially diverse and divergent design to simultaneously operate on the same content stream or file. This powerful property acts a safety net for choice and for countering attempts of vendor lock-in. The technique is widely deployed in numerous systems today including several major US MVPD's and almost all external to North America. It is also widely used in OTT

and Internet delivery systems and called out in the related standards. Implicit in common encryption is the use of a standardized encryption algorithm (e.g. AES).

W3C Web Crypto provides basic cryptographic operations to support use cases such as user authentication and certificate access.

Note that while these W3C APIs are used in Web browsers, they can also be used outside of a browser in a traditional native application, in a widget or as a Web view exposed by the device platform.

Note that this discussion should be considered informative - the normative references are the latest versions of the referenced W3C & IETF specs.

2. System Description

The system consists of MVPD/OVDs supplying media streams over HTTPS and CE/CPE devices accessing and decrypting those media streams by supplying devices that implement the HTML5, EME, MSE and Web Crypto APIs.

a) Software components

(1) MVPD/OVD Media Requirements

The following describes how MVPD/OVDs supply media streams over HTTPS.

(a) MVPD/OVD provides media via HTTP(S) [HTML5].

(b) MVPD/OVD supplies MIME types with codecs and profiles for all media files. [RFC 2045][RFC6381]

(c) MVPD/OVD media may be made available on any mix of cloud-based URLs and/or home LAN-based URLs. The distribution of media across cloud vs. LAN is flexible.

(d) MVPD/OVD media on cloud-based URLs may be unencrypted or encrypted with a common encryption method. (e.g. ISO Common Encryption). [EME]

(e) MVPD/OVD media on home LAN-based URLs may be unencrypted, encrypted with a common encryption method or sent via a link level encryption method (e.g. DTCP-IP or HDCP).

(f) MVPD/OVD supports at least one key server (for any DRM that supports EME) for each common encryption format supported by that MVPD/OVD. [EME]

(g) MVPD/OVDs can support adaptive bit-rate video access for cloud-based media and optionally for home LAN based media. [MSE]

(2) CE/CPE Platform Requirements

The following describes how CE/CPE devices access and decrypt MVPD/OVD media streams by supplying devices which implement the HTML5, EME, MSE and Web Crypto APIs.

(a) CE/CPE provides HTML5 Media Element APIs for all media access.

(b) CE/CPE describes support for all media MIME types with codecs and profiles via canPlayType() [HTML5][RFC 2045][RFC6381]

(c) CE/CPE plays all supported unencrypted and all link encrypted media (e.g. DTCP-IP or HDCP) via HTML5 video and audio elements

(d) CE/CPE plays all supported common encryption media (e.g. ISO Common Encryption) via EME API.

(e) CE/CPE supports at least one DRM Content Decryption Module (CDM) capable of decrypting each common encryption format supported [EME].

(f) CE/CPE supports MSE API for all adaptive video.

(g) CE/CPE supports Web Crypto for application-based user authentication and for access to any platform certificates.

(3) Overall Requirements

The following describe overall requirements applying to MVPD/OVDs and CE/CPE platforms

(a) Following the practice of the IETF and W3C, the specific CDM/DRM, link protection, media format and common encryption technologies used are not mandated, allowing technology evolution, vendor interoperability, and marketplace competition.

(b) Following the practice of the IETF and W3C, all referenced specs will be considered to refer to the latest spec versions. For example, HTML5 may be replaced with HTML5.1, when published. Similarly, key IETF RFCs are updated over time.

(c) This usage of the HTML5 APIs is non-exclusive for both MVPD/OVDs and CE/CPE, because while HTML5 provides the best environment for portable, write-once, run-everywhere applications, there are still market requirements for non-portable applications that may not use these APIs for security system access. For example, applications on popular mobile platforms are often written in native code. Also, apps are sometimes written to non-portable APIs to access special platform capabilities (e.g. game platforms with gesticulation interfaces).

(d) Following the practice of the W3C, the HTML5, EME, MSE, and Web Crypto specifications were drafted under a royalty free patent license policy. IETF specifications are drafted under a RAND IPR policy, but in practice contributions are generally only accepted under royalty free terms.

(e) The software programs (applications and libraries) which call the HTML5, EME, MSE, and Web Crypto APIs, choose from available content protection technologies, resolutions and formats and also implement some security aspects, such as user authentication and certificate access. There is no restriction on authorship of these programs, which could be written by an MVPD, OVD or CE company.

b) Hardware components (if any)

There are no specific hardware requirements.

Some media may have generic hardware requirements. For example, UHD content may require a hardware root of trust. As another example, 3D video may require a hardware 3D display. But there are no specific hardware requirements, such as a particular CPU architecture, a particular hardware root of trust or a particular chip or chip component of any kind.

c) Operational description (download, startup, update, etc.)

The MVPD/OVD media is accessed over the well-understood HTTP(S) model. The CE/CPE HTML5, EME, MSE & Web Crypto APIs operate under the well-understood HTML runtime.

The software downloadable security system (DSS) runtime operations of discovery and key server communication are defined in the EME Content Decryption Module (CDM) abstraction, which standardizes this behavior across all supported DRMs.

All other DSS operations (downloading the DSS, installing the DSS, updating the DSS, DSS rollback, etc.) are not standardized in the HTML5 model. These operations may be defined by the DSS, the operating system, the user agent and/or the underlying hardware root of trust.

Each CDM or link level protection may be implemented in software or hardware or some combination of the two. The HTML5 and EME APIs are the same.

The CDM or link level protection system itself is downloadable and can be downloaded with an application, downloaded separately or pre-integrated in a hardware or software platform.

The combination of a common API with differing security operations provides for portable, write-once, run-everywhere applications while still preserving a competitive market of DSS systems and a competitive market of hardware roots of trust.

3. Benefits/Costs

a) Royalty Free: HTML5, EME, MSE, Web Crypto and all W3C APIs are available Royalty Free under the W3C Patent Policy [W3CPP] with Royalty-Free licensing commitments from over sixty companies [HTML5LIC]

b) Open source: HTML5, EME, MSE, Web Crypto software implementations are available at no cost from at least three open source libraries - Chromium, Gecko and WebKit - which have been integrated into hundreds of millions of devices.

c) Portable applications: The single HTML5 API, supported across all major CPU architectures, all major DRMs and on all types of devices from smart phones, tablets, PCs, Macs, smart TVs, set-tops and game systems, enable write-once, run everywhere applications.

d) Competitive security systems: A common abstraction for both CA/DRM systems and link protection systems makes for a competitive market for security systems. Additionally, EME enables innovation in both hardware and software implementations that can advance ahead of, or in response to, the growing sophistication of attacks on these security systems. By not mandating a single security system, it avoids creating a single point of attack for hackers.

e) Evolving functionality: By requiring usage of latest specification APIs, the architecture will evolve to meet new requirements rather than being stuck with the technology at the initial definition.

f) Support TV and Internet merging: By basing the proposal on leading Web and Internet protocols, the proposal supports continued merging of TV and Internet media services.

g) Field proven: This proposal is not unduly burdensome, as it has been implemented by all of the commercial browser vendors and is already being used by multiple content distributors, including Netflix, Google YouTube and Apple for premium content.

h) Uniform API: HTML5, EME, MSE and Web Crypto provide a uniform architectural framework and provide uniform JavaScript APIs.

