DSTAC SUMMARY REPORT

FINAL: 8/28/2015

Introduction

The STELA Reauthorization (STELAR) Act of 2014 directed the FCC Chairman to establish a working group of technical experts that represent the viewpoints of a wide range of stakeholders "to identify, report, and recommend performance objectives, technical capabilities, and technical standards of a not unduly burdensome, uniform, and technology- and platform-neutral software-based downloadable security system designed to promote the competitive availability of navigation devices in furtherance of Section 629 of the Communications Act."

The Commission in turn chartered the Downloadable Security Technology Advisory Committee (DSTAC) for this assignment.

The DSTAC undertook extensive surveys and studies (including 50 technical presentations from 33 industry experts) of various security systems, of the trust infrastructure used for the secure delivery of commercial content and multichannel services, the variation in current video providers' distribution technologies and platforms, and the capabilities of various original equipment manufacturers and retail devices used with video services[1].

Scope

One of the points of contention within the advisory committee is whether examination of non-security related issues is beyond the scope of the congressional mandate. STELAR gave the committee a very specific mission as stated in the Introduction. STELAR does not direct the committee to recommend just any performance objectives, technical capabilities, or technical standards, but only those related to designing a downloadable security system, and only to the extent that they are not unduly burdensome. Thus some committee members believe the analysis of Working Group 4 on non-security issues exceeds the scope of issues Congress intended the advisory committee to consider.

Additionally, the definition of what is meant by "MVPD service" (multichannel video programming distributor) is a point of disagreement in the group. Some members of the DSTAC consider MVPD service to include all the various functionalities and features that the MVPD provides to its customers, including the interactive features and the User Interface which they use in their retail offerings and consider protected by copyright, licensing, and other requirements determining how their service is distributed and presented; retaining these elements is also part of respecting the contractual and copyright terms between content providers and distributors for the commercial distribution of programming.

Other members consider "MVPD Service" to be primarily video transport, and consider the inclusion of the MVPD's User Interface and other features to prevent retail devices from innovating and differentiating their products, which they believe is essential for success in the

[1] In addition, material from interested parties was captured in FCC MB Docket No. 15-64, and in demonstrations of service offerings and in public comments made during advisory committee meetings.

marketplace. They also point out the current cable specific CableCARD system allows consumer electronics (CE) manufacturers to build such products today and are in use by consumers.

FCC staff instructed DSTAC to make recommendations concerning both approaches. Both approaches were pursued as options and have been documented in the Working Group Reports.

Organization of Working Groups

The DSTAC's work was conducted and is presented primarily within four Working Group Reports. The Working Group 1 Report presents the commercial requirements of content owners, multichannel video programming distributors (MVPDs), consumer electronics companies, system equipment manufacturers, and consumers. The Working Group 2 Report presents information on current video providers' distribution architectures, technologies and platforms.

The Working Group 3 Report covers two approaches for addressing the security elements of a downloadable security system, including performance objectives, technical capabilities, and industry standards. The Working Group 4 Report presents two proposals for handling non-security elements, as well as critiques of each approach by members of DSTAC.

The four reports produced by the Working Groups, in addition to this Summary document, comprise the whole of the DSTAC congressionally mandated technical report that will be submitted to the Commission on or before September 4, 2015.

Points of Agreement

Although DSTAC is not reporting a consensus recommendation, there were major points of agreement:

- Proposals acknowledge there is a wide diversity in delivery networks, conditional access systems, bi-directional communication paths, and other technology choices across MVPDs (and even within MVPDs of a similar type). It should not be necessary to disturb the potentially multiple present and future CA/DRM[2] system choices made by cable, DBS and IPTV systems, which effectively leaves in place several proprietary systems for delivering digital video programming and services across MVPDs.
- None of the proposals recommend a solution based on common reliance[3].
- Proposals acknowledge that it is unreasonable to expect that retail devices connect directly to all of the various MVPDs' access networks; rather they should connect via an IP (Internet Protocol) connection with specified APIs[4]/protocols, via the MVPD's cloud and/or from within the home.

---

[2] Conditional Access / Digital Rights Management

[3] Common reliance is the concept that operator supplied equipment use the same security solution as retail devices to receive MVPD services.

[4] Application Program Interface; a set of routines, protocols, and tools for building software applications.

- Proposals acknowledge that is unreasonable to expect that MVPDs will modify their access networks to converge on a single common security solution
- Proposals acknowledge that the downloaded security components need to remain in the control of the MVPD.
- It would not be a step forward or economically viable to require an environment in which a retail manufacturer would have to equip a device with RF tuners for cable and satellite, [and] varied semiconductor platforms, to support the dozen-plus proprietary CAS technologies that are currently in use.
- It is not reasonable to expect that all MVPDs will re-architect their networks in order to converge on a common solution.

Security

WG3 "HTML5 Security APIs" Proposal

The WG3 (Working Group 3) HTML5 Security APIs proposal recommends that MVPD/OVDs (online video distributor[5]) and CE/CPE (customer premise equipment) companies adopt the security APIs in HTML5 as a non-exclusive security system interface between MVPD/OVD services and consumer electronic devices. According to its proponents, this proposal has the following characteristics:

HTML5 is the new standard defined in 2014 by the World Wide Web Consortium (W3C) as a common and open approach to deliver IP streaming media based on Internet protocols. HTML5 is a full application foundation, supporting both security elements and non-security elements. HTML5 and its Encrypted Media Extensions (EME), Media Source Extensions (MSE) and Web Cryptography (WebCrypto) extensions are being deployed across the Web today by multiple vendors on hundreds of millions of devices, and are widely supported by all major browsers.

The EME extension defines standard APIs (software programming interfaces) that permit HTML5 to support media under common encryption[6], even while protected by a variety of DRMs. EME operates as a bridge that permits competing DRM security systems to operate on a variety of platforms, including platforms that offer hardware roots of trust[7] and platforms that do not. EME enables device manufacturers and service providers to choose from a competitive market of commercial content protection technologies and enables security systems to advance ahead of, or in response to, the growing sophistication of attacks. By not mandating a single security system, it avoids creating a single point of attack for hackers.

---

[5] In the Working Group reports, OVD is sometimes referred to as OTT.

[6] "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." Source: Working Group 3 Report.

[7] "Roots of trust are highly reliable hardware, firmware, and software components that perform specific, critical security functions. Because roots of trust are inherently trusted, they must be secure by design. As such, many roots of trust are implemented in hardware so that malware cannot tamper with the functions they provide." Source: Working Group 3 Report.

Almost all content protection companies surveyed and discussed in WG3 now support or plan to support EME. These W3C APIs are used in Web browsers but can also be used outside of a browser on other device platforms. This approach makes for a competitive market for security systems, and is technology- and platform-neutral. It is royalty free and open source.

WG3 "Virtual Headend System" Proposal

The WG3 Virtual Headend System proposal recommends that network security and conditional access are performed in the cloud, and the security between the cloud and retail navigation devices be a well-defined, widely used link protection mechanism such as DTCP-IP. According to its proponents, this proposal has the following characteristics:

An MVPD may choose a system architecture for a Virtual Headend System that includes a device located at a consumer's home, which provides a "local cloud" which has security system components downloaded to it as necessary, or the entire solution may be in their network "cloud" and offered as IP services directly to devices in the home. Because the interface to the home network (and retail devices) is standardized across MVPDs at the link protection, this enables nationally portable retail navigation devices.

Current efforts from MVPDs are cited as demonstrating that operators are working towards Virtual Headend System technology that defines a new set of interfaces to legacy network systems under a common set of IP network protocols, served from devices in the home or from the MVPD's cloud that can serve a variety of navigation devices.

Proponents have indicated that an existing link protection mechanism such as DTCP-IP would need to be modified to protect certain kinds of content (such as 4K) and for cloud-to-ground delivery.

Non-security

WG4 "Application-Based Service with Operator Provided User-Interface" Proposal

The Working Group 4 (WG4) "Application-Based" proposal is based on the downloadable apps that MVPDs and OVD providers use today to provide video and other services on CE devices such as PCs/Macs, iOS & Android tablets and smartphones, game stations, Roku, and Smart TVs. Apps are widely adopted, and MVPDs are beginning to extend this apps approach beyond large platforms by using new W3C HTML5 standards to reach more retail devices. According to its proponents, this proposal has the following characteristics:

In this System, the retail device manufacturer can choose one or more methods to enable the MVPD's services through a downloaded MVPD issued app and remote user interface.

- Device Specific Apps (e.g. iOS, Android, Samsung, LG, Xbox, PlayStation, Roku).
- HTML5 Web Apps, using W3C HTML5 standards to reach retail devices that include an HTML5 browser or components with multiple DRM support.
- DLNA VidiPath, as developed by the Digital Living Network Alliance (DLNA) and major CE manufacturers, chip manufacturers, and MVPDs. DLNA-certified retail devices on the home network receive an HTML5 Web app enabling video services to be delivered via a home server and/or via the cloud/network.

- RVU, as developed by the RVU Alliance, a technology standards alliance of service providers, consumer electronics manufacturers and technology providers. The protocol enables retail devices on the home network to receive full-featured service while leaving most of the “hard work” to the in-home “server”.
- DISH Virtual Joey enables navigation of DISH’s broadcast system and Hopper DVR recordings using HTML5.
- Sling Media Technology Clients enables retail devices to receive and navigate service.

All six app approaches enable MVPD supported retail devices to receive multiple MVPD and OVD video services with the CE user interface controlling the device, and the MVPD/OVD video provider’s user interface controlling the service. The app model allows the applications to connect to the many different parts of each network involved in delivering service and still take advantage of each networks’ efficiencies, which vary based on architectures optimized for their different physical natures (RF over coax, twisted pair copper, light signals over fiber, wireless RF). This system hides the diversity and complexity of service providers’ access network technologies and customer-owned IP devices and accommodates rapid change and innovation by both service providers and consumer electronics manufacturers.

The apps deliver the MVPD service that includes modern features such as interactivity, on-screen caller ID, the ability to navigate, see recent tuning history and pause/resume on different devices in the home, regardless of which device was used. Consumers receive service as advertised and as intended by the service provider, including a user interface designed for interacting with the MVPD’s experience.

Consumers receive automatic service and feature upgrades from the MVPD as service evolves via app updates, without awaiting industry consensus, standards, or rule changes.

Apps permit MVPDs to offer their services consistent with the copyright law, content licenses, and requirements under which they acquire distribution rights, such as terms governing the geographic area for delivery, provisions related to 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 restricting certain types of ads or overlays from being shown with content. Apps also give MVPDs the tools to support the advertising that funds the dual-revenue MVPD business.

Apps support all regulatory requirements, including delivery of the Emergency Alert System (EAS), privacy requirements, and restrictions on the display of commercial web links in association with programming directed to children.

WG4 “Competitive Navigation” System

The WG4 “Competitive Navigation” proposal is based on proposed protocols and APIs derived from CableCARD specifications, and some based on cable TV broadcast TV or Internet APIs and protocols. According to its proponents, this proposal has the following characteristics:

In this System, MVPDs would provide a new set of interfaces to their service to allow the user interface (UI) on a retail device to differentiate itself from the UI provided by the MVPD and enable new innovation.

Three new main interfaces would be created:

- a Service Discovery Interface, providing information about available services and messaging from the MVPD
- an Entitlement Information Interface, providing information on the rights associated with the services
- a Content Delivery Interface, delivering Live, Linear, VOD, and network DVR content streams, the content protection mechanism, and the secure transfer of metadata such as entitlement and copy control information

This system would terminate the MVPD's content protection system and protect it using a single common format like DTCP-IP or similar link protection. A Digital Rights Management system (DRM), such as PlayReady, or an enhanced link protection system such as DTCP+, would be suitable for Cloud based delivery.

Additional service features could be supported by widgets[8] to be developed by all MVPDs and delivered through an enhanced Man Machine Interface (MMI). These could support unique consumer interactions, communication with MVPD network "back office" components, billing, and certain service features. Hyperlinks inside an expanded MMI widget could support targets on the greater Internet to communicate directly with an MVPD web service. Display of widgets on the device must be optional, based on user input, regulatory requirements (e.g., EAS would not be optional), and user actions. Widget requirements would need analysis to determine the level of HTML that the MMI should support.

Under this system, obligations of devices should be established by the Commission, rather than by the terms of MVPDs' regulatory and contractual obligations.

This system would require standardization from a number of different standards and the development and implementation of some new protocols and standards.

Relationship of System Proposals

DSTAC considered how the various proposals might work or not work with each other. The WG3 HTML5 Security APIs proposal can support the WG4 "Application-Based" proposal, and the WG3 "Virtual Headend" Proposal can work with the WG4 "Competitive Navigation" proposal. The WG3 HTML5 Security APIs proposal also supports the security elements mentioned in the WG4 "Competitive Navigation" proposal, but there was insufficient time and insufficient detail about other combinations to assess the likely amount of interoperability in the time allotted to the committee.