i) Technology- and platform-neutral: The HTML5 architecture is technology- and platform-neutral as it does not mandate specific software or hardware technologies or platforms. Nor does it mandate a particular network technology or architecture.

j) Software-based downloadable security systems: HTML5 and EME MIME and EME are clearly software-based solutions and provide access to downloadable security systems.

k) CE/CPE choice: A device manufacturer can choose one or more link level protection technologies and/or one or more DRM/CA technologies from a competitive market of commercial content protection technologies to implement on their device. These technology choices can be updated or changed after the device is sold and in the market as a device manufacturer chooses to renew the security systems on its devices. A wide variety of CE devices support HTML5 including smart phones, tablets, PCs, Macs, smart TVs, set-tops and game systems.

l) Security providers competition: Content protection providers can compete on the robustness of their implementation, their countermeasures, threat monitoring, etc. Content protection technologies can easily be updated or abandoned based on security breaches. As multiple CA/DRMs are abstracted and supported, no single point of attack is created.

m) Chip manufacturer competition: Hardware chip manufacturers can continue to compete on the quality of their hardware roots of trust

and on their integration with DRM, CA and link level protection technologies and trust models.

n) MVPD/OVD choice: MVPD/OVDs can choose from a competitive content protection market which technologies to support on their network to secure their content. MVPD/OVDs can also add to or replace their content protection systems over time.

o) Minimizes proprietary code: From the EME spec: "The common API supports a simple set of content encryption capabilities, leaving application functions such as authentication and authorization to page authors. This is achieved by requiring content protection system-specific messaging to be mediated by the page rather than assuming out-of-band communication between the encryption system and a license or other server." These security-related functions rely on apps and other means that are CDM/DRM/CA security-system independent.

p) Provides common IP abstraction to MVPD/OVD network security elements: By supporting IETF and W3C APIs for access to security elements for MVPD/OVD streams made available via IP, this proposal avoids the cost and complexity of building to and testing against each of the divergent MVPD/OVD access network security elements.

4. Requirements Analysis

The HTML5 Proposal is evaluated against the requirements outlined in section II.B Downloadable Security System – Common Requirements.

1) *Verifies the navigation device reports having the necessary components for receiving the media provider's service, and it identifies if the device has been tampered with or compromised.*

This verification remains the responsibility of the security system. The related robustness and compliance rules govern the level of security provided by the implementation. CA/DRM providers typically leverage hardware components (e.g. root of trust and trusted execution environment) to perform this function (see section II.C Existing Downloadable Security System Solutions). In the case of link level protection, it is the robustness and compliance rules of the link protection that govern the implementation.

2) *Verifies the integrity of the software components that are downloaded and installed in the navigation device to ensure that those components have not been compromised at download, installation, boot, or runtime. This is typically done by code signature verification.*

A CA/DRM implementation can either be downloaded separately or as a part of the OS. In the case where it is a separate download, the download process (either provided by the OS or a separate application) validates the integrity of

the implementation. In the case where the CA/DRM is a part of the OS, it is the OS download process that performs this function. CA/DRM providers typically make use of proprietary protocols and leverage any hardware support (e.g. root of trust and trusted execution environment) to perform this function (see section II.C Existing Downloadable Security System Solutions). In the case of link level protection, it is the robustness and compliance rules of the link protection that govern this.

3) *Authenticates or supports the authentication of the user of the device as being authorized for receiving the media provider's service. This may be implicit when using a managed device assigned to a user.*

User authentication is the responsibility of the application. The Web Crypto library supports user authentication. In the case of a CA/DRM implementation, it is the responsibility of the security system to securely communicate the device entitlements or usage rights for this user. In the case of link level protection, the content source and destination are trusted based on mutual authentication.

4) *Provides to the navigation device secure and verifiable information on the authorized services available to the device and user.*

In the case of an EME implementation the JavaScript APIs are used to communicate to the application whether the service is available to the device and user. In a CA/DRM implementation the implementation provide APIs specific to that implementation to convey this information (see section II.C Existing Downloadable Security System Solutions). In the case of link level protection, it is the robustness and compliance rules of the link protection that govern the implementation.

5) *Enables descrambling of the authorized services available to the device.*

In the case of a CA/DRM implementation it is the implementation that is responsible for descrambling the authorized services available to the device. CA/DRM providers typically leverage hardware components (e.g. hardware decryption engines and trusted execution environment) to perform this function (see section II.C Existing Downloadable Security System Solutions for the types of scrambling algorithms supported). In the case of link level protection, the encryption on the link is specified by the link protection technology (e.g. DTCP-IP).

6) *Performs a secure download from the network to a client device, for either first time installation of content security software, or a software update.*

See (2) above.

7) *In the network, encrypts content for later consumption, either on a real time or pre-encrypted basis, packetized in accordance with the target delivery system.*

In the case of a CA/DRM implementation content encryption is performed in the network, either on a real time or pre-encrypted basis, packetized in accordance with the target delivery (see section II.C Existing Downloadable Security System Solutions for the types of scrambling algorithms supported). In the case of link level protection within the home network, the encryption/decryption is performed by endpoints and the content is packetized on the link as specified by the link protection technology.

8) *In the network, encrypts software to be downloaded, either on a per client device basis, or based on a parameter or set of parameters that enables a group of devices to be targeted for download as an ensemble.*

See (2) above.

9) *In the network, distributes entitlement information in various forms, using either one-way or two-way protocols, depending on the delivery network type.*

See (3) above and section II.C Existing Downloadable Security System Solutions.

From the EME spec: "The common API supports a simple set of content encryption capabilities, leaving application functions such as authentication and authorization to page authors. This is achieved by requiring content protection system-specific messaging to be mediated by the page rather than assuming out-of-band communication between the encryption system and a license or other server."

10) *The DSS fulfills the commercial and/or regulatory obligations of an MVPD to protect content from content sources/owners.*

In the case of a CA/DRM implementation it is the implementation that fulfills the commercial and/or regulatory obligations of an MVPD. The related robustness and compliance rules govern the level of security provided by the implementation. CA/DRM providers typically leverage hardware components (e.g. root of trust and trusted execution environment) to perform this function (see section II.C Existing Downloadable Security System Solutions). In the case of link level protection, it is the robustness and compliance rules of the link protection that govern the implementation.

5. Additional Specifications

HTML5	W3C HTML5	http://www.w3.org/TR/html5/
EME	W3C Encrypted Media Extensions	http://www.w3.org/TR/encrypted-media/
MSE	W3C Media Source Extensions	http://www.w3.org/TR/media-source/
WEBCRYPTO	W3C Web Cryptography API	http://www.w3.org/TR/WebCryptoAPI/
W3CMEMBERS	W3C Current Members	http://www.w3.org/Consortium/Member/List
RFC2045	IETF RFC 2045	https://tools.ietf.org/html/rfc2045
RFC6381	IETF RFC 6381	http://tools.ietf.org/html/rfc6381
W3CPP	W3C Patent Policy	http://www.w3.org/Consortium/Patent-Policy-20040205/
HTML5LIC	HTML5 Royalty Free License Commitments	http://www.w3.org/2004/01/pp-impl/40318/showCommitments
IETF IPR	IETF IPR Policy	http://tools.ietf.org/html/rfc3979

Applicable Devices

Any DLNA VidiPath certified device including: smart/connected TVs, game consoles, PCs, tablets, and smart phones.