[8] Reference: http://www.w3.org/TR/widgets-apis/

REPORT OF WORKING GROUP 1 TO DSTAC

"WG1 REPORT #1"

April 21, 2015

Introduction

Working Group 1 (WG1) was formed out of the larger DSTAC to address the topic of commercial requirements. This is in furtherance of the overall mission, to "identify, report, and recommend performance objectives, technical capabilities, and technical standards of a not unduly burdensome, uniform, and technology- and platform-neutral software-based downloadable security system designed to promote the competitive availability of navigation devices in furtherance of section 629 of the Communications Act of 1934."

This report serves to represent a more formal summary of the activities of WG1 and also captures additional dialog and a few conclusions that have been reached by the group since the group issued its initial feedback in late March.

The first report from WG1 ("Talking points for WG1 Report v09") is included as Appendix 1, and thus this second report incorporates all read-outs from the team thus far.

To refresh, the group was chartered to identify the commercial requirements of content owners, multichannel video programming distributors (MVPDs), consumer electronics companies, system equipment manufacturers, and consumers. The group was to consider risks and threats, including, but not limited to: content piracy, brand protection, consumer privacy, device cloning, and device spoofing. The group split requirements into five primary areas: MVPDs; CE/device manufacturers; consumer; content providers; and security.

Since the initial "Talking points" summary was issued, the group has compiled a list of more specific requirements consisting of nearly 200 different line items. The list serves as a tool for working group participants to express their proposed requirements based on their areas of expertise and study. This list is based on current requirements and anticipated (future) requirements. However, this list is by no means comprehensive. That list is attached as Appendix 2.

The list continues to be subject to clarifications and additions. After the initial list was compiled, the group worked to identify major areas of alignment and non-alignment (conflicting language). Due to the volume of requirements in the list and the perceived areas of overlap, there was a recognition that we needed to focus on the key themes and areas. Some classes of items are obviously more important than others. These important item classes came to be referred to as "tenets". Some of these tenets were discussed – see below – but others were not (e.g., privacy). With more time to discuss requirements, other tenets would have been discussed as well.

Tenets

Generally WG1 recognizes that programming and content has value, and mechanisms need to be put in place to protect intellectual property rights in such content. At a fundamental level this involves encryption and the use of a secure system that can identify, authenticate, and protect content from all of the points that have access to this system.

The group did not have sufficient time to completely identify all of the tenets, but a few key ones did surface and received extensive discussion, and at times debate.

Tenet: User Interface

The tenet that received the most focus had to do with the presentation of a MVPD's service. Although more comprehensive than just the user interface, the "UI" was the term we used to frame the discussion. Should a MVPD's UI be allowed to exist as the only possible method through which an MVPD's customer consumes the MVPD service? Or should competitive devices have access to (or continue to in the case of cable MSOs) a MVPD's services (or "Service" as MVPD's like to refer to it), for instance licensed linear programming, and enable those services to be presented by a retail device with its own UI? This topic received fervent debate. MVPDs state that they have come a long way from the days of simply broadcasting video channels, and placing them up on a list or grid on a TV guide. MVPDs also assert that a profusion of additional features have been added to their offerings, with most being incorporated into their UI.[1]

Other participants, such as consumer advocates, retail device manufacturers, and other MVPDs, assert that a fundamental feature of a competitive navigation device is that it has the option to present its own unique UI to access the MVPD services. Without the ability to present a unique UI, such parties assert, retail devices would be denied some ability to innovate and present the consumer with a differentiated and competitive alternative to an operator-supplied device. As a counter-point to this argument, the MVPDs noted that they are simply trying to honor their programming agreements.

[1] Examples include Start Over & Look Back, recent tuning history across devices, Voice Control, Caller ID on the TV (integrated with an operator's telephone service), HD Auto-tune (the automatic selection of HD versus SD channels when detected that an HD television set is attached), and on-screen Instant Upgrade and/or Bill Pay.

Tenet: Guide Data

Another topic that received much deliberation and discussion related to intellectual property rights in guide data. Some group members advocate that MVPDs should be required to provide retail devices with MVPD guide data (program information).

MVPDs pointed out that some of this data is provided under commercial terms that only allow a B-to-C (business to consumer) distribution, not a B-to-B (business to business) type arrangement. Consumer advocates and retail device manufacturers point out that certain guide data, such as VOD, is not subject to such constraints and is only available from the MVPDs.

Tenet: Technology Licensing

Additionally, CE manufacturers assert that technology required by the MVPD's architecture to implement their conditional access solution needs to be available through particular licensing terms (*i.e.,* be fair, reasonable, and non-discriminatory, or FRAND) to enable a competitive retail market. Some MVPDs have made clear that many such technologies are owned and controlled by third parties, with terms not under the control of the MVPD. Consumer advocates and retail manufacturers have made clear that they believe the FCC has the authority to require such licensing.[2]

[2] For example, see 47 CFR 76.1204(c), "No multichannel video programming distributor shall by contract, agreement, patent, intellectual property right or otherwise preclude the addition of features or functions to the equipment made available pursuant to this section that are not designed, intended or function to defeat the conditional access controls of such devices or to provide unauthorized access to service."

General Topics of Discussion

This section discusses other important areas of interest that were discussed amongst the WG1 members.

Scope of Work

Some group members expressed concern that several of the proposed requirements and tenets go beyond recommendations for downloadable security, and could conflict with contractual agreements (including licensing terms), intellectual property rights, and copyright law. Other group members state that the purpose of the working group is to help the FCC determine technical solutions in furtherance of Section 629 of the Communications Act which directs the FCC to assure the development of a market for retail navigation devices.

Technological Differences

An additional topic that received a lot of attention was the fact that a DBS system is essentially a one-way system while others are two-way.

Given that the statutory requirement calls for a “uniform, and technology- and platform-neutral” system, some think that this presents an immediate paradox: either two separate systems are described, bifurcated into one-way and two-way (thus no longer honoring the requirement), or the system must be treated solely as a one-way system, which is an objectionable compromise to some group members. Those members still think the requirements can be uniformly met, but we did not get into details.

Others do not believe there is any such paradox, and believe that “uniform, and technology- and platform-neutral” can be met without making two separate systems. Indeed, those WG1 members state that there are no particularly insurmountable issues to meeting the statutory requirement.

Appendix 1

REPORT OF WORKING GROUP 1 TO DSTAC

March 24, 2015

Introduction

Working Group 1 has collected a set of commercial requirements through presentations from five perspectives: MVPDs; CE/device manufacturers; consumer; content providers; and security.

The working group has not yet tried to reconcile the requirements presented.

The primary points that have been raised are summarized below.

MVPD Requirements

Jay Rolls, Charter, John Card, DISH and Steve Dulac, DIRECTV, presented requirements for MVPDs. Common elements include:

Security and Content Protection. Security and content protection for MVPD services includes support for the conditional access systems' (CAS) and Digital Rights Management (DRM) systems' trust infrastructure and model. MVPDs must follow compliance and robustness rules that help control how resistant devices must be to attack and how they manage content and related copy, retransmission, or use restrictions in order to prevent piracy and to protect content holders' rights. Protection also requires meeting content provider requirements that are part of negotiated licenses that give each party defined rights and obligations. For example, the content provider may define a geographic area, give larger in-home rights than out-of-home rights, require a hardware root of trust for high value content, limit what content is available to less trusted devices, and require other terms that rely on an unbroken chain of trust. Licenses may also include terms to protect the content providers' brand, such as acceptable advertising, channel position and neighborhood, and subscription tier placement.

Consumer Protection Obligations. MVPDs design their service to meet regulatory requirements, such as emergency alerts (EAS), closed captions, and limits on the web links shown to children. Cable and satellite providers have privacy obligations to protect personally identifiable information, including subscriber viewing habits. Proposed recommendation: A downloadable security solution must comply with these legal requirements placed on service providers.

Execution of Video Provider's Service Offering. Each MVPD assembles, markets and delivers a branded service that includes programming, integrated data, interactive features, a guide, and software that enforces content provider requirements. MVPDs continue to enhance their service. A poor consumer experience caused by either an MVPD or third party device adversely impacts the MVPD customer relationship. MVPDs protect and promote their brand and marketing to customers through their service.

Support for Business Operations. Any solution has to support the business operations of the service provider. For example, there are ordering processes for VOD and audit trails to handle billing disputes. Consumers may be provided the ability to upgrade their account from the application UI, which must then integrate with various billing systems.

Support for Distribution Architecture. Each MVPD also has unique and specific transport layers, codecs, control channels, etc., so the end-to-end delivery of service all the way to the consumer has to fit within that architecture.

Support for Service Installation and Configuration. Each MVPD also has requirements for how service is enabled or installed. For example, a satellite receiver (IRD) will not receive DBS service unless there is an Out Door Unit (ODU), Multiswitch and professional installation to point the ODU at the satellite; when service providers install wired networks, they test signal levels and use remote diagnostics to insure proper installation.

Advertising. MVPD operations are funded in part by advertising, so MVPDs operate advertising systems that: meet content provider restrictions; provide audit paths for advertisers; and enable a variety of more advanced types of advertising, such as zone advertising, local advertising using DVR technology, advertising targeted to election districts, advertising targeted to different interest groups, transactions and usage reporting, and interactive Request For Information (RFI) ads where the consumer can, for example, order a coupon with their remote.

Customer Support. MVPDs need built-in support for customer service, such as access to diagnostic tools that are often included in CPE. Customers may need to access information generated by these tools in conversations with Customer Service Reps to resolve customer problems.

Change. These systems change on a frequent, sometimes regular basis. There are regular updates, bug fixes and feature enhancements. MVPDs continually maintain and enhance security to protect consumers and content. Device robustness requirements can also change over time. On occasion, systems can change in a way that obsoletes older devices.

Intellectual Property. MVPDs operate within limits of intellectual property. They must: respect conditions of copyright licenses from commercial video content providers that are typically included in bilaterally negotiated affiliation and retransmission agreements; respect the intellectual property controlled by other licenses (e.g. guide data that Rovi or Tribune licenses for limited use); license or otherwise accommodate patents and intellectual property in their implementations.

Device Manufacturer Requirements

Brad Love, Hauppauge, presented device requirements that manufacturers would like to see in the future:

User Interface. The system must allow for, but not require, third-party manufacturers to supply their own user interfaces. Third-party user interfaces allow for unique consumer experiences and differing feature sets than offered by an MVPD, in addition to fostering meaningful competition. The third-party user interfaces must be allowed full access to all linear channels, VOD, and PPV. Remote presentation of user interface (RUI) must also be allowed, such as might be the case for 'headless' (non-HDMI) gateway devices.

Uniform Provider Terms. All content providers should ideally follow uniform terms of affiliation license, and use common copy control instructions. Signaling or embedding of copy control data is required for all programs. Recording must not be prohibited for non-premium programs, and fair use should apply for all recorded material.

Output Restrictions. A device must be able to output to any secure/licensed device. Recordings must be able to be exported to any licensed/secure device in approved formats, depending on copy control restriction. Secure network retransmission of programs via DTCP-IP or other secure methods must be allowed. In the case of 'copy free' programs network transmission in the clear must be allowed, as is the case currently.

Guide Data. A device should ideally receive guide data from MVPD's for at least 7 days. However, guide data for VOD and PPV must always be supplied by the MVPD in order to receive accurate and up to date information on dynamic content. A unified method of distribution must be chosen for guide data delivered from MVPD's.

EAS. A device must have some uniform way of receiving EAS data from MVPD's.

Security. Every MVPD should ideally use the same security methods and CAS, or at most, a limited number of permutations. There should be common reliance on security methods for the DCAS module. There must also remain a 'man machine interface' (MMI) to allow interaction with the DCAS module.

Terms. All required technology should be available under FRAND licenses (fair, reasonable, and non-discriminatory). A neutral organization should be responsible for initial certification and self certification should be allowed for subsequent re-testing.

Portability. The device must work uniformly across all MVPD's and be user friendly to activate. If upstream communication is required minimal restriction should be placed on the source of the connection.

Consumer Requirements

Adam Goldberg, Public Knowledge, presented a consumer view that included these requirements:

The system must allow unaffiliated third-party manufacturers to build navigation devices, and the system must allow those devices to be sold directly to consumers through unaffiliated (and unconstrained) retail channels.

Retail navigation devices must function properly on all MVPD’s networks, and must be portable to other networks (e.g., when a consumer changes MVPD or moves into another cable operator’s footprint).

Retail navigation devices must allow for a wide range of product prices, features, manufacturers, etc., and the system must impose only requirements necessary on retail navigation devices to enable the system.

The system must provide discovery of all available television services to retail navigation devices (what services are available on the network), and must provide a mechanism for identifying them in, e.g., an electronic program guide.

The system must allow (but need not require) a retail navigation device to provide its own user interface, and such user interface must be capable of enabling navigation to all available services (including services which require a commercial interaction, like PPV).

The system must enable retail navigation devices to provide EAS information, and closed captioning. The system must enable retail navigation devices to provide parental controls (v-chip).

Content Providers Requirements

John McCoskey, MPAA, presented requirements of content providers:

Authentication. The system must require and support basic authentication practices, including: subscriber validation, device authentication, subscription validation and service entitlement.