Section VI: W3C HTML5 Web Browser

The World Wide Web Consortium (W3C - http://www.w3.org/) is an open standards body that defines the standards used to implement the Web today. HTML5 represents the latest version of the W3C standards and is being implemented by all commercial web browsers today. Web browsers for mobile devices are also implementing HTML5. Smart TVs and other connected entertainment devices are also implementing HTML5 capabilities.

The HTML5 Media elements, Media Source Extensions (MSE) [57] and Encrypted Media Extensions (EME) [58] are the W3C specifications for processing multi-media, including protected audio/video content. All major web browsers are implementing Media elements, MSE and EME to support both protected and unprotected video content. These specifications are being adopted by video distributors across the Web. For example, Netflix already uses HTML5 with EME to distribute protected content and other OTT distributers and MVPDs are following their lead. HTML EME can also be used in devices that do not have browsers.

HTML5 Media elements are used to present video and/or audio data to the user. HTML5 media resources can have multiple audio, video and data tracks. HTML5 includes standard definitions for special media tracks, including alternative media, captions, descriptive audio, sign language, subtitles, translation and commentary.

The MSE specification [57] defines an API that a web page can use to feed media data to the HTML5 video or audio element. This API enables JavaScript in the page to:

- Handle processing of an adaptive media manifest file.
- Fetch the media segments using the URL from the manifest file
- Append the media segments for playback by the browser's media player.

The MSE API can be used for insertion of other content like advertisements, alternative media or playback of a local media file.

While the MSE API is independent of any particular adaptive delivery protocol, MPEG DASH [40] has been a specific design and implementation focus. MPEG DASH takes advantage of the most recent MPEG technology to seamlessly adapt to changing network conditions, and provide high quality play back with fewer stalls or re-buffering events.

Media Source Extensions [57] enables JavaScript to send byte streams to the various media codecs implemented in HTML5 web browsers. This allows the prefetching and buffering of media streams to be implemented in JavaScript providing greater flexibility and application

control over these media streams. This flexibility allows the application to optimize the playback of media from multiple sources. Figure 29 is the diagram of the MSE architecture from the W3C MSE draft specification.

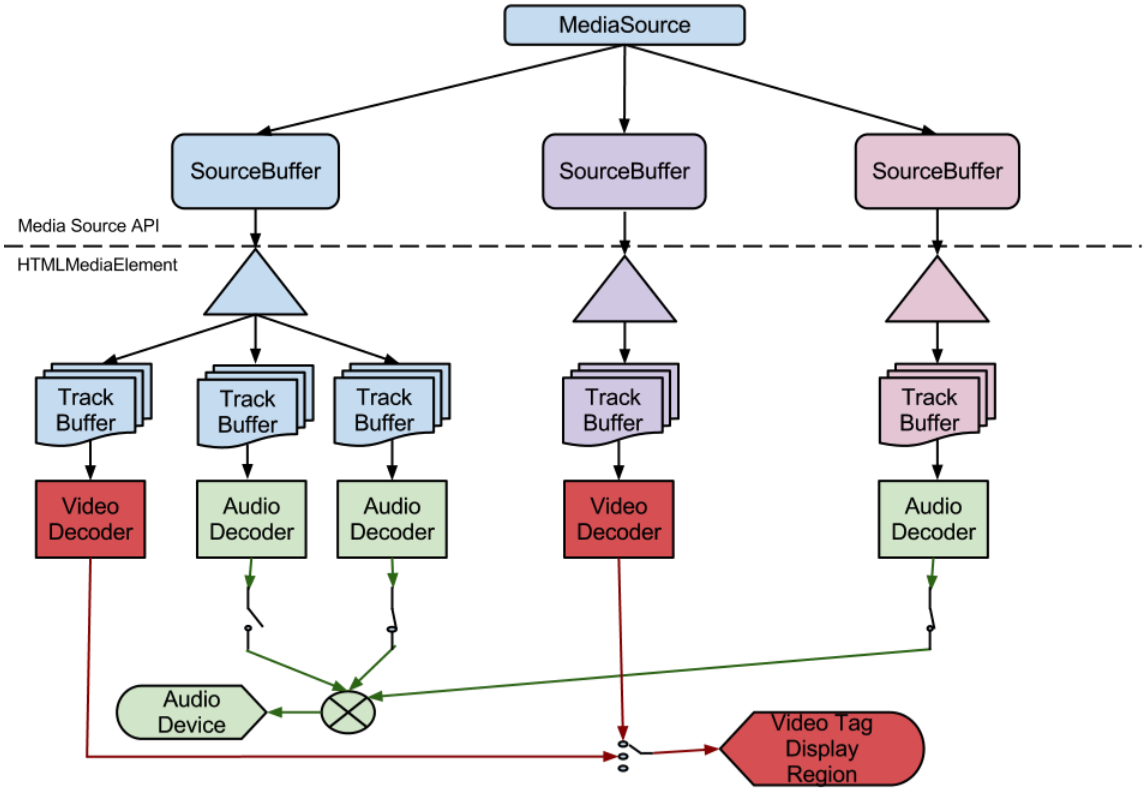

Figure 29- Media Source Extensions Architecture

The EME specification [58] defines an API that a web page can use to playback content, securely protected by any EME-compliant DRM system, using the video or audio element. The API enables the page to:

- Detect attempted playback of protected content.
- Learn what DRMs may be used to playback the content.
- Request the appropriate DRM license needed for content playback.
- Provide DRM licenses to the user agent for content decoding.

A browser may implement any number of DRM-specific content decryption modules (CDM) that handle license processing and content decryption. EME does not specify any particular content encryption or any set of DRMs, nor does it define how a CDM is implemented in the browser.

EME does require support for the Clear Key [61] decryption so that browser EME implementations can be tested or used without a commercial DRM. EMEs is the W3C specification that defines the APIs necessary to control the playback of protected content. Per the EME specification:

"The API supports use cases ranging from simple clear key decryption to high value video (given an appropriate user agent implementation). License/key exchange is controlled by the application, facilitating the development of robust playback applications supporting a range of content decryption and protection technologies.

This specification does not define a content protection or Digital Rights Management system. Rather, it defines a common API that may be used to discover, select and interact with such systems as well as with simpler content encryption systems. Implementation of Digital Rights Management is not required for compliance with this specification: only the Clear Key system is required to be implemented as a common baseline.

The common API supports a simple set of content encryption capabilities, leaving application functions such as authentication and authorization to page authors. This is achieved by requiring content protection system-specific messaging to be mediated by the page rather than assuming out-of-band communication between the encryption system and a license or other server."

Figure 30 shows the high-level architecture of the EME specification. In this example, content is encrypted using Common Encryption Scheme (CENC) and is typically distributed from a Content Distribution Network (CDN).