Content Protection. The system must meet at least the same content protection requirements that existing solutions meet today, with no decrease in content security due to downloadable security. The system must be upgradable. The MovieLabs *Specification for Enhanced Content Protection – Version 1.1* shall be the reference model for content protection.

Respect of Licensing Agreements. The system must support the technical requirements of content/service licenses. The solution must ensure content/service handoff is consistent with license terms with MVPDs.

No Disaggregation of Service. The solution must prevent disaggregation of retail content offerings licensed to MVPDs. Devices are to access the existing service provided by the content owner and MVPD, not to disaggregate service elements outside of contractual agreements.

Security Requirements

Robin Wilson, NAGRA, presented requirements for security that include:

Robustness. Robustness requirements establish different levels of resistance to different levels of resources applied by attackers, which can range from college student with little time and money to state actors. There are conventional breaking points for different levels of robustness, such as 480i (Standard Definition), 720p (low end of High Definition), 1080i and 1080p (high end of High Definition) and 4K (Ultra High Definition).

Encryption and key exchange. There are two complementary processes in CAS: encryption and key exchange. Encryption has advanced from DES to Triple DES to AES. The integrity is strong if you have strong keys. The second part of the process is key exchange and how you securely get the keys to the subs to decrypt content. Common encryption can support multiple key exchanges.

Certification. Certification or auditing is required to ensure that security is implemented to the level specified and required by the content owner.

Downloadable. The presentation also addressed some future issues associated with downloadable security:

- A key ladder attached to a root of trust
- The security downloader itself, and management of keys. The function has to trust the code to operate within a chain of trust.
- Need to address renewability
- Need to preserve room for innovation in rights management

- Need to evaluate balance between security implemented in secure software and one or more hardware roots of trust

Ban the term "Black Box." The term "black box" has specialized meaning in cryptography, and DSTAC should avoid the term.

Further Discussion

There is much room for further discussion. Because of the short period provided, the working group only had time to take an initial snapshot, and not to completely analyze these requirements or try to reconcile them.

Appendix 2

Number	Requirement
M 1	The system must support the Conditional Access System (CAS) and Digital Rights Management (DRM) trust model and infrastructure requirements in the service provider's system.
M 2	The system must follow the service provider's rules for compliance and robustness rules, for managing content and related copy, retransmission, or use restrictions.
M 3	The system must support each service provider's fundamental data and video delivery mechanisms: transport layers, codecs, control channels, return paths etc. as required to fit within the service provider's delivery architecture.
M 4	The system must preserve and present the branded service that represents the MVPD's offering, including but not limited to the programming, integrated data, interactive features, a guide, and software that enforces content provider requirements.
M 5	The system must meet content provider requirements that are part of negotiated licenses and retransmission agreements that give each party defined rights and obligations.
M 6	The system must support all of the service provider's regulatory requirements for content delivery, such as channel position, emergency alerts (EAS), closed captioning, and limits on web links shown to children.
M 7	The system must not allow relocating a channel to a different number or 'neighborhood' in the line up.
M 8	The system must support the service provider's obligation to protect all personally identifiable information of the customers, including subscriber and viewing habits
M 9	The system must support the service provider's protection of the privacy of video streams.
M 10	The system must not run advertisements, promotions or overlays over the service provider's video programs or over the guide.
M 11	The system must support the service provider's advertising systems that honor content provider rules and restrictions, and must prevent alteration of advertising as provided.
M 12	The system must support the service provider's audit paths for the tracking of advertising and viewership.
M 13	The system must support the service provider's requirements for service enablement and installation. The system must support the appropriate network connections or receivers (such as a satellite receiver), and wired networks with appropriate signal levels and diagnostics.
M 14	The system must support all business operations of the service provider, as required to support ordering, upgrading, billing, authorizing, and promoting services offered to customers.

M 15	The system must support the service provider's advanced advertising features, such as zone advertising, local advertising using DVR technology, advertising targeted to election districts, advertising targeted to different interest groups, transactions and usage reporting, and interactive Request For Information (RFI) ads
M 16	The system must support diagnostic tools required by the service provider to install, upgrade and troubleshoot operation of the system. These tools must be accessible by customers and/or service provider customer service representatives to resolve customer problems.
M 17	The system must support the service provider's ability to be update service with feature enhancements and bug fixes required to maintain or enhance the security system that protects content and users.
M 18	The system must allow for updating of robustness requirements to match the current state of the art.
M 19	The system must respect the intellectual property controlled by other licenses, such as data and properties delivered by 3rd party EPG or content providers
M 20	The system must not impose new patent or intellectual property obligations on the service provider.
M21	Guide and Program data will only be provided via the MVPD's integrated service environment. See M4.

B1	The system must protect linear channels and linear PPV.
B2	The system must support "pushed" (precached) VOD content delivered by DBS.
B3	The system must support "pulled" (on-demand) buffered content delivered by DBS or broadband.
B4	The system must support start over/look back content delivered by broadband to STB.
B5	The system must support linear streamed content to in-home devices in proximity to the STB.
B6	The system must support streaming linear channels to authenticated out-of-home devices via (native) app and (HTML5) website.
B7	The system must support streaming on-demand programming to authenticated out-of-home devices via (native) app and (HTML5) website. (Differs from B6 because of included search and possible purchase.)
B8	The system must support download of on-demand programming to authenticated out-of-home devices via (native) app and (HTML5) website.
B9	The system must support start over/look back content delivered by broadband to to authenticated in-home devices via (native) app and (HTML5) website.
B10	The system must support start over/look back content delivered by broadband to to authenticated out-of-home devices via (native) app and (HTML5) website.
B11	The system must support authenticated linear and/or on demand streaming and/or download, using content owner's app and/or website.

B12	The system must support place-shifted content , streaming and/or download in-home and/or out-of-home and/or streaming via STB (or an external transcoder device) to devices (on service provider's app or website).
B13	The system must support delivery of content that is restricted by exclusivity deals managed by the content owner.
B14	The system must support delivery of content that is restricted by the service provider because of rational reasons. (Expected future discussion)
B15	3rd party devices should by default present all content available from the service provider.
B16	The system must support channels assigned to discrete packages. Packages must have unambiguous definition; contain enough channels; and there must be enough packages available to manage current and foreseeable operations. (Design requirement both inside the CAS and for security API)
B17	The system must allow different resolutions of content to be managed by different entitlements.
B18	Rights managed by the system must have different availability windows with defined start and end times.
B19	The system must support restricting the availability windows (times and dates) for features and content to the broadcast time of events.
B20	The system must support expiration dates and times (possibly never) for content.
B21	The system must support the addition and deletion of channels in one or many packages.
B22	Same as B15.
B23	The system must support different packages and channels between DBS and broadband delivery.
B24	The system must support different event lineups on a channel simultaneously received by DBS and broadband.
B25	The system must support timely deletion (removal, "take down") of events and channels.
B26	The system must respond to deletion (removal, "take down") events and channels within one hour. (3rd party device accuracy implications)
B27	The system must support simultaneous delivery of the same channel on DBS and broadband.
B28	The system must distinguish between instances of a channel delivered on DBS and broadband.
B29	The system must distinguish between instances of content delivered over different IP networks. (For DBS when additional carriage agreements are in place)
B30	The system must support delivery to single family homes.
B31	The system must support delivery to multi-dwelling units.
B32	The system must support delivery to restaurants and hotels.
B33	The system must support delivery to hospitals.
B34	The system must support delivery to schools.
B35	The system must support delivery to business offices.

B36	The system must support delivery to malls and commercial shopping establishments.
B37	The system must support delivery to aircraft and other vehicles.
B38	The system must support limiting delivery of content to within or excluded from one or more disjoint, adjacent, and/or overlapping geographic territories.
B39	The system must support limiting delivery to a subscriber account billing address within a territory.
B40	The system must support use of geofiltering technology.
B41	The system must support use of Content Delivery Networks for broadband distribution.
B42	The system must support blackouts of particular programs.
B43	The system must distinguish between and blackout specific instances of particular programs.
	The system must support real-time updates to blackouts.
B45	Same as B15.
B46	The system must allow content to be restricted to "in-home" use.
B47	The system should support an authenticated communications path with a 3rd party device.
B48	The system must support different rights for different devices.
B49	The system must distinguish among different other CAS and DRM systems, and allow reasonable treatment of differences.
B50	The system must support delivery of SD and/or HD to particular devices.
B51	The system must not interfere with viewing measurement technologies.
B52	The system must not interfere with watermark technologies.
B53	The system must support content-owner approved content protection (output) technologies.
B54	The system must support the pass-through and generation of CCI on outputs.
B55	The system must support CCI settings agreed to between content owners and service providers.
B56	Content owners must approve the system.
B57	The system must support content-owner approved DRM systems.
B58	The system must support a range of robust solutions.
B59	The system must support a requirement that devices must be registered to a subscriber account.
B60	The system must support a requirement that no more than X devices may be registered to a subscriber account at any given time.
B61	The system must support a requirement that no more than X concurrent streams of a content owner’s programs might be allowed to devices registered to one subscriber account .
B62	The system must support a requirement that no more than X downloads of a content owner’s programs might be allowed to devices registered to one subscriber account.
B63	The system must support AES-128.
B64	The system must support different behaviors with "jailbroken" devices.

B65	The system must support restrictions on user authentication methods (e.g. user ID and passwords of sufficient complexity).
B66	same as B55
B67	same as B40
B68	The system must support 3rd party security audits.
B69	same as B52
B70	The system must allow appropriate response to security threats of varying magnitudes.
B71	The system must support monitoring live operations.
B72	The system must support reasonable withholding of content to particular devices or subscribers.
B73	The system must support reinstatement of service after security issues are resolved.
B74	The system must support "channel neighborhoods".
B75	The system must allow particular programs not be listed with other programs.
B76	The system must support reasonable restrictions on foreign content overlays.
B77	The system must support use of service provider provisioned logos on 3rd party devices.
B78	The system must support updates to service provider provisioned logos.
B79	The system must support presentation of pre-roll information.
B80	The system must support Disabling the “Fast Forward” remote control feature during advertising for services (e.g. Start Over / Look Back).
B81	The system must preclude automatic deletion of ads from DVR recordings of linear services.
B82	The system must support use of DVR recording space for dynamic ad insertion.
B83	The system must support dynamic ad insertion for content distributed by CDN.
B84	The system must support "blind" ad sales.
B85	The system must support pre-order of PPV content.
B86	The system must support instant purchase of PPV content.
B87	The system must allow a subscriber to manage features of their subscription packages in online and offline operation.
B88	The system must support timely purchase reports.
B89	The system must operate in accordance with privacy regulations and user agreements.
B90	The system must support collection of information about the viewing of DBS distributed programs by its subscribers.
B91	The system must support report of usage/viewership of broadband delivered content and downloaded content.
B92	The system must support communication of a Listing Service ID.
B93	The system must support controlled announcement of a program or channel availability.
B94	The system must support start and stop dates for program availability and start dates for certain features like DVR recording and customer directed commercial skips.

B95	The system must support the delivery of trigger information for collecting programs from DBS distribtion or broadband.
B96	The system must support different lead times for service and program related metadata.
B97	The system must operate in accordance with applicable regulations and laws.
B98	The system must allow a service provider to respond to market requirements and customer needs
B99	The system must allow a service provider to define a competitive product – "The Service"
B100	The system must allow a service provider to offer a competitive product – "The Service"
B101	The system must allow the service to be maintained (throughput and scale)
B102	The system must allow a service provider to control its costs of doing business
B103	The system must not interfere with the measurement of the effectiveness of other deployed systems
B104	The system must not interfere with the measurement of the effectiveness of existing business processes
B105	The system must allow changes to other deployed systems
B106	The system must allow changes to existing business processes
B107	The system must allow the service provider to specify systems used to deliver the service
B108	The system must allow the service provider to manage systems used to deliver the service
B109	The system must allow a service provider to stop support for obsolete features that are no longer cost effective
B110	The system must allow for delivery system and component testing and qualification
B111	The system must secure the signal
B112	The system must secure the content
B113	The system must itself be secure
B114	The system must allow a service provider to maintain existing customer relationships
B115	The system must allow a service provider to negotiate for the best deal with vendors, suppliers, and 3rd party partners
B116	The system must support management of expected events (DST)
B117	The system must support management of unexpected events (system failure)
B118	The system must allow a service provider's business to grow
B119	The system must allow a service provider to add new customers
B120	The system must allow a service provider to increase revenue from existing customers
B121	The system must respond to changes in content owner requirements
B122	The system must allow the service provider to develop new features and new services
B123	The system must allow the service provider to deploy more efficient technology and processes

B124	The system must enforce agreements customers make with the service provider.
B125	The system must not leak unpaid-for content.
B126	The system must enforce agreements service providers make with the customer.
B127	The system must support the communication of clear terms and pricing.
B128	The system must communicate the subscriber's clear acceptance of an offer.
B129	The system must support the service provider to resolve customer issues.
B130	Same as B97

C1	The system must allow unaffiliated third-party manufacturers to build navigation devices, and the system must allow those devices to be sold directly to consumers through unaffiliated (and unconstrained) retail channels.
C2	Retail navigation devices must function properly on all MVPD's networks.
C3	Retail navigation devices must be portable to other networks (e.g., when a consumer changes MVPD or moves into another cable operator's footprint)
C4	Retail navigation devices must allow for a wide range of product prices, features, manufacturers, etc.
C5	The system must impose only (the minimal set of) requirements necessary on retail navigation devices to enable the system.
C6	The system must provide discovery of all available television services to retail navigation devices (what services are available on the network).
C7	The system must provide a mechanism for identifying all available television services in, e.g., an electronic program guide.
C8	The system must allow (but need not require) a retail navigation device to provide its own user interface, and such user interface must be capable of enabling navigation to all available services (including services which require a commercial interaction, like PPV).
C9	The system must enable retail navigation devices to provide EAS information, and closed captioning. The system must enable retail navigation devices to provide parental controls (v-chip).