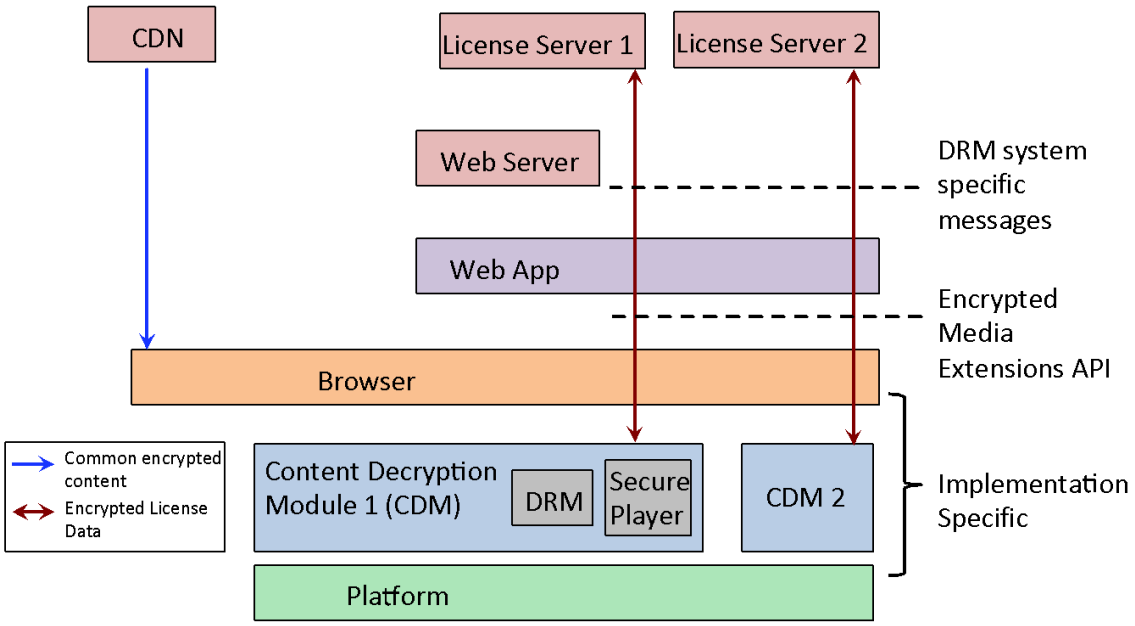

Figure 30- Encrypted Media Extensions Architecture

Error! Reference source not found. is the detailed EME architecture from the EME draft specification and shows the APIs implemented to abstract the DRM implementations.

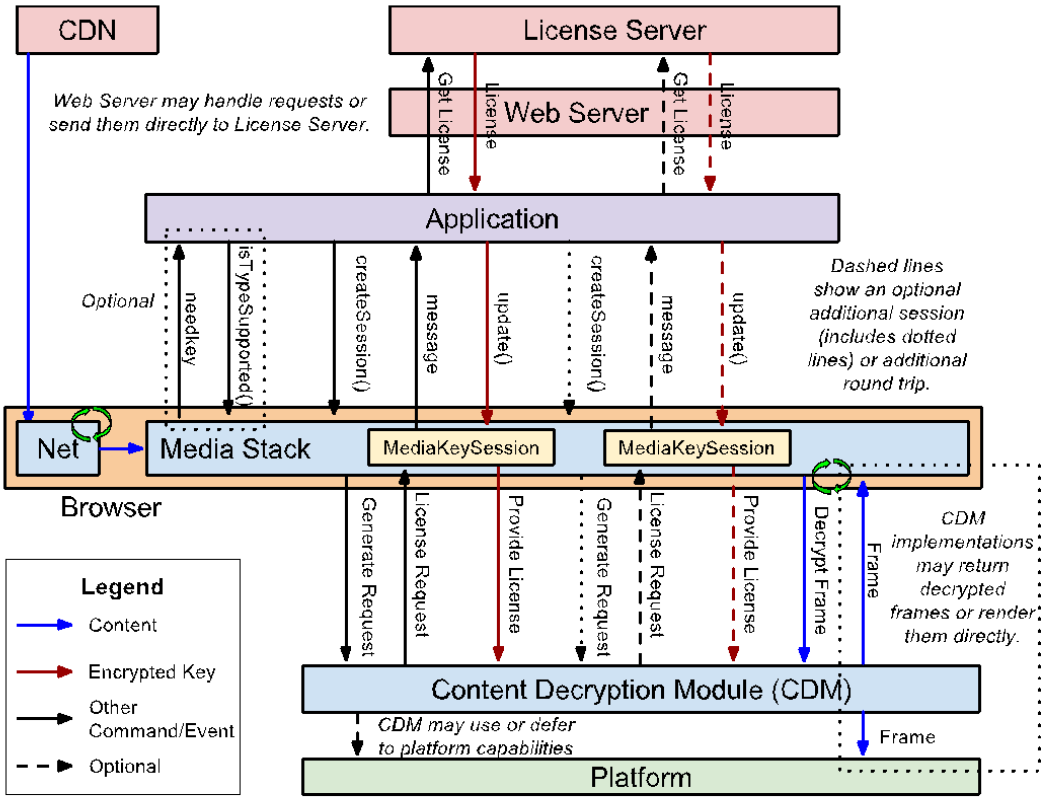

Figure 31 - Detailed EME Architecture with APIs

All of the major browsers have implemented EME, including Google/Widevine, Apple/Fairplay, Microsoft/Playready, and Adobe/Access. Thus, there is competitive downloadable browser/DRM marketplace.

World Wide Web Consortium (W3C) Standards

The W3C Specifications are publicly available at: http://www.w3.org/TR/. The following W3C Specifications are relevant to enabling competitive availability of devices that receive MVPD services:

- HTML5 - A vocabulary and associated APIs for HTML and XHTML, W3C Recommendation, World Wide Web Consortium, http://www.w3.org/TR/html5/ [39]
- W3C WOFF File Format 1.0. http://www.w3.org/TR/WOFF/
- W3C MSE, *Media Source Extensions*. http://www.w3.org/TR/media-source/ [57]
- W3C EME, *Encrypted Media Extensions*. http://www.w3.org/TR/encrypted-media/ [58]

- W3C Crypto, *Web Cryptography API*. http://www.w3.org/TR/WebCryptoAPI/ [61]

Protocols

The protocols used include:

- TCP/IP
- HTTP
- HTTPS
- MPEG DASH [40]

Information

The W3C Specifications are publicly available at: http://www.w3.org/TR/.

Applicable Devices

HTML5 with EME and MSE is applicable to any device that implements these specifications including: smart/connected TVs, game consoles, PCs, tablets, and smart phones. HTML5 can support a browser user interface (e.g. Chrome or Firefox on a PC) or HTML5 can support an application environment that looks just like a native app environment (e.g. Smart TVs from Firefox OS, Tizen or WebOS). Consequently, HTML EME can be used in devices that do not have browsers.

Section VII: RVU™

The RVU protocol is available to consumer electronics (CE) manufacturers via the RVU Protocol Specification. RVU is based on open standards such as UPnP to simplify software integration and enable cost effective solutions that CE manufacturers can leverage to create RVU clients such as TVs.

RVU eases the provision of home networked commercial entertainment content while heightening the user experience. Viewers can access either pre-recorded or live content, premium content such as high definition or ultra-high definition video and multi-channel audio, or personal content such as photos and videos via the media server. RVU supports a novel process-light remote user interface that allows user interactions such as trick play (e.g., pause and rewind) and the running of interactive applications.

In addition to a full featured remote user interface that allows the user of a connect client device to navigate through user screens generated by a compatible RVU server, RVU technology provides Internet Protocol (IP) connectivity, service discovery built from UPnP and DLNA protocols, a remote commanding protocol, and industry standard media formats protected by DTCP-IP content protection.