P1	The system must require and support basic authentication practices, including: subscriber validation, device authentication, subscription validation and service entitlement, and must include geolocation to support territorial and regionally restricted content distribution.
P2	The system must meet at least the same content protection requirements that existing solutions meet today, with no decrease in content security due to downloadable security. The system must be upgradable. The MovieLabs Specification for Enhanced Content Protection – Version 1.1 shall be the reference model for content protection.
P3	The system must support the technical requirements of content/service licenses. The solution must ensure content/service handoff is consistent with license terms with MVPDs.

P4	The solution must prevent disaggregation of retail content offerings licensed to MVPDs. Devices are to access the existing service provided by the content owner and MVPD, not to disaggregate service elements outside of contractual agreements.

D1	The system must support, but not require, third party user interfaces.
D2	Third party user interfaces must have access to all linear channels, VOD, and PPV.
D3	Remote presentation of user interface (RUI) must be supported, but not required.
D4	All content providers must have common copy control instructions.
D5	Signaling or embedding of copy control data must be required for all programs.
D6	Recording must not be prohibited for non-premium programs.
D7	Devices must be able to output content via any secure output to any secure device.
D8	Recordings must be exportable to any secure device, subject to copy control restrictions.
D9	Notably, DTCP-IP outputs must be supported.
D10	TO BE DISCUSSED: In the case of 'copy free' programs, network transmission in the clear must be allowed, as is the case currently.
D11	Retail devices should be provided with MVPD guide data by the MVPD's for at least the subsequent seven days.
D12	Guide data for VOD and PPV must be supplied by the MVPD to the retail device.
D13	Guide data, when provided, must be in a single standardized format.
D14	The system must have a uniform way of supplying EAS data from MVPD to retail devices.
D15	Retail devices must be supplied content secured by a uniform security method and CAS, or at most, a limited number of permutations.
D16	There should be a common reliance on security methods for the DCAS module.
D17	There must also remain a 'man machine interface' (MMI) to allow interaction with the DCAS module.
D18	All required technology must be available under FRAND licenses (fair, reasonable, and non-discriminatory).
D19	Neutral organization(s) must be responsible for initial certification of a device, and self-certification should be allowed for subsequent re-testing.
D20	The device must work uniformly across all MVPD's and must be user friendly to activate.
D21	If upstream communication is required, minimal restriction should be placed on the source of the connection.

S1	The system shall avoid common failure modes and careful consideration should be given to avoid selecting any single system or subsystem that could result in catastrophic failure to the whole system.

S2	In addition to downloading a CAS or DRM client, the system shall have a mechanism(s) to download countermeasures (SW patches) to fix security or other flaws without replacing the whole security application or SW stack.
S3	The additional security aspects and risks associated with the downloader needs to be tied to the security of the whole system and addressed.
S4	The scrambling or encryption algorithm used for the content should conform to open and fully disclosed industry standards such as AES 128 and defined in such a way (block size, key periodicity, etc...) that allows common encryption (key sharing / simulcrypt) across both CAS and DRM use cases.
S5	The security system shall allow different levels of robustness to match the license agreements requirements, content value, content resolution, and threat models while matching appropriate cost and complexity goals of rendering devices.
S6	Compatibility should be provided for browser or application environments using emerging standards such as EME.
S7	The system shall be designed such that CAS and DRM system can interoperate with common encryption (i.e. without trans-encryption).
S8	The system shall allow use cases that include linear/live broadcast/OTT, VOD and sideloading (redunant to other more verbose definitions).
S9	All SW components of the system shall be replaceable via download.
S10	The system shall support one or more HW roots of trust (more than one to avoid a potential single point of catastrophic failure.
S11	The system shall support a SW root of trust but only in devices where no HW root can be used and in addition, the robustness requirements can be met for the type of content processed.
S12	The system shall provide the necessary robustness to sustain the likely threat models.
S13	Scalability: The system must scale such that there should be no limits on addressing many tens of millions of devices in a timely manner without undue latency in authorizing or de-authorizing a device.
S14	Latency: The performance of the system must be fast enough to avoid adding to customer support issues and maintain subscriber satisfaction. A goal may be for instant or near instant authorization which greatly helps in customer satisfaction, acquisition, retention, self-provisioning etc. (Instant gratification makes for happy customers)
S15	Addressability: The system must be able to efficiently address all combinations of individually channel line ups, at the required Scale, and with the required Latency (these are often technically conflicting challenges).
S16	One Way Network Use: If this mode is deemed within the scope, the system must have a mode of operation so that communications such as authorization and de-authorization must be able to be carried in the one-way data stream (DBS to land, DBS to aircraft....)

Letter	Section
M	MVPD - MSO
B	MVPD - DBS
C	Consumer
P	Content / Programming
S	Security
D	Device

REPORT OF WORKING GROUP 2 TO DSTAC

April 21, 2015

I. SUMMARY

There is variation in current video providers' distribution technologies and platforms, as the Multichannel Video Programming Distributor (MVPD) distribution networks were not built to a common set of nationwide standards. At a high level, the larger US Cable operators and Verizon mostly use one or both of two the two primary CAS (Conditional Access Systems) vendors, and all support CableCARD for limited services. Both US Cable and Verizon use Quadrature Amplitude Modulation (QAM) for broadcast signals while over Hybrid Fiber Coax (HFC) or B/GPON (Broadband-/Gigabit-capable Passive Optical Networks) fiber networks. Verizon adds hybrid QAM/IP for on-demand content and two-way services. Direct Broadcast Satellite (DBS) also has two major variants for transport and CAS. AT&T uses IP unicast and multicast over DSL or B/GPON fiber, with a Digital Rights Management (DRM) approach instead of CAS.

MPEG-2 is still the most common transport mechanism used for broadcast content; however, there are variations in transport structure for linear and for Video On Demand (VOD) content, and newer IP transports are starting to be used for broadcast over IP. In video encoding technology, while many older devices tied to MPEG-2 Transport in hardware are also tied to MPEG-2 video format, different variants of MPEG-2, MPEG-4 AVC and MPEG HEVC are used for video compression across MVPDs. For IP delivered content to consumer-owned devices, a range of software DRM solutions are used, across two dominant transport models, Apple HTTP Live Streaming (HLS) and Microsoft Smooth Streaming. There is a cross industry effort to standardize streaming formats using MPEG-DASH and DRM access using W3C HTML5 Encrypted Media Extensions (EME) standards.

Content protections systems, like CAS and DRM systems, are one part of the secure delivery of all providers' commercial content and multichannel service. CAS and DRM control the authorizations that turn video on and off, but there are many threats to security and other parts of their systems that MVPDs must address.

All content protection systems, including CAS and DRM solutions, use a combination of hardware and/or software to secure delivery of video services. And most solutions have software downloadable components. Security can be improved by judicious use of hardware. For example, parts of the software solution can execute in a secure portion of the hardware (Trusted Execution Environment (TEE)) instead of on the less-secure general purpose Central Processing Unit (CPU).

Across all service providers, a widespread and fast growing approach that has developed for delivering video service to customer owned devices is through "apps." The consumer electronics world broadly uses this app model as the means for bridging the differences between varied and rapidly changing services and varied and rapidly changing consumer electronics platforms. The app model uses IP-distributed and enabled applications with either software-downloadable DRMs or platform supported DRMs. "Over the top" video distributers, like

Netflix and Amazon, have to custom build and support different versions of their client software for every different platform they support, and some device manufacturers accommodate and test against some of these applications. Multichannel providers follow the same model. Each distributor and provider delivers their video services through apps to millions of customer-owned IP-enabled devices, including iOS, Android, Mac/OS X, PC/Windows, Xbox, Roku, Kindle, and a variety of Smart TVs.

There are early deployments of VidiPath and broad deployment of RVU technology, developed in multi-industry bodies, for delivering multichannel service via apps to client devices on home networks. VidiPath supports IP video delivery through an in-home device and/or "cloud-to-ground" delivery directly from a network to the client. VidiPath leverages browser technology to present the MVPD's user interface as part of the consumer device navigation framework, but does not directly provide for access to MVPD content via third-party UI today.

The application approaches abstract the diversity and complexity of service providers' access network technologies and customer-owned IP devices, accommodate rapid change and innovation by both service providers and consumer electronics manufacturers, and may make use of a combination of software-downloadable security with hardware roots of trust.

II. OVERVIEW: SOFTWARE, HARDWARE AND DOWNLOADABLE SECURITY

All content protection systems, including CAS and DRM solutions, use hardware and/or software to secure delivery of video services. Although CableCARD has downloadable elements, it is not considered a downloadable CAS solution. There are different capabilities and therefore robustness of solutions in what features the hardware provides to assist the software in securing the solution. Most solutions have a way to download the software component. A downloadable CAS solution can include combinations of software component, hardware component, Trusted Execution Environment provided by the hardware, secure download model for the software component, and secure root of trust that can authenticate the hardware so the software can trust it.

Content protection systems vary in how and when the content protection system is installed:

- Built-in: Some content-protection systems are installed at time of device manufacture. While they may include some software-updatable components, they cannot be changed.

- Hardware installable: Some content-protection systems consist of hardware that can be installed into a device by the operator or by the consumer into an external hardware connector. For example, a smart card content-protection system is installed into a smart card reader external hardware connector, while a CableCARD (and DVB-CI) are installed into a PCMCIA external hardware connector. While they may include some software updatable components, they require installation of hardware to an external connector.

- Software downloadable: Some content-protection systems consist of a software-only module that is installed onto a device through downloading. For example, content-protection in PC Web browsers uses software downloadable DRMs. Software downloadable DRMs run on the general-purpose CPU of the device and may also use TEEs, if present, but don't require any hardware to be installed via a external hardware connector.

There is a range of security depending on the type and use of hardware elements. For example the security of the solution can be improved by judicious use of hardware. Hardware elements can be used to keep some elements more secure, for example having parts of the software execute in a secure portion of the hardware (Trusted Execution Environment) instead of the general purpose CPU so that secrets are not exposed in general purpose RAM or on accessible buses within the device. For many solutions on consumer devices such software-only DRM used on tablets and PCs, the general purpose CPU is not used as a hardware element of security and the software component may try to obfuscate critical elements (object code, variable names, cryptographic elements, etc.) because of the lack of secure hardware components.

There are standardization efforts underway for these trusted execution environments, secure download models, and common ciphers/scramblers. There is work underway in W3C to develop a standard for an application interface to a DRM. There is no W3C effort to standardize the DRM model.

III. CURRENT VIDEO PROVIDERS' DISTRIBUTION TECHNOLOGIES

This section discusses the current distribution technologies in use today by MVPD's. Table 1 summarizes the various CAS, core ciphers, transports, control channels, and video codecs in use.

A. Cable

Cable system architectures reflect fundamental differences dating from different design goals, different vendors, and different owners. The General Instruments (now ARRIS) design was tailored primarily for the more rural and less clustered systems owned by Tele-Communications, Inc., with a focus on increased channel capacity, minimized head-end cost, and centralized set-top control and authorization. The Scientific-Atlanta (now Cisco) design was tailored primarily for the more urban and clustered systems primarily owned by Time Warner Cable, with a focus on two-way interactive services such as VoD, the ability to add applications and services to set-top boxes over time, and local control and authorization. Thus, even though there are some shared elements, such as MPEG-2 video compression, there are fundamental differences in technologies for CAS, controllers, the out-of-band (OOB) communications channels used for command and control of the set-top box, network transports, QAM modulation, video codecs, core ciphers, advanced system information such as network configuration, session management, operating system, processor instruction set, interactive services, billing systems, applications necessary for presentation of services and in the set-top boxes. [3] Unlike the telephone network that was originally built to a common nationwide standard, the cable industry is a roll up of these many technologies. [4] A single company can be operating both Cisco and ARRIS systems in different parts of their network.

CableCARD technology works across all US cable systems and FiOS. There is a competitive multi-vendor set-top box market for MVPD-purchased devices in the US, including TiVo as a supplier of set-top boxes to cable operators that depends on CableCARD.

B. Satellite

The Direct Broadcast Satellite (DBS) architectures of DIRECTV and DISH Network contrast through fundamental differences. Although they both transmit signals one-way from satellite to ground, there are differences in orbital slots that customer outdoor units (ODUs) must face, the satellite frequencies used, antenna components such as the low-noise block downconverters (LNBs), the multiswitches used to "tune" a channel to the right input frequency and/or right satellite, the CAS systems, the RF encoding of the signals, the transport stream structures, and the set-top boxes (also known as IRDs). While both systems base multiswitch control on the DiSEqC standard, each uses proprietary extensions. The systems also support different home installation architectures. [5][8].

C. AT&T U-verse

AT&T delivers its U-Verse service over both copper (VDSL) and Fiber (FTTP) networks using Internet Protocol (IP) (although not using the Internet). Service is delivered from one Super Hub Office (SHO) to multiple Video Hub Offices (VHOs). Linear content is multicast to the end user, when requested. AT&T's proprietary Instant Channel Change (ICC) unicasts to the subscriber until a multicast stream is joined. U-verse delivers a combination of Unicast and Multicast streams even for live linear channels. VOD is unicast to the subscriber on request. [2]

D. FiOS

Verizon's FiOS service is a hybrid QAM and IP service. Verizon designed its downstream linear service to leverage prior work by the cable industry and emulates cable for downstream linear using an overlay wavelength on its fiber, but there is no cable RF return path, so interactivity is handled using IP. FiOS VOD is delivered using Internet Protocol (IP). Each set-top box includes two interfaces: an interface to the overlay wavelength for linear services and certain control signaling; and an IP interface for IP VOD, widgets, guide data, gaming, and certain control plane signaling. All feeds are integrated into a single service within the set-top box. [9]

E. Conditional Access

There is variation in conditional access deployment and use among all providers.

Diversity of conditional access can be a source of strength in security by reducing the target size (and raising the proportional costs to an attacker) and by reducing the consequences of a breach. For example, both satellite companies have designed their conditional access to accommodate ongoing and continual evolution in the CAS used with their customer base. [6] Cable operators use a variety of CAS systems. [3] MVPDs refresh their entitlement messaging in order to limit the amount of service that may be illegally consumed before a new entitlement message is required. [3] Table 1 summarizes variation in known, deployed CAS systems, each

of which has its own unique licensing and trust infrastructure, along with the associated core ciphers, transports, control channels, and video codecs in use.

MVPD	CAS	Core Cipher	Transport	Control Channel	Video Codec
Cable	• DigiCipher 2 • MediaCipher • PowerKey • NDS VideoGuard • Conax • Nagravision • DTA • OMS • BBT • Verimatrix VCAS for Broadcast-Hybrid	• DES-CBC • DES-CBC • DES-ECB • CSA • CSA • CSA • DES-CBC/ECB • CSA/DES/AES • AES • AES/DES/CSA	• QAM/MPEG-2 TS • QAM/MPEG-2 TS • QAM/MPEG-2 TS • QAM/MPEG-2 TS • QAM/MPEG-2 TS • QAM/MPEG-2 TS • QAM/MPEG-2 TS • QAM/MPEG-2 TS • QAM/MPEG-2 TS • QAM/IP/MPEG-2 TS	• SCTE-55-1 • SCTE-55-1/DOCSIS • SCTE-55-2/DOCSIS • Generic IP • Generic IP • SCTE-55-2/DOCSIS • In-Band • DOCSIS • Generic IP • Generic IP	• MPEG-2/AVC • MPEG-2/AVC • MPEG-2/AVC • MPEG-2/AVC • MPEG-2/AVC • MPEG-2/AVC • MPEG-2/AVC • MPEG-2/AVC • MPEG-2/AVC • MPEG-2, MPEG-4/H.264
Satellite	• NDS VideoGuard • Nagravision • Terrestrial free-to-air	• DES/AES • CSA/DES/AES • N/A	• QPSK/DSS TS, DVB-S2/MPEG-2 TS • QPSK, 8-PSK Turbo/MPEG-2 TS • 8-VSB/MPEG-2 TS	• In-Band • In-Band • N/A	• MPEG-2/AVC • MPEG-2/AVC • MPEG-2
Telco	• Mediaroom DRM • MediaCipher/PowerKey • Verimatrix VCAS for IPTV	• AES • CSA • AES/DES/CSA	• Multicast/Unicast-IP/VDSL/FTTP • QAM/MPEG-2 TS & IP/BPON or IP/GPON • IP Multicast MPEG-2 TS	• IP/VDSL/FTTP • SCTE-55-1/SCTE-55-2 • Generic IP	• AVC • MPEG-2/AVC • MPEG-2, MPEG-4/H.264
Google Fiber TV	• Widevine	• AES	• IP/GPON	• IP/GPON	• AVC

Table 1 – Currently Deployed CAS Systems [3][24]

Terrestrial methods are included because some DBS implementations still use local off-air broadcast pickup at the set-top box. “Universal DTA” CAS is designed to work with both Cisco and ARRIS conditional access.

Verizon operates cable systems which support both MediaCipher and PowerKey at the same time on the same distribution plant using key sharing technology similar to Simulcrypt, where the MediaCipher is the key master, e.g. creates the key content scrambling key used by the PowerKey. These systems operate using only the Common Scrambling Algorithm (CSA) scrambling mode. Some Time Warner Cable systems use the Cisco Overlay feature which supports both DigiCipher and PowerKey use at the same time. The Cisco Overlay feature uses selective multiple encryption to independently encrypt content where critical packets are duplicated and each copy separately encrypted with DigiCipher and PowerKey. Non-critical packets are sent in-the-clear. Cisco Overlay is very similar to Sony Passage. With Cisco overlay, neither CAS is the “key master” and specific use of CSA is not required.

CAS vendor Verimatrix’s presentation showed how smaller US telco and cable companies use “multi-rights” head-ends that support two or more CA/DRM systems and “downloadable clients” where the in-home device supports two or more downloadable CA/DRM clients, so that, not all devices have to support all CA/DRM systems. Verimatrix also showed how an operator CPE device can terminate the network CAS and bridge to multiple third-party DRMs or link protection systems to reach various kinds of devices. Forensic watermarking, a method that enables after-the-fact detection of potential sources of unlawful distribution of content, can also be added either within the client’s SOC (for chips that include watermarking capability) or in the head-end (for on-demand content) [21]

IV. PROTECTION AGAINST SECURITY THREATS AND RISKS

CAS and DRM are a small but necessary part of the secure delivery of commercial content and multichannel service. Service providers use other techniques to protect against security threats and risks. CAS turns video on and off, but there are many other threats that MVPDs must address:

- threats that arise through circumvention of content license restrictions;
- threats to the chain of trust model that assures secure flow of content from content supplier to the distributor to the consumer;
- threats to privacy protections; and
- threats to the service itself, such as failure to render service, failure to support billing, or interference with advertising.

MVPDs address these threats through a variety of technological measures

A. Content license restrictions on geographic or device segmentation

All video distributors assemble a collection of licensed commercial content through individually-negotiated copyright licenses with content owners and licensors (for example, for the right to carry ESPN) and retransmission consent agreements for terrestrial broadcasts (for example, for the right to carry FOX broadcasting affiliates in particular local markets). All are bound separately by the varying terms of these bilateral agreements.

Content providers segment the market through licenses. For example, they impose geographic and mobility restrictions on distribution, such as distinguishing the right to distribute content in-home versus out-of-home, or licensing on some devices or DRM systems but not others. Not all content is licensed for reception on all devices. Licensors typically value their content higher when distribution is closer to its original release than at later dates, and content at a higher resolution is generally valued higher than at lower resolution. [3] Thus, certain platforms or devices that have a higher level of security may enjoy higher resolution content or earlier release window content than devices with a lower level of security. [6] “Over the top” providers are also part of this licensing system. As the Wall Street Journal recently explained, “Virtually every major online video player is in the market for the kind of ‘premium’ programming that traditional entertainment firms create.” [11]

When licensing to multichannel platforms, agreements between service providers and content providers enforce availability windows, define channel placement and the neighborhood in which the channel is located, subscription tier placement, acceptable advertising, scope of distribution permitted, and security requirements. Content providers may negotiate terms to assure a uniform nationwide presentation and provide consumers with a consistent experience with their branded content. Content may be licensed to a distributor for in home distribution, but only a subset is licensed for out of home use. [6] One provider noted how its Mosaic service included licensed thumbnails, but use of the thumbnails came with license restrictions and application requirements. [18] Some satellite licenses require geolocation of the subscriber

account, or remote, IP-connected consumer device. Other satellite licenses forbid outputs to televisions that lack the HDCP protection required to enforce license restrictions on copy control and redistribution. [6] Licenses for VOD may require a network branded point of entry for the VOD library, rather than simply commingling that network's licensed content with other VOD. For "over the top" distribution, HBO has announced that it will initially exclusively launch on iOS (exclusivity is only for 90 days) and Cablevision; SlingTV includes ESPN; but ESPN has not yet licensed its content for Sony's new Internet television service, Vue. [15] Copyright and contract requirements all inform these different business models.

Programs are licensed to distributors (MVPDs and "over the top" video distributers). The distributors select and negotiate license rights from content providers and other rights holders (for example, licensors of program guide data), combine them with a variety of features (guides, on-demand, Start Over, look back, etc.), search tools, specialized applications, and cross-platform features like on-screen caller ID, and compile these into distinctive, branded offerings. [3][14][12][2]. Some WG members would prefer to separate programming from MVPD application features and create their own distinctive, branded offering on a competitive navigation device.

Over the top video distributors continue to emerge rapidly. Just since the commencement of DSTAC, Sony launched its PlayStation Vue Internet TV service and its licensed channel lineup; Apple is in negotiations with television networks to provide a TV-streaming service similar to DISH Network's Sling TV; and HBO announced the price for its new over-the-top service, to be launched exclusively on Apple devices.

Video providers use software and the delivery of an integrated service to protect against breaches of these licensing requirements. For example, the DISH guide is involved in the enforcement of varying entitlements to receive local channels, which vary depending on the location of the subscriber. DISH also uses its guide data to distinguish among program recordings that a subscriber may move to USB drive, and programming for which DISH does not have that license right. Charter's downloadable security system uses a network adapter similar to a Conditional Access Network Handler (CANH) Adaptor, HTML extensions, and its guide to enforce restrictions in carriage and retransmission consent agreements. AT&T uses a U-Verse application to manage which outputs are permitted from a set-top box depending on the rights licensed by content providers. [1] [2] [3] [6]

The FCC's former Encoding Rules put limits on how programming could be encoded for copy and output control in an effort to set consumer expectations with respect to various programming categories. The rules did not apply to distribution of any content over the Internet, via cable modem or DSL [28].

B. Chain of trust model that assures flow of content from content supplier to the distributor to the consumer

All video distributors operate within a complex system that creates a "chain of trust" from the content supplier to the distributor to the consumer with protections in place to respect the license restrictions on the content. For example, if content is licensed solely for display as an early release VOD title, there must be some protections in place so that the VOD title does not

flow out from an insecure platform or device to a pirate Internet site for unrestricted redistribution. The protections connect a variety of security regimes to one another through contracts and licensing.

The trust model includes:

- Specifying System on a Chip (SoC) and/or manufacturer-based provisioning methods, for example to include a hardware root of trust from which a variety of trust relations can be built.

- Specifying hardware requirements, SoC security firmware OS, software hardening measures, and digital certificates to provide assurance that the device in which the chip is placed is itself resistant to hacks.

- Securing integration of SoC/OS/SW into receivers

- Assuring that copy protection and use restrictions are carried through to receiver outputs – e.g., assuring that a device receiving content that is only permitted to be output for display does not make a recording; sends the content through an output with instructions that the downstream device may only display the content; and establishes a handshake with the downstream device that assures that the downstream device will respect that instruction. These copy and redistribution instructions vary and continue to evolve.

- Proactively detecting and disabling potential security threats; countering actual hacks and where possible prosecuting the perpetrators; and supplying on-going software upgrades in response to threats/hacks.

- Enabling and supporting renewability.

- Enforcing these trust conditions through device licenses (which create enforceable responsibilities), chip and device testing, affiliation agreements with enforceable restrictions, the chain of trust from content provider to the distributor, and assorted third-party beneficiary clauses providing content providers with rights of enforcement against downstream parties with whom they may have no direct contract relationship.

- In the case of DBS, pairing the SoC with a smartcard to enable a cryptographically secure communications with hardware roots of trust.

This trust model assures the flow of commercial content from content suppliers to the various distributors so that they may include them as part of the retail offering to consumers. [3] Devices must operate within this ecosystem in order to be part of the chain of trust. In the case of MVPD-provided client devices, the “chain of trust” is maintained by components that are all specified by the MVPD. However, in the case of delivery to third-party devices, the “chain of trust” is supported by a mixture of MVPD-provided support (CAS, window controls, downloaded app, etc.) and third-party components that meet the content rights, business

agreements and compliance and robustness necessary. In these cases, SW only (platform provided or downloaded) or SoC with commodity security support such as TEE and Secure Boot ROMs are used to provide the "chain of trust" to the end user.