- Personal computers (both Windows and Mac)
- Tablets
- Smart phones

HTML5 Web Apps

MVPD Web apps make use of the W3C HTML5 standards to reach retail devices. This includes personal computers (both Windows and Mac OS based), as well as other retail devices that implement the W3C HTML5 standards. The interface between the MVPD Web apps and the secure video player are defined by the HTML5 Media elements, Media Source Extensions (MSE) [57] and Encrypted Media Extensions (EME) [58], which are the W3C specifications for processing multi-media, including protected audio/video content, exposed through JavaScript APIs.

As in the case of the device specific apps, the functionalities comprising the MVPD service, including those features and functionalities expressed via a remote user interface, are provided via the application operating on the device. The MVPD service is enhanced and updated by updating the application.

HTML5 Media elements are used to present video and/or audio data to the user. HTML5 media resources can have multiple audio, video and data tracks. HTML5 includes standard definitions for special media tracks, including alternative media, captions, descriptive audio, sign language, subtitles, translation and commentary.

The Media Source Extensions (MSE) specification [57] defines an API that a web page can use to feed media data to the HTML5 video or audio element. This API enables JavaScript in the page to:

- Handle processing of an adaptive media manifest file.
- Fetch the media segments using the URL from the manifest file
- Append the media segments for playback by the platform's media player.

The MSE API can be used for insertion of other content like advertisements, alternative media or playback of a local media file.

The MSE API enables JavaScript to send byte streams to the various media codecs implemented in HTML5 platforms. This allows the prefetching and buffering of media streams to be implemented in JavaScript providing greater flexibility and application control over these media streams. This flexibility allows the application to optimize the playback of media from multiple sources.

Encrypted Media Extensions (EME) [58] is the W3C specification that defines the APIs necessary to control the playback of protected content. The EME specification [58] specifies a JavaScript API that a Web app can use to playback content, securely protected by any EME-compliant DRM system, using the HTML5 Video or Audio element. The API enables the page to:

- Detect attempted playback of protected content.
- Learn what DRMs may be used to playback the content.
- Request the appropriate DRM license needed for content playback.

- Provide DRM licenses to the user agent for content decoding.

A platform supporting EME may implement any number of DRM-specific content decryption modules (CDM) that handle license processing and content decryption. EME does not specify any particular content encryption nor any set of DRMs, nor does it define how a CDM is implemented (including installation, updating or revocation) in the platform. EME does require support for the Clear Key [61] decryption so that platform EME implementations can be tested or used without a commercial DRM.

As in the case of device specific apps, the robustness of the DRM implementations embedded into the HTML5/EME platform varies and will impact the quality of the content that can be displayed on the device subject to content license requirements. Some HTML5/EME implementations allow for multiple or alternative DRMs to be selected by the HTML5 application. Figure 40 shows two examples of the HTML5/EME implementation. In the case of Device 1, the platform provides access to an embedded DRM client (DRM A) integrated into the underlying OS and hardware root of trust. In the case of Device 2, the software DRM client is integrated into the HTML5 software platform and not integrated into the underlying OS and hardware root of trust. The MVPD then operates a DRM server for each DRM used, one for DRM A and one for DRM B. It also shows how through the use of common encryption and DASH transport one set of video files can be decrypted and displayed through different DRMs. The DRM control plane and the secure video content data plane are identified in this diagram. Note that due to content license requirements, since the embedded DRM A is integrated into a hardware root of trust, Device 1 may be able to decrypt and display a higher quality of video than enabled by the software DRM B client in Device 2.

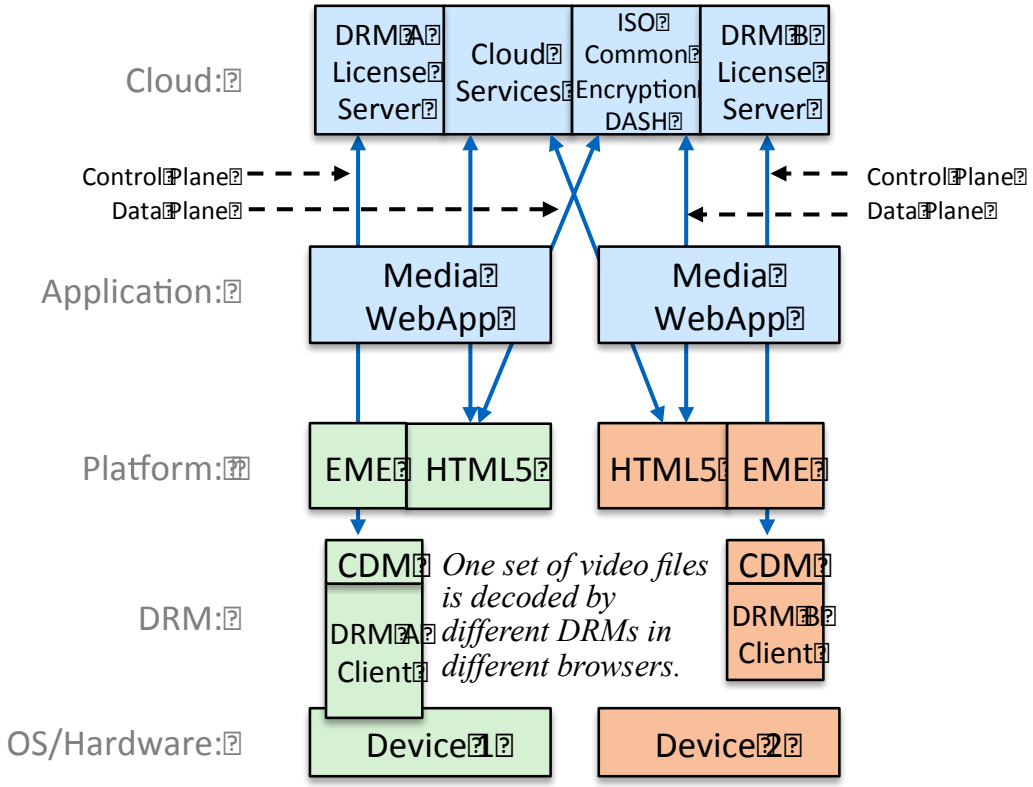

Figure 40 - HTML5/EME Implementation

World Wide Web Consortium (W3C) Specifications

The W3C Specifications are publicly available at: http://www.w3.org/TR/. The following W3C Standards are relevant to enabling competitive availability of devices that receive MVPD services:

- HTML5 - A vocabulary and associated APIs for HTML and XHTML, W3C Recommendation, World Wide Web Consortium, http://www.w3.org/TR/html5/ [39]
- W3C MSE, *Media Source Extensions*. http://www.w3.org/TR/media-source/ [57]
- W3C EME, *Encrypted Media Extensions*. http://www.w3.org/TR/encrypted-media/ [58]
- W3C Crypto, *Web Cryptography API*. http://www.w3.org/TR/WebCryptoAPI/ [61]

Protocols

The protocols used include:

- TCP/IP https://tools.ietf.org/html/rfc793
- HTTP, HTTPS https://tools.ietf.org/html/rfc7230
- MPEG DASH [40]
- MPEG CENC

.

Applicable Devices

HTML5 with EME and MSE is applicable to any device that implements these standards including: smart/connected TVs, set-top boxes, game consoles, PCs, tablets, and smart phones.