The MovieLabs Specification for Next Generation Video and MovieLabs Specification for Enhanced Content Protection are examples of expected protections that major content providers have for securing high value content. [19] The Specification for Enhanced Content Protection requires, for example, a hardware root of trust, forensic watermarking, and corresponding video requirements for "4K" or Ultra High Definition programs. [3]

The trust model does not require uniformity in security techniques. In fact, diversity of approaches is a source of strength in security by reducing the target size and raising the costs to an attacker. For example, there can be multiple roots of trust, and there can be a variety of conditional access systems built from a common root of trust. [13] But there are consequences for devices that do not meet the expectations of content providers. Devices that do not expose a hardware root of trust to third parties will not receive the same third-party content as a device that does. [14]

Video providers use software and the delivery of an integrated service to trusted devices in order to protect against breaches of these chain of trust requirements.

Some members express the view that encoding rules and fair use should be considered a defense against content providers' attempts to limit access to content.

For CableCARD devices, security arrangements were extended from the CableCARD to third party retail navigation devices. A regulatory and licensing framework was put in place to define retail devices' handling of unidirectional cable linear programming. The DFAST technology license included compliance and robustness rules to secure content. The copy control information (CCI) provided a secure way to convey certain copy protection requirements from content agreements. Approved digital outputs allowed content, subject to the CCI settings, to be shared among other consumer devices that met security requirements. The Encoding Rules put limitations on what content owners could require. [22, 23, 28]

C. Privacy protections

Cable and satellite operators are required by statute to prevent unauthorized access to and release of subscriber information, such as the titles of programming viewed by an individual subscriber.

Cable and satellite providers use software and the delivery of an integrated service to trusted devices in order to protect against breaches of these privacy requirements. For example, Charter uses software to prevent a neighbor from seeing the VOD selection being streamed to a subscriber's home.

At present, some retail navigation devices have also adopted independent privacy policies. MVPD privacy policies and obligations may differ from the retailers' policies.

Cable and satellite providers believe that privacy protections should apply to all of their subscribers. Some members hold the position that a provider's obligations do not apply to retail devices.

D. Harm to service

Multichannel services are no longer simple broadcast videos that can be sent one-way to a cable-ready TV. Today, cable service is a complex interaction of licensed content, a variety of networks, different security and content protection measures, hardware, software, licensed metadata, diagnostics, application data synchronized with content, interactivity, user interfaces, advertising, ad reporting, audit paths, and more. [2][3][14] Even fundamentally one-way systems like DBS do more than simply broadcast video to a set-top box. Threats include harm to service, such as the failure to render service, the failure to support billing, and interference with advertising. One member does not consider interference with advertising to be harm to service.

DBS partitions the hard-drive of the provided set-top box and uses that partitioned drive to provide the set-top box with popular titles in advance of any customer order to deliver VOD. It uses the set-top box to render pay per view and the smartcard to record charges for pay-per-view which it reconciles when the set-top is next connected to a return path (e.g., Internet or telephone) or returned to the satellite provider for final billing. DBS also uses a collection of CPE to translate the "tune" from a remote control into a series of commands that decode the right frequencies (and the right orbital slots) for the tuned channels. [6]

FiOS uses the set-top box to merge two distinct networks – one in QAM and one in IP – into a single service. [9]

Cable renders closed captioning in the set-top box and outputs it through HDMI for display on a screen. (As discussed more fully below, when serving retail devices, it integrates the player into its app to provide captioning to the tablet or other customer owned device.) [18]

Many MVPDs use apps to provide voice control for the sight disabled, the subscriber's recent tuning history across devices, and other features. [2][14]

All MVPDs use software and integrated service to assure that services are delivered to consumers as advertised. They all render their services as an app to a predictable execution environment in the set-top box and in other client devices.

The use of applications is not limited to the video network side of multichannel plant. Cable systems typically offer residential multichannel video service, voice service, and broadband Internet access service. The cable industry is migrating towards unified edge QAMs in the headend to manage the QAM channels used in delivering all of these services. BrightHouse is an example of a cable operator that has rapidly advanced in the deployment of unified edge QAMs. BHN relies on interaction between the connected device and the unified edge QAM to allocate network resources among video, voice, data services. BHN has invested $[redacted] million in 2014 alone in unified edge QAMs that support video, VoIP and HSD services. End devices have to communicate with resource managers to allocate edge capacity on the QAM and that communications is done through application today. [7]

V. RAPID CHANGE IN SYSTEMS AND SERVICE

Multichannel service has evolved over time across all platforms. Cable evolved from analog to digital, then from digital to IP and cloud delivery. The original DigiCipher 2 moved from progressive refresh (I-macro-blocks instead of I-frames) to MPEG-2. Now video codecs are evolving from MPEG-2 to AVC to HEVC, as well as open source codecs such as VP-8 and VP-9. Audio codecs are evolving from MPEG Audio to AC-3 to MP3 to AACS to ATMOS, but any or all may still be in use. Satellite moved from proprietary transport protocol (DSS) to MPEG-2 then to MPEG-4. AT&T created U-Verse and Verizon created a hybrid QAM/IP service in FiOS.

The feature sets supported by an operator's application can include:

- Start Over and Look Back;
- Interactive applications within programming, such as DirectTV NFL Ticket/RedZone, Weather Channel, HSN Shop-by-Remote, and request for information ads
- Remote access to the DVR
- Recommendations, recent tuning history across devices; and personal profiles
- Social apps and widgets
- Online photos
- Audience measurement to optimize program mix
- Network DVR/Whole Home DVR
- Account management, such as self-serve upgrade to the subscription package from the guide
- Voice control
- On-screen caller ID and voicemail notifications
- On-screen voice to text playback
- Mosaic channels
- Multiviews
- What's trending
- Home control
- Home networking output with remote user interface (RUI)
- Cloud delivery to consumer-owned and managed devices, including iOS tablets and smartphones, Android tablets and smartphones, Blackberry, Kindle Fire, Xbox, Roku, PC, Mac, and Smart TVs

[2][3][14][18]

Changes in MPEG application and feature updates occurred over the course of years. IP application and feature updates are occurring multiple times a month (as consumers experience on their mobile phones). [14] The changes do not await agreement on a standard. Transport protocols for IP video have evolved from RTSP/UDP to various forms of Adaptive Bit Rate (ABR) protocols (HLS, HDS, DASH, etc.). These are still being debated. The same has happened with broadband access network technology (D1.0 to D1.1 to D2.0 to D3.0 to D3.1 or ISDN to DSL to ADSL to VDSL or BPON to GPON or IPv4 to IPv6. There is also a diversity of approaches to Ultra High Definition (UHD), with different studios currently in different places.

MVPDs test and use diverse solutions that can adapt to rapid changes in technology, competition, and consumer demand. As one operator put it, if they had waited for the evolution of a standard Mosaic, their Mosaic service would never have launched and consumers would have been denied the competitive choice. [18] Another operator offers instant channel change using a proprietary technology. [2] This diversity of approaches has produced innovation and competition. MVPDs have been able to enhance their networks over time to increase network capabilities, and have – within limits discussed in Part VII – been able to retire obsolete networking and broadcast technologies as necessary to achieve these enhancements. 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, and all providers innovate and compete, with consumers as the ultimate winners.

VI. APPLICATIONS MODEL

Just as the application model is used in delivering multichannel service to leased set-top boxes, it is in wide use by both CE manufacturers and video service providers as the most widespread method for delivering service, including some programming to customer owned devices.

Customer owned devices do not offer the same predictable execution environment that a multichannel provider relies upon in its leased set-top boxes. CE manufacturers do not build a single common platform for applications. Android, iOS, and HTML all differ from each other, and an Android app is not an iOS app and neither are HTML, although they may behave identically to an end-user. Likewise, the Microsoft Xbox, Nintendo Wii and Sony PlayStation platforms each have their own unique development environment, interface, streaming platform and encryption technology. Connected televisions use competing middleware. Panasonic is using Firefox OS. Sony, Sharp, and TP Vision are using Android TV. Vizio uses the Yahoo Connected TV Platform. Samsung just announced its new Tizen platform. LG uses webOS. Apple will use iOS. And all these systems frequently evolve and update their supported platforms.

The app model is in broad use in consumer electronics world as a means for abstracting the differences between varied and rapidly changing consumer electronics platforms and varied and rapidly changing services. The app model uses IP applications with software-downloadable DRMs or platform-supported DRMs that started with the PC Web browsers and now extends it to all the new consumer-owned mobile, game, TV and set-top devices above. [14] Video service providers use the same app model to serve a wide variety of rapidly changing customer owned devices while maintaining their protections against the various threats identified in Part IV, and the ability to change the service rapidly.

Netflix, Amazon and other “over the top” video distributers have to custom build and support many different versions of their apps for every different device, and each app must be individually coded, tested, improved, and maintained. Likewise some device manufacturers test against some of these applications with every software change and make accommodations such as licensing DRM software to support them. Multichannel providers follow the same model. Every one of the Top 10 multichannel video providers has built “apps” that deliver their services to millions of customer-owned IP-enabled devices, including iOS, Android, Mac/OS X,

PC/Windows, Xbox, Roku, Kindle, and a variety of Smart TVs. Not all services are available through these applications. Depending on the platform type and implementation these may or may not support a HW root of trust or SW root of trust and as a result there may or may not be limits on accessible content (such as high-resolution content) depending on the rights, business agreements and compliance and robustness rules of the protection being used. The content rights are defined through license agreement with content providers. They continue to grow in availability. TiVo notes that all cable linear services are available through CableCARD (when coupled with additional hardware or software to receive switched digital video).

Like Netflix and other "over the top" video providers, MVPDs must write separate apps to the different platforms, and some device manufacturers must work with Netflix and the MVPDs to support the apps. Tablets and many other popular customer-owned devices include multiple apps from multiple video providers. The device presents its own interface, environment and user experience, along with a selection of available applications. The device operates as a retail "mall" in which many different video providers can operate as retail stores presenting their own brands and experiences. The different video providers all appear as selectable app icons on the native interface of the device. Each video provider's app uses a downloadable software-based DRM for content security. The DRM used can be the DRM packaged with the device or one included in the video-provider's app download. The consumer selects each app, and enters the retail experience of each provider. Once clicked, the user interface on the consumer device presents the retail experience in a way that respects the content license restrictions and chain of trust under which video services are offered. It does not provide for the presentation of the product within a third-party UI or a different service.

The WG viewed a demonstration of the TWC TV application appearing on a Samsung TV navigation ribbon, and then launching by click to display the TWC guide and services on the Samsung TV. The app is programmed to honor the provider's licensing rules and to accommodate updates as service features change. [5][9][12][13][14] In some cases the provider embeds the video player into the app to assure that the IP device includes closed captioning and has the right codec(s) as they evolve (MPEG AVC, MPEGS HEVC, DASH, VC8, etc.) [6][18]

There have been millions of downloads of MVPD apps and millions of unique users. [7][12] Table 2 quantifies the number of mobile downloads for IP devices and TV Everywhere applications.

Mobile App	Android	iPhone	iPad	Total
DirecTV	10,000,000	6,100,000	2,700,000	18,800,000
Xfinity TV Go	5,100,000	2,300,000	1,400,000	8,800,000
DISH Anywhere	5,200,000	1,800,000	1,700,000	8,700,000
AT&T U-Verse	2,200,000	2,400,000	1,600	4,601,600
TWC TV	2,300,000	882,000	788,000	3,970,000
Verizon FiOS Mobile	1,200,000	756,000	729,000	2,685,000
Cablevision Optimum	508,000	617,000	607,000	1,732,000
Charter TV	510,000	147,000	89,000	746,000
Bright House TV	268,000	256,000	184,000	708,000
Cox TV Connect	146,000	80,000	366,000	592,000
Google Fiber TV	194,000	19,000	8,800	221,800
Total	27,626,000	15,357,000	8,573,400	51,556,400

Table 2 - Estimated Downloads of MVPD Mobile TV Apps

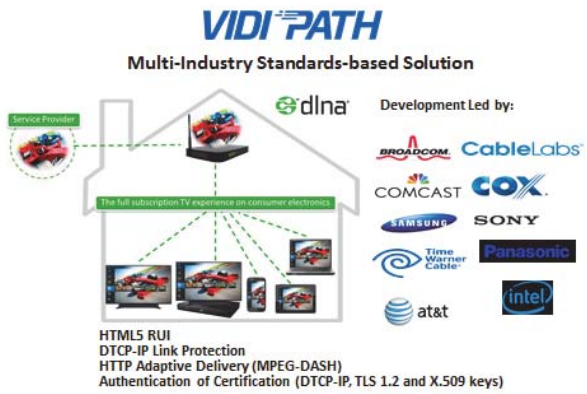
Source: http://xyo.net (accessed 2/6/15)

These are currently the best examples of applications-based support for consumer devices that can move among different video providers. Not every video source is yet ported to every platform, but across the industry, the platforms supported are increasing in response to consumer demand.