DLNA VidiPath™

DLNA VidiPath defines a set of guidelines for accessing protected media services from a device in the home network a Remote User Interface (RUI). VidiPath enables MVPDs and OTTs to deliver their service to DLNA-certified retail devices by using an HTML5 Web app. VidiPath enables video services to be delivered via a home server model and/or via a cloud to ground model. DLNA VidiPath adopted HTML5 for its Remote User Interface (RUI) functionality and thus uses the same APIs described in the HTML5 Web Apps section above, including MSE, EME and WebCrypto. DLNA VidiPath also makes use of DTCP-IP link-layer protection for the transmission of content over the home network. DLNA adds the ability to discover digital media servers (DMS) on the home network and access content on them. As is the case for device specific apps and HTML5, the functionalities comprising the MVPD service, including those expressed via a remote user interface, are provided via the application operating on the device. The MVPD service is enhanced and updated by updating the application.

CableLabs, in partnership with industry participants such as Intel and ARM, has developed open source implementations of VidiPath Server and Client [55]. These implementations are aligned with libraries used by Reference Device Kit (RDK), an integrated software platform initiative for MVPD customer premise equipment (CPE) led by major MVPDs in the U.S. and Europe [56].

The VidiPath specifications enable consumers to consume premium subscription TV content on devices of their choice with a consistent user experience across all devices. Using VidiPath HTML5 RUI, service providers are able to enhance their Web application in the cloud (just like any other Web based company) and evolve their services more rapidly, thus reducing time-to-market for new services and products features. The auto service discovery feature supported by VidiPath facilitates easy installation and setup, which is a benefit to both consumers and service providers.

The Diagnostics feature allows service providers to remotely diagnose and troubleshoot any service related issues.

VidiPath authentication provides assurance to service providers and content providers that only certified VidiPath devices access their services and provides assurance for their user experience on retail devices. VidiPath offers a single, interoperable solution to retail device manufacturers to enable premium subscription TV services from different service providers.

Standards

DLNA Guidelines, http://www.dlna.org/dlna-for-industry/technical-overview/guidelines [60]

Protocols

The protocols used include:

- UPnP

Evaluation of "Application-Based Service with MVPD UI" ("Apps Approach") by Proponents of Application-Based Service

Consumer Experience

The apps approach is based on the successful model developed in the market and widely adopted by consumers. Consumers are embracing an apps-based way of enjoying MVPD services on their own retail devices, without the need for an MVPD's set-top box.

The apps approach enables the delivery of multichannel service that has evolved far beyond simple broadcast video service and is delivered from a wide variety of video providers using a wide variety of technologies. Applications support the modern features of MVPD service, such as interactivity, recommendations from what's trending, on-screen caller ID, voicemail notifications, and pause/resume from last point viewed on different devices in the home.

The apps approach also provides the consumer with automatic service and feature upgrades as service evolves with an app update, as consumers have grown accustomed to on tablets and smartphones. Application and feature updates are occurring multiple times a month, effected with an application update.

Applications help to seamlessly integrate software and hardware for a quality consumer experience. Applications help to seamlessly integrate software and hardware for a quality consumer experience. Apple's iPad considerably raised consumers' expectations of how well hardware and software should work together. With applications, consumers receive the service as advertised and through a familiar interface on multiple platforms—TV, tablet, phone, and other video devices. Consumers can enjoy a common experience on the many devices consumers use to access the service across devices—including the ability to navigate and see recent tuning history regardless of which device was used—the way it works with Netflix.

Consumers are guaranteed to receive service as advertised and as intended by the service provider, including all features. If consumers experience problems, they know where to seek help and who is responsible for responding to customer complaints.

Enabling service providers to offer their own presentation and remote user interface through an app permits MVPDs to fulfill the many consumer protections (like statutory privacy requirements) built into regulated MVPD service. By contrast, there is nothing in a disaggregation approach that prevents a retail device manufacturer from sharing sensitive viewing information with third parties.

Retail devices that host the application may continue to differentiate themselves with features, functions, networks, drives, speed, look, feel and price, and may have their own top level user interface, app store, and menu structure.

Development and Testing

App development work is provided by the service provider for the platform to which the app is directed. MVPDs, like Netflix, Amazon and other "over the top" video distributers, individually code, test, improve, and maintain different versions of their apps for the different supported customer-owned devices and platforms, such as iOS, Android, Mac/OS X, PC/Windows, Xbox, Roku, Kindle, and a variety

of Smart TVs. Every one of the Top 10 MVPDs offers such apps. Some device manufacturers test against some of these applications with software changes but the primary burden is on the app developer.

Apps developed for HTML5 are portable, consistent and "write once run anywhere" for all retail devices that support HTML5.

Apps developed for VidiPath are portable, consistent and "write once run anywhere" for all retail devices that support VidiPath.

This app development work has been undertaken by MVPDs and OTT providers in response to demonstrable consumer demand. It has been successful and built upon rather than displaced.

Service Provider

The service provider may update its service and features by updating the app. The new feature set becomes available through the app. This permits rapid innovation by the service provider. By contrast, fixed protocols require long timeframes for standardization of APIs or protocols for each new feature, which is difficult given the variety and pace of change among video providers, technologies, platforms, services and features. It would take years to develop the hundreds of protocols for use across all MVPDs,[76] and even then the protocols may not anticipate new services, features, or technologies for MVPD distribution. Protocols/APIs would also have to be constantly deprecated as technologies evolve. The apps approach avoids the constraints on service provider innovation that would be a major burden and cost to the MVPD and to consumers.

A key benefit of the apps approach is its support of the economic fundamentals that have fueled the growth and development of today's multichannel ecosystem. Apps give MVPDs the tools to serve retail devices and assure compliance with their copyright and retransmission consent agreements that define and segment rights. This is essential to MVPDs' ability to obtain content from third parties who rely upon a trusted distribution system. Apps give MVPDs the tools to support the advertising that funds the dual-revenue MVPD business, and to provide an interactive and accountable ad platform that can continue to compete for those ad revenues.

Apps give MVPDs the tools to keep enhancing service continuously without awaiting industry consensus, standards, or rule changes; to create value and consumer recognition of that growing value from their (branded) service provider; and to help retain them as customers. Apps give MVPDs the tools to innovate with new technologies, to shape and reshape their offerings to meet changing consumer demands. Now that there are so many MVPD and OTT providers of video programming, the ongoing ability to enhance service are critical to an MVPD's branding and competitiveness. It would be a major burden and cost to MVPDs and a major loss to consumers if MVPDs were restricted from enhancing their services and competing. Apps protect against those burdens.

Enabling service providers to offer their own presentation and remote user interface through an app permits MVPDs to fulfill the many consumer protections (like statutory privacy requirements), "must carry" rules (like channel position and channel neighborhood), accessibility, and other requirements built into regulated MVPD service. For example, cable and satellite operators are required to protect the

[76] Estimates from among the top 10 MVPDs indicate that the number of protocols or APIs in each of their systems to deliver the MVPD service range from hundreds to as many as ten thousand.

privacy of the video records and other personally identifiable information of their video subscribers, particularly against government intrusion. CE manufacturers are not. Cable operators are required to restrict the display of commercial web links in association with programming directed to children. A CE device can overlay prohibited links. Cable operators are required to provide parents the ability to block channels they consider offensive regardless of rating. CE manufacturers are not. Applications allow cable operators to send emergency alerts, including force tuning the device. Applications allow cable to meet channel positioning commitments to local broadcast stations, and to precede changes in channel position with advance notice. The use of an application based approach permits MVPDs to meet all of these requirements built into regulated MVPD service.