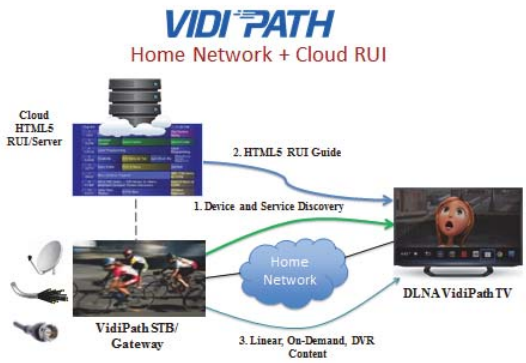
Some members did not agree with the MVPD's conclusions that these are the best examples of getting MVPD service on to consumer devices. The working group was also shown presentations on current retail CableCARD devices from TiVo and Hauppauge that offer consumers another alternative. In the CableCARD environment, the consumer uses a third party user interface instead of the cable operator's user interface. In addition when the device provider had a business deal with OTT application providers the consumer could use the third party device to search across all services to select content for viewing instead of each application separately. Consumers were also able to use the OTT provider's service application to select content from the OTT provider's user interface. Most WG members consider the cable operator's user interface to be features of the cable operator's service. Manufacturers of retail CableCARD devices do not treat the cable operator's user interface as part of the service.

VidiPath and RVU are additional approaches that have limited deployments and are expected to grow. [8][12] VidiPath and RVU are industry standards that enable a RUI (Remote User Interface) to be displayed on connected consumer electronics devices in the home. In VidiPath these screens are defined using an HTML5 application, while RVU employs server and client elements and the HTML-5 Canvas layer. These approaches abstract the diversity and complexity of service providers and customer-owned IP and QAM devices, accommodate rapid change and innovation by both service providers and consumer electronics manufacturers, and make use of a combination of software-downloadable security with hardware roots of trust.

VidiPath was developed in the multi-industry DLNA through development work by major CE manufacturers (including Samsung, Panasonic, and Sony); major chip manufacturers (Intel & Broadcom) and major MVPDs (including Comcast, TWC, AT&T, and DISH). VidiPath uses HTML5 with W3C extensions to deliver multichannel service via app to a client device and provides a different way to load apps on the client than the traditional Apple or Android apps store. The WG viewed a demonstration of a beta Comcast application using DLNA VidiPath to connect to a Samsung TV. Current implementations are through an IP output from a set-top box, but VidiPath also supports "cloud-to-ground" delivery directly from a network to the client. [3]

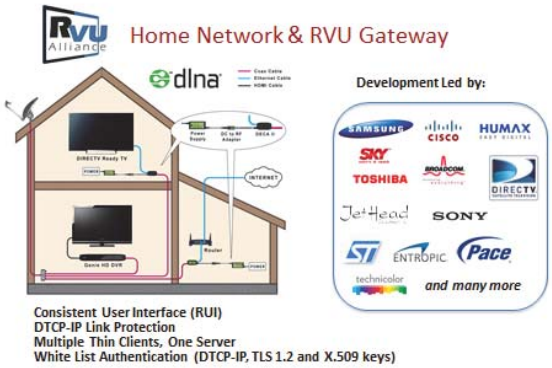


(1B) Example: Technology Survey – DLNA VidiPath



(1B) Example: Technology Survey – DLNA VidiPath

RVU was developed through the multi-industry RVU Alliance and incorporated into DLNA. It also delivers services via apps to RVU TVs, also known as "DirecTV ready TV." [8]



(1B) Example: Technology Survey – DLNA RVU

(1B) Example: Technology Survey – DLNA RVU

Both VidiPath and RVU present a remote user interface (RUI), providing the consumer with an experience similar to the tablet example above. A DLNA VidiPath output flows content control bits (CCI) and standard video formats through to the client device to provide for recordability of a program (e.g., a linear cable network like ESPN marked "copy one generation" is accessible on the DTCP-IP output).

Currently VidiPath and RVU require use of the provider's RUI to receive the provider's service.

It was noted that DLNA CVP-1 defines protocols for listing and retrieving recorded DVR content without the use of the operator's application. However, Vidipath was developed to provide access to MVPD service via the MVPD's application only, including features not supported by DLNA protocols (such as EAS) and to other aspects of an MVPD's service as it continues to evolve.

TiVo presented to the WG that an alternative to writing different applications from different MVPDs and OTT services across variations in platforms in a retail environment is to use standard protocols on interfaces between devices instead, and allow a third party application

to access the content. Internet Web services such as email, web browsing and chat are based on protocols, defining the communication interface between networked devices. The protocols are independent of the operating system and programming language used in the components and allow flexibility in implementation. For example the CableCARD interface defines a hardware interface and protocol for accessing content that is independent of cable operator CAS system or DRM, and agnostic to operating system or software environment. MVPDs assert that MVPD services are more diverse, complex and change more rapidly than fixed protocols permit. TiVo asserts that the current application environment is analogous to prior middleware environments like tru2way that defined a specific programming language and execution environment for MVPD applications. MVPDs assert that the current application approach provides applications written to multiple different target platforms, rather than requiring common middleware, which was the tru2way approach.

Multichannel providers also offer a variety of "Everywhere" and "Anywhere" applications for use with browsers, Mac/OS X, and PC/Windows. The precise offerings are dependent on negotiated rights with the content owners. A small sample of the offerings are shown in Table 3. [6]

Exhibit 5 – TVE Authentication Availability for Top 15 Networks among Top 15 MVPDs

TVE Authentication Availability for Top 15 Networks among Top 15 MVPDs*

	ABC (bdcast)	FOX (bdcast)	USA (#1 cable net)	ESPN (#2)	Disney Ch. (#3)	TBS (#4)	Fox News (#5)	History (#6)	TNT (#7)	A&E (#8)	F/X (#9)	ABC Family (#10)	HBO	Show-time	Starz
Comcast	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
DirecTV			●			●	●	●	●	●			●	●	●
DISH	●	●	●	●	●	●		●	●	●		●	●		●
Time Warner Cable		●		●			●	●		●	●		●	●	●
AT&T	●	●	●	●	●	●	●		●		●	●	●	●	●
Verizon	●	●	●	●	●	●	●	●	●	●		●	●	●	●
Cox	●	●	●	●	●	●			●		●	●	●	●	●
Charter	●		●	●	●	●			●			●	●	●	
Cablevision	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Bright House		●		●			●	●		●	●		●	●	●
Suddenlink		●	●	●	●	●	●	●	●	●	●	●	●		●
Mediacom		●	●	●	●	●	●		●		●	●	●	●	●
Wide Open West		●	●	●		●	●	●	●	●	●		●	●	
Cable One		●		●		●	●		●		●		●		
RCN		●	●	●		●	●	●	●	●			●	●	

© 2014 TDG Research *Survey conducted October 2014 - CBS and NBC broadcast networks do not require authentication for next day full episodes

Table 3 – TVE Authentication Availability for Top 15 Networks Among Top 15 MVPDs

Content providers also provide content directly to authenticated subscribers via their own apps and license content to subscription "over the top" video providers. Authenticated offerings

include: ABC, CBS, NBC, Fox, USA, Watch ESPN, Disney, HBO GO, TBS, Fox Sports GO, History, TNT, A&E, Showtime, and Starz. "Over the top" subscription video providers include Netflix, Amazon Prime, Hulu Plus, Sling TV, Sony Vue, Xbox Live, Nintendo Network, and Playstation Network. "Over the top" ad supported video providers include YouTube and Hulu.

Market shares as of 3Q 2014 are shown in Table 4.

	3Q 14
Netflix	36,265,000
Amazon Prime	20,800,000
Hulu Plus	7,000,000
All Others	1,207,000

Table 4 – Market Shares of OTT Video Service Providers [6]

The applications approach abstracts the diversity and complexity of service providers and customer-owned devices, and allows rapid updates and rapid innovation by service providers and device manufacturers. It does not require long timeframes for standardization of APIs for each new feature, which is difficult given the variety and pace of change among video providers, technologies, services and features. The provider simply updates the app and the feature set becomes available through the app. Apps also reduce the burden on CE to map to multiple network technologies and CAS trust infrastructures. The approach has been developed through responses to consumer behavior and preferences found in the marketplace for devices.

VII. CABLECARD

A. Current Deployments

CableCARDs are deployed by all major cable operators in over 50 million of their leased devices, as well as in just under 620,000 retail navigation devices (served by the nine largest cable operators). CableCARDs and the FCC's "UDCP" rules were originally designed for retail UDCPs that receive one-way linear cable services, but not services that required interactivity, such as VOD and interactive program guides. Cable operators were later required to use CableCARDs in most of their fully featured set-top boxes, and have designed those leased set-top boxes to present their full service offering in set-tops with CableCARDs by tightly integrating the experience into an interactive app. For some providers, that app runs on a particular middleware. UDCPs are not utilizing that app or that middleware. Through bilateral negotiated agreements between the cable operator and the CableCARD device manufacturer, like the one between TiVo and several cable operators, the TiVo "one-way" CableCARD device has access to two-way cable services such as VOD, PPV, CallerID, Switched Digital Video, Catchup, StartOver and more.

CableCARDs are not required or used by current major video distributors like DISH, DIRECTV, AT&T, or over-the-top providers. However "Section 629 subjects all MVPDs to its requirements, including cable operators, DBS providers, multichannel multipoint distribution service operators and satellite master antenna television providers" [28]

No television manufacturers currently use CableCARD. CableCARDs are also not used by mobile devices, for direct delivery to PCs, by game platforms or by most retail set-top boxes, such as Amazon Fire TV, Apple TV, Chromecast, and Roku. Devices that use CableCARDs have never been portable across all technologies, platforms, or services.

CableCARD is the only technology that, across all cable systems, allows products sourced independently from the cable operator to receive in the home's primary viewing area, and record (if marked eligible for recording), all of the operator's streamed content. MVPDs also provide service to customer-owned devices using applications. Some of these provide full service (including cloud recording) to PCs, tablets and mobile phones. In addition, DLNA VidiPath provides for recordability of video streams (if marked eligible for recording) on those outputs protected by DTCP-IP.

FCC rules for CableCARD-reliant retail devices provide that unidirectional digital cable products do not by default get access to interactive two-way digital television products. Under business-to-business agreements, some retail CableCARD devices may include Video On Demand ("VOD") and other two-way service, as well as OTT video and audio service providers. Through bilateral negotiated agreements between the cable operator and the CableCARD device manufacturer, like the one between TiVo and several cable operators, the TiVo "one-way" CableCARD device has access to two-way cable services such as VOD, PPV, CallerID, Switched Digital Video, Catchup, and StartOver. [23].

Cable operators seek to present the consumer with the full and expected cable experience as advertised, ensure the features (including captioning, EAS, and other regulatory requirements) run properly, and have the ability to enhance the service as technology, features, and consumer demands change.

B. CableCARD as Means for Accessing Programming Signals

A decade ago, the technology for CableCARD-enabled UDCPs required device manufacturers to create their own guides, rather than downloading the MVPD's full service. However, the one-way MOU creating the framework for UDCPs committed cable operators and CE manufacturers to work together to create a two-way solution using OCAP or its successor technology in advanced (interactive) retail devices, in order to render the full cable experience. [FCC 03-3 contains the commitment, at 18 FCC Rcd 518, 548, http://telecomlaw.bna.com/terc/core_adp/get_object/FCCRCD18-518.pdf .] Technology has since advanced to support the full cable UI through apps for navigating and presenting services.

Some members consider CableCARD to be a model for separating navigation from access to programming signals, and for providing an equipment manufacturer with the opportunity to provide an alternative user interface and features for use with that programming.

The working group was also shown presentations on current retail CableCARD devices from TiVo and Hauppauge that provide consumers an alternative user interface supplied by the equipment manufacturer, instead of the cable operator's navigation and user interface. In the case of TiVo, TiVo has made business-to-business agreements with other non-cable video providers, so that users could use the TiVo user interface across all of the services.

C. Impact of CableCARD on Innovation

Some members stated that CableCARD has supported innovation by cable operators. The presence of CableCARD has enabled TiVo Series 3+, SiliconDust and Hauppauge devices, but most others members believe that CableCARD has impeded innovation by cable operators and FiOS. The requirement to use CableCARDs in leased devices delayed cable operators' ability to use the DTAs essential for their transition to all-digital. The need to create a custom solution for UDCPs delayed cable's use of switched digital video to expand channel capacity. Verizon was required to bolt on a redundant method for delivering entitlements to UDCPs using CableCARDs – using a slower carousel approach for which CableCARDs were designed rather than the instant entitlement designed for FiOS. Verizon also had to add additional EAS and OOB signaling just to address UDCPs using CableCARDs. FiOS IP services do not pass through the CableCARD. The CableCARDs limitation to 1995's MPEG-2 Transport Streams is incompatible with modern video delivery formats (e.g. ISO Base Media File Format) used by competing video providers. [9] Innovation has occurred "in spite of" CableCARD, but at high cost. [9] Most working group members conclude from their experience with CableCARD that we should not repeat such technology lock-ins, given today's pace of change.

Retail CableCARD devices, and new manufacturers of leased STB equipment made possible by CableCARD and sold directly to cable operators, introduced many new features that some members believe benefited both consumers and cable operators. Hauppauge demonstrated how a user could view the unidirectional, live linear cable channel lineup on a PC with its own grid guide. TiVo demonstrated a single user experience that integrated Cable Service, Netflix Service, Amazon Service, and other OTT video services. The user has a choice of launching the OTT Application separately, or watching content from within the TiVo user experience instead. CableCARD-enabled retail navigation devices are not required to offer users the option of using the cable operator's guide.