Enabling service providers to offer their own presentation and remote user interface through an app permits MVPDs to offer their services consistent with the content licenses and retransmission consent requirements under which they acquire distribution rights. For example, apps may assure that programming is kept in the right neighborhood, such as a news channel placed in a news "neighborhood" or a premium service kept adjacent to its multiplex channels. Apps may assure that search returns do not place a programmer next to an X-rated offering. If service providers are unable to effectuate the very arrangements under which they are licensed to distribute secure high value programming and services, why should they bother to encrypt the service, negotiate distribution agreements, develop new business models and architect their systems and chains of trust in the first place? Applications permit the delivery of MVPD services in ways that respect all of these arrangements.

Enabling service providers to offer their own presentation and remote user interface through an app also respects service providers' First Amendment rights to operate as a publisher and the copyright and intellectual property rights under which video services are licensed and distributed. Apps assure that channels and services are presented as intended and marketed and that the presentation carries the content, features, brand, look and feel of the MVPD.

Enabling service providers to offer their own presentation and remote user interface through an app allows the MVPDs to offer better and consistent support and diagnostics to consumers.

A disaggregation approach would require MVPDs to create new technologies that would separate their program content from the services they offer so that third parties may reassemble that programming into their own, unlicensed services. The device maker would have no obligation to present the MVPD programming with all of its service features intact. The service provider may be unable to provide consumers with interactive and other enhancements to programming, as well as the future innovations that do not fit within today's conception for protocols link-protected or gateway device outputs offering its service without invoking its user interface, and shut it down. Like Netflix, YouTube now presents its service through an app and its own user interface.

The apps approach does not permit MVPDs' services to be reassembled into a different look and feel or product provided by a device manufacturer, unless there is mutual negotiated agreement. MVPD retail distributors are not licensed to be wholesale content suppliers to CE device manufacturers to disassemble the service and create a new service from its components. Content owners license terms govern the geographic area for delivery, restrictions on copying or redistribution, specifications for how content is displayed, requirements that particular advertising, branding, polling or other interactive material be associated with their content, and/or restrict certain types of ads or overlays from being

shown with their content. Some content providers require that their on-demand programs be grouped together through a branded entry point (i.e., all shows accessed from a program network-branded folder). Over-the-top providers such as Netflix use their own application-based UIs and negotiated business-to-business agreements to enforce these terms on retail devices. MVPDs would be significantly disadvantaged if they could not enforce applicable license terms when their services are delivered on retail devices. Without application-level enforcement or negotiated agreements, third party devices could rearrange channel or program placement, insert different advertising into or on top of programs, ignore blackout or other geographic restrictions, or use search functionalities to promote illegitimate content sources over legitimate ones, such that a user about to purchase an on-demand movie might be directed to a lower-cost pirate option instead. The retail device might also use search functionalities to promote, or otherwise skew how consumers identify and choose which content to watch (such as manufacturers charging content sources to improve their search rankings).

Applications can deliver service in several ways to IP-connected devices, including broadband modems and VidiPath servers. Applications do not compel the redesign of networks to support simulcrypt (a methodology that enables dual or multiple CAS systems on an MVPD network).

Content Providers

Commercial video content providers segment the market based on specific distribution paths, security, devices, audiences, and advertising opportunities. Content licenses define channel position, tier placement, acceptable advertising, scope of distribution permitted, security requirements and consistent presentation of branded content. Content distribution rights have grown far beyond the simple states defined by the CCI bits sent to CableCARDs. Content providers may specify which devices are trusted and permitted to receive content. Some content is not available to devices unless they support a HW root of trust. Content providers may limit distribution rights to the home, or may place limitations on out of home uses. Content may be permitted only for defined periods of time, and then erased. Some MVPD distribution networks distribute all content to set-top boxes, and then rely on the set-top box to limit use to only permitted geographic areas. License conditions on the devices that receive programming are required to assure that security and a chain of trust will limit the distribution and use of the content to consumers and devices that are entitled to receive the programming. Applications permit MVPDs to enforce these complex and variable arrangements. The intellectual property rights underlying copyright licenses provide the incentives for content providers to produce great content, for inventors to create new methods of distribution and new applications, and for licensed distributors to compete as differentiated retailers, all to the benefit of consumers. Intellectual property rights support the rich video and distribution environment that consumers enjoy, and need to be respected. Applications permit MVPDs to operate within these intellectual property rights.

MVPD retail distributors are not licensed to be wholesale content suppliers to CE device manufacturers who in turn want to present multichannel video service as if it were their own, without responsibility to programmers or to the MVPD to deliver the content as required by contract. A CE manufacturer, who likely will have no contractual arrangement with programmers, should not have the ability to present multichannel video service as if it were its own and without responsibility to programmers and the MVPD to deliver the content as contracted for by the MVPD.

Program networks and other content providers are entering into direct distribution contracts with CE device manufacturers (e.g., Apple and Sony), licensing new video distributors (e.g., Netflix, Hulu and Amazon), licensing non-traditional online packages (e.g., Sling TV), and offering their own apps directly

to retail devices (e.g. HBO Now). This provides the opportunity for device manufacturers who wish to create their own branded service to receive video service directly from content providers on an appropriately licensed basis.

Device Manufacturer

Applications permit MVPDs to bring more devices into the distribution system. For example, an application may deliver standard definition content to devices that lack a hardware root of trust, rather than denying all content. The apps approach has radically expanded the number of video devices on which consumers can enjoy their MVPD services, far more quickly than any regulatory approach.

With an apps approach, the retail device can have its own distinctive top-level interface, app store, and menu structure, and can also differentiate itself with features, functions, look and feel, networks, drives, speed and price. Regardless of MVPD and other apps presented, Android & iOS compete vigorously in user interface; Nintendo, PlayStation, and XBOX have competitive user interfaces; LG, Panasonic, Samsung, Sony, and Vizio compete in user interface. All allow MVPD apps to present MVPD service as offered and branded by the MVPD. The different video apps all appear as selectable apps that, once clicked, present the retail experience of that video provider in the manner selected by that provider. Apps reduce the burden on CE to map to multiple network technologies and CAS trust infrastructures. The CE manufacturer can expose distinctive resources of the device to app developers, such as multi-touch and speech recognition. The CE manufacturer can also continue to innovate in its devices without the constraints of fixed protocols. For HTML5-based models, all the CE manufacturer has to support is a common HTML5 browser or interface.

Retail devices are clearly succeeding under this apps model. As noted above, Roku has sold over 5 million units, relying entirely on apps (including a cable-operator supplied guide), outselling TiVo (with its “third party” TiVo guide) ten-to-one. No evidence has been presented to the DSTAC to indicate that retail devices needs to interfere with the retail relationship between an MVPD and its customers to distinguish themselves.

Consumers should be able to buy devices with different capabilities, but the devices need to meet content provider requirements, enable the MVPD to present services as intended and advertised, and enable the MVPD to continue to innovate and compete. See Report of WG1, MVPD Requirements and Content Providers Requirements [76]. The [Disaggregated Protocols System model proposed by Brad Love] would not meet these fundamental requirements. There is no need to dumb down MVPD service or strip out features in order to serve a variety of retail devices. For example, MVPDs and content providers already support the highly successful smart phone and tablet market by using a variety of apps tailored to their iOS or Android platforms. When consumers chose a smart phone, they understand that their services are delivered through applications created for that platform, not through a uniform regulatory protocol. Consumers may also chose a feature phone, but they understand that they may not receive MVPD services on those devices, because feature phones are not designed with the resources and platform necessary to render the services that MVPDs offer. No video app developer is compelled to deprecate its service to appear on a feature phone. Likewise, there should be no requirement that modern MVPD service be dumbed down for reception on a supposedly smart video device, when applications can present the MVPD service as offered.

Innovation

The CableCARD model adopted more than a decade ago was designed only for reception of one-way linear cable channels from digital cable systems, and required retail CableCARD devices to use their own guides. This approach reflected basic technical limitations at the time – a one-way device could not support interactive services or the cable program guide, and suitable remote user interface technology did not exist. The protocols in use for CableCARD were designed only for non-interactive linear channels on cable systems. The resulting devices met with very little consumer acceptance.

Much has changed in the past decade. Multichannel service is no longer a simple broadcast video service, but a complex interaction of licensed content, network, security, content protection, hardware, software, licensed metadata, diagnostics, application data synchronized with content, UI, advertising, ad reporting, audit paths, etc. The technology varies across platforms and changes continuously without awaiting industry consensus, standards, or rule changes. Apps allows delivery of this service to a wide variety of CE devices and platforms, none of which are built to a common standard. Reducing MVPD service to unimproved broadcast channels sacrifices decades of improvement and frustrates the continued innovation among competing MVPDs that keeps driving more innovation.

Like MVPD services, today's market has also changed considerably from the environment in which CableCARD was created. When Section 629 of the Communications Act was enacted in 1996, almost everyone had to lease a specific, proprietary set-top box from the cable company to receive digitally-delivered multichannel programming. Today, cable operators' share of MVPD customers has eroded over two decades from 98% to 53%, and DBS and telephone companies are the second, third, fifth and sixth largest MVPDs. Program networks and other content providers are entering into contracts with CE device manufacturers (e.g., Apple and Sony) and other new video distributors (e.g., Netflix, Hulu and Amazon), licensing non-traditional online packages (e.g., Sling TV), and offering their own apps directly to retail devices (e.g. HBO Now).[77] Cable and other MVPDs provide customers with multichannel services on millions of tablets, smartphones, gaming consoles, PCs, smart TVs and other IP-enabled devices that also access online video. None of these devices use CableCARDs, relies on FCC technology mandates or follow a uniform technology. The FCC need not "create" an IP successor to CableCARD; the retail marketplace *today* has created unprecedented and growing choices for multichannel content and online content, eliminating the need to pursue a regulatory route.

Consumer demand varies and evolves, and competitors have the right to innovate with new technologies, to add value-added services, to shape and reshape their offerings to meet changing consumer demands. Diversity and an apps approach enables MVPDs to enhance their networks over time to increase network capabilities, such as increased capacity, device addressability, security, reliability, energy efficiency, quality of service, and operational efficiency. Application and feature updates are occurring multiple times a month, effected with an application update. The changes do not await agreement on a new protocol or standard. Applications allow the MVPD to advertise and promote these new features through their applications. Diversity and an apps approach also enables MVPDs to retire obsolete networking technologies as necessary to achieve these enhancements.

[77] The amended proposal inexplicably describes DOCSIS cable modems as "outdated technology." DOCSIS and DOCSIS modems are the foundation of the infrastructure that has enabled the distribution of online video and the modern broadband economy.

Competition

The apps approach has been developed in the marketplace through competitive responses to consumer behavior and preferences. The app model builds upon existing standards and solutions developed to deliver rapidly changing services to varied and rapidly changing consumer electronics devices and platforms. It has been widely and successfully adopted by consumer electronics manufacturers, MVPDs and OTT video service providers such as Netflix and Amazon. The apps approach leverages technological advancement and the development work in Internet (W3C) HTML5, DLNA, iOS, and Android. It enables the delivery of multichannel service that has evolved far beyond simple broadcast video service and is delivered from a wide variety of video providers using a wide variety technologies to a wide variety of consumer devices.

The apps approach preserves innovation and competition by MVPD and OTT video providers. Apps permit service providers to innovate with new technologies, to add value-added services, and to shape and reshape their offerings to meet changing consumer demands with a code update. It does not require long timeframes for invention and standardization of APIs, protocols, or modules for each new feature.

The apps approach promotes competition in the manner intended by Section 629. Video distributors operate as differentiated retailers who compile bundles of programming, guides, navigation features, applications and other inputs into distinctive, branded offerings. Video providers compete with each other by adding more features and creating value and continued consumer recognition of that growing value from their (branded) service provider. Competition among these retail distributors has fueled and funded competition, innovation, network upgrades, broadband deployment, and consumer choice, and is helping to drive expanding consumer access to MVPD services on smartphones, tablets, and other retail devices and platforms. DISH launched its commercial DVR in 1999; DirecTV and cable operators soon followed. Subsequent innovations by one MVPD lead others to match or better their offerings: multiple tuners; high definition tuners; remote scheduling of DVRs; multi-room DVRs; video-on-demand libraries; StartOver; interactive program guides; t-commerce; voting, polling and other interactive and cross-platform services like Caller ID on TV. Each innovation by one provider spurs competitive responses by others in the market.

This continuous change reflects innovation without permission, and without awaiting industry consensus or standards. New MVPDs developed new networks and services that do not conform to a standard. Verizon devoted an entire fiber wavelength to its linear video offering and transitioned to all-digital. AT&T launched its all-digital U-verse service with all channels switched to maximize its bandwidth for HD and other services. Cable operators responded with switched digital video (SDV) and DTAs to repurpose analog spectrum and add more channels, more High Definition, faster broadband, and more innovative services. As MVPDs innovate and compete, consumers are the ultimate winners. Regulation, fixed protocols, and technology mandates constrain this competition. Section 629 is directed to equipment used to access services offered by MVPDs over multichannel systems, not to promote services provided by third parties and created from disaggregated components. Reducing competition among MVPDs would be a major burden and cost to MVPDs and to consumers.

MVPDs are not seeking to prevent competition from CE manufacturers. They are supporting many more retail devices than they are their own set-top boxes, and continue to expand service to more devices. The Top 10 MVPDs have all used applications to enable an ever-expanding set of customer-owned devices to receive their services. Unlike the Bell System that sought to prevent competition to its wholly-

owned Western Electric equipment division, cable operators, Verizon, AT&T and DirecTV do not own any of their set-top box vendors. They are supplied by a growing number of consumer electronics manufacturers (including TiVo). Cable operators now constitute TiVo's fastest growing market, and comprise approximately 80% of TiVo's customers. An applications-based approach promotes competition by CE manufacturers.

An apps approach is also consistent with the approach used by OTT video providers. Singling out only MVPDs with a different mandate will create the same competitive disparities which undermined the cable-centric CableCARD regime, and would create a competitive burden on MVPDs contrary to the technology- and platform-neutrality required by STELAR. The apps approach also permits device manufacturers and platforms to continue to innovate and compete with one another. The retail device may present (and continuously improve) its own interface, environment and user experience. The device presents a selection of available applications from multiple MVPDs and OTT video providers that can operate as retail stores presenting their own brands and experiences. This apps approach preserves the "chain of trust" from the content supplier to the distributor to the consumer, respects the license restrictions on the content, and preserves the subscription and advertising ecosystem which funds these services and the networks that deliver them.