VIII. COMMON MIDDLEWARE APPROACH

A common middleware is another approach for serving diverse devices without attempting to create thousands of ever changing APIs. In the 2000s, using common middleware between a variety of hardware platforms and write-once-run-anywhere applications was part of an international trend, and provided a path for delivering rapidly changing services.

Many cable operators implemented the Java-based "tru2way" as a common middleware to abstract the differences in native hardware. Panasonic launched a retail tru2way TV in 2008, but soon withdrew it from market. [20] Several major CE manufacturers committed to tru2way in a cross-industry 2008 Memorandum of Understanding, but they did not bring tru2way products to market. [3] OCAP, MHP, and tru2way which were all based on DVB Globally Executable MHP (GEM).

Even tru2way would not necessarily work with other platforms. FiOS lacks the RF upstream assumed by tru2way, and the satellite signal path lacks any upstream. [5][9]

RDK is another middleware approach. The reference design kit (RDK) is an integrated software bundle that can be utilized as a software stack for QAM, IP and Hybrid set-tops,

gateways, video clients and customer-owned equipment. The RDK platform has helped to speed innovation by reducing development cycles and time to deployment. For example, over the last 4 years the only RDK adopter to deploy in the US claimed that it reduced the time for deployment of innovative features by 30 months, enabling it to deploy new features rapidly after conception. Among recent features rapidly deployed on the one RDK deployment are Kids View guide views, personalized browsing, increased search speed, voice remote, and a Spanish menu. At most recent count, 235 companies, including set-top and chipmakers, system integrators, software vendors and cable operators, have signed RDK licenses since the project debuted in early 2012. Comcast as the only US operator to deploy RDK has deployed RDK based devices to more than 5 million homes. Time Warner Cable has announced its intention to use the RDK as the platform for next generation CPE. [16][17]

IX. IMPACT OF CHANGING CAS

A service provider's choice of CAS must accommodate millions of legacy devices currently in the homes of existing customers.

For example, even when cable systems are sold to a new owner that uses a different CAS, the system stays with the original CAS. [10]

Charter's construction of a downloadable CAS (for its QAM network) illustrates the scale of the undertaking to change CAS. It was building a CAS system that could continue to support two existing CAS systems (Cisco's PowerKey and ARRIS's MediaCipher) plus a new CAS from NDS, all in the same box. This is the first time this has been achieved for cable operators that were built with multiple legacy CAS systems. In order not to strand its existing client base, it rebuilt its entire network and all QAMs. [1].

X. CHARTER AND CABLEVISION "DOWNLOADABLE" IMPLEMENTATIONS

Open Media Security (OMS) is currently deployed by Cablevision and has been tested on live plant by Charter as it prepares for commercial launch. The CAS system is based on a standardized key ladder (K-LAD) given to many chip manufacturers (currently four+ manufacturers and several dozen chip families), activated at time of manufacture with a secret key to satisfy content providers' requirements for a hardware root of trust. The network can talk to the downloadable CAS client to build a trust relationship with the device when it connects to a network. The K-LAD authenticates these two-way transactions to provide a very secure CAS solution without the need for a dedicated security processor. Use of OMS with additional requirements listed below could allow a retail set-top box to be portable across the Charter and Cablevision footprint. [1][13] The currently deployed Cablevision leased set-top using OMS was not specifically designed to be portable to other cable systems, but it will work on the Charter systems that use legacy Cisco CAS. Charter's leased set-top box was designed to be ported between ARRIS and Cisco footprints.

Using a fully defined model, retail devices do not need to have different chips or device software for each video provider. Today Charter and Cablevision operate using different chips that could theoretically interoperate. It is common for chip manufacturers to include other security elements for other regimes in commodity chips. Different security systems can also be

built from the same root of trust in a chip, or from separate roots of trust if the security vendors agree. Next generation DRMs can use the OMS challenge-response process to build a hardware-based trust relationship with an OMS compliant device.

As currently implemented, OMS is designed for QAM and interactivity and, according to an OMS adopter, is not a good fit for one-way satellite devices. [13]

If OMS were to be adopted for retail devices that were portable across all MVPDs, other elements beyond OMS must be defined, including:

- every MVPD would need to support the OMS profiles adopted for retail devices;
- every participating downloadable conditional access software vendor would need to support a single trust authority or federated system of trust authorities working in concert with chip manufacturers;
- participants would need to develop and support specifications defining how the downloadable elements are identified, securely delivered and hosted;
- a common set of ciphers would be agreed upon. OMS currently supports a set of license-free industry standard ciphers – the Advanced Encryption Standard (AES), Triple Data Encryption Standard (3DES) and the Common Scrambling Algorithm (CSA), and a defined set of emerging ciphers (AES, etc.). However many US Cable plants today use a proprietary cipher that requires a license;
- CAS-specific APIs would need to be made common between the retail device application and the OMS software.

XI. OVER THE TOP (OTT) VIDEO DISTRIBUTION AND THE IP VIDEO TRANSITION

A. Sling TV [25]

Sling TV is an example of a subscription over-the-top video service that includes streaming linear video content. The service uses multiple data centers, distribution centers and CDNs for distribution to subscribers, who can access the service using a variety of ISP distribution methods (fiber, cable modems, DSL, LTE, and Wi-Fi) to IP-enabled devices.

Unlike traditional MVPDs that can determine the CAS system they wish to use, Sling TV and other over-the-top video services make use of multiple DRMs in order to support the variety of DRMs on consumer-owned devices and/or required by content providers for specific content. Sling TV uses five DRMs. The approval of content providers (studio and networks) is obtained for the use of DRMs. Content providers may require audits of the technology (and sometimes of supporting facilities), to be conducted by third-parties such as Merdan.

Common requirements for an all-software, open platform CA/DRM serving customer-owned devices are:

- Content encryption for broadcast and VOD
- Device registration
- Device authentication and clone detection
- Secure offline playback (for mobile devices), with entitlement delivery (for example, to restrict playback of a program for which there is no out-of-home playback rights)
- Platform dependent robustness, including a hardware root of trust, tamper detection, white-box cryptography including code obfuscation, and detecting jailbreak status in an iOS or Android device.

Common requirements for a CA/DRM in set-top boxes are:

- Secure boot (hardware root of trust)
- SoC unique keys
- Protected DRAM
- HDCP output protection
- Code signing, secure boot, and secure software download
- DRM client embedded in client platform code
- Video quality-related protection guidelines, such as MovieLabs Specification [19] for 4K content.

Diversity (such as different random binaries in white-box cryptography) can provide additional security; but there is always a tradeoff and balance between the cost (in complexity of management) of a solution and its benefits.

Almost all content providers allow SD content to be delivered to tablets and mobile phones. For HD content, content providers insist on a trusted video path and processing on CPUs with security support. For example, a Trusted Execution Environment (TEE), such as ARM TrustZone, isolates trusted code that executes in the trusted execution environment from application code that is executed in a general processor, based upon the known characteristics of the device. ARM-based chips, as well as chips from Broadcom, MediaTek and Intel all provide alternative implementations of a trusted execution environment for isolating secure software execution. Global Platform reportedly is trying to develop a standard interface to the various trusted execution environments. TrustZone and Global Platform are intended for use with multiple DRMs. In addition, some but not all studios are said to insist upon the protections in MovieLabs Specification for 4K content.

The system downloads an app on request to mobile devices based on the entitlement of the mobile device and a unique identifier created by the system. The content is then packaged with a media player or for use with a native media player on the device. Output control varies by device. Unlike set-top boxes, where certificates and keys may be installed at the factory, mobile devices are addressed after-the-fact based on the credential of the device. Although this is not as secure as factory installed elements, there are other tools of protection (such as how long content

is authorized, more clone detection, differences in resolution and other tools of active DRM management) that can bring protection close enough that most content providers will make the business decision to tolerate the risk and allow content to be delivered to mobile devices as well.

Entitlements are managed in accordance with content rights. For example, if a content provider has broadcast rights that they are able to license to distributors, but not the rights to license streaming over the Internet, Sling Television sends a blackout message to the device. Content providers may also only authorize full resolution using certain DRMs, so Sling Television needs to switch the DRM in use as the content source switches.

Other features built into the Sling TV service are analytics for accountability to content providers; dynamic ad insertion (DAI); and ratings. Sling TV also supports billing and taxation for the approximately 1,000 jurisdictions that assess fees on the service.

Expected requirements for downloadable security that protects the highest value content would include:

- Hardware root of trust
- Secure boot
- Signed platform code
- Trusted execution environment
- Protected video path
- Diverse download mechanisms for diverse clients

B. Amazon Instant Video [26]

Amazon Instant Video is an example of an over-the-top video-on-demand service that is delivered in a manner similar to Sling TV.

It delivers video using multiple DRMs, such as those included in HTML 5 EME, Ultraviolet or other multi-DRM solutions.

The receiver device must meet robustness rules, such as those adopted by Playready or Widevine, and output controls.

The content is protected in the device with hardware-enforced security, including device-specific identity for device-specific keying and encrypted license storage and policy execution. Manufacturing includes SoC fused protection of provisioning secrets. Service is provided through an application. Playback is assumed to be taking place in a hostile environment; so software-driven playback is driven through execution in a trusted environment. The application is updated through signed code and secure software download.

C. Cable's IP Video Transition [27]

In the cable industry's transition from analog to digital (MPEG), the presence of analog receiving devices in subscriber homes required a lengthy transition period beginning in 1996

which included the continued network carriage of analog signals and for some period of time duplicate transmission of signals in both analog and digital form, also known as simulcasting. This constrained the network capacity available for high-speed data and digital video services. Some cable operators have made the final transition to 100% all-digital (no analog simulcast) service, while others remain in transition with some amount of simulcast analog channels remaining.

There are some similarities to the analog to digital transition in the current transition from digital (MPEG) to IP, with cable operators carrying some services as MPEG-only, some services as IP-only, and some duplicated or simulcast in both. The presence of MPEG-only receiving devices in subscriber homes will also require a lengthy transition period. An all-IP fiber access network could be more simply and efficiently designed as pure EPON or GPON networks, but to accommodate existing devices in subscriber homes that receive MPEG over QAM, cable operators have deployed FTTP networks using RF over Glass (RFoG), which replicates the full spectrum of MPEG channels at substantial additional cost. There are also differences between the analog to digital and MPEG to IP transition. The analog to digital transition continued to confine the service to home reception; the IP transition enables reception anywhere via mobile devices. Digital cable still uses cable-specific CAS for content protection, and has extended it through hardware-based CableCARDs; with the IP transition, the cable industry is using the software-downloadable DRMs that started with consumer devices and are now moving into set-top boxes. The analog to digital transition still uses cable-specific specifications; with the IP transition, the cable industry is moving to worldwide standards (MPEG-4 AVC, MPEG-H HEVC, MPEG DASH, W3C EME), as have video providers like Amazon, Netflix, Hulu Plus, and others.

Vidipath supports both MPEG video and IP video, enabling service providers to transition from MPEG to IP over time by updating the application and enabling Vidipath client devices to move from MPEG to IP by using the updated application. There may be other designs that can accommodate the IP transition.

Certain cable operators have deployed all-IP networks on college campuses that do not utilize set-top boxes. Live linear, premium channels, and VOD are delivered to consumer-owned devices (e.g. tablets, phones, laptops) that can be used anywhere, rather than just in the home (or dorm). The service can be coupled with cloud DVR service. This all-IP service is packaged as an app and uses DRMs for content protection.

Like an Amazon device (such as Fire TV), cable IP set-top boxes present their user-interface via an application; use Internet DRMs with hardware roots of trust; comply with robustness rules; support output protection; and use secure code download.

XII. SUMMARY OF MVPD CAS AND DRM TRUST INFRASTRUCTURES [29]

MVPDs have traditionally used CAS as the security system for the video content they distribute to their subscribers via the set-tops they provide. DRM systems were originally adopted by Over the Top (OTT) video providers and more recently by MVPDs to deliver video content to retail devices. In some instances OTT providers will also supply a device to support their service. While the trust infrastructures for CAS and DRM systems have similarities, they

also have significant differences based upon a different number of parties involved and different types of relationships among them.

A. Example MVPD CAS Trust Infrastructure

Figure 1 is an example diagram of an MVPD CAS trust infrastructure. It is intended to show many of the relationships, whether they are through license, contract, transfer of security data, or transfer of hardware/software. This is just an example of a trust infrastructure. Each implementation in a deployed system is likely to be different. Further, multiple functions can be performed or provided by the same organization depending on the implementation. For example, the set-top box manufacturer could also be the CAS provider or the CAS provider could choose not to outsource the black box function. In addition, this diagram doesn't show numerous other relationships in the ecosystem, for example, one set-top box vendor licensing their technology to a second source supplier, or an MVPD contracting with a contract manufacturer to produce set-top boxes or set-top application providers licensing their IPR to other application developers.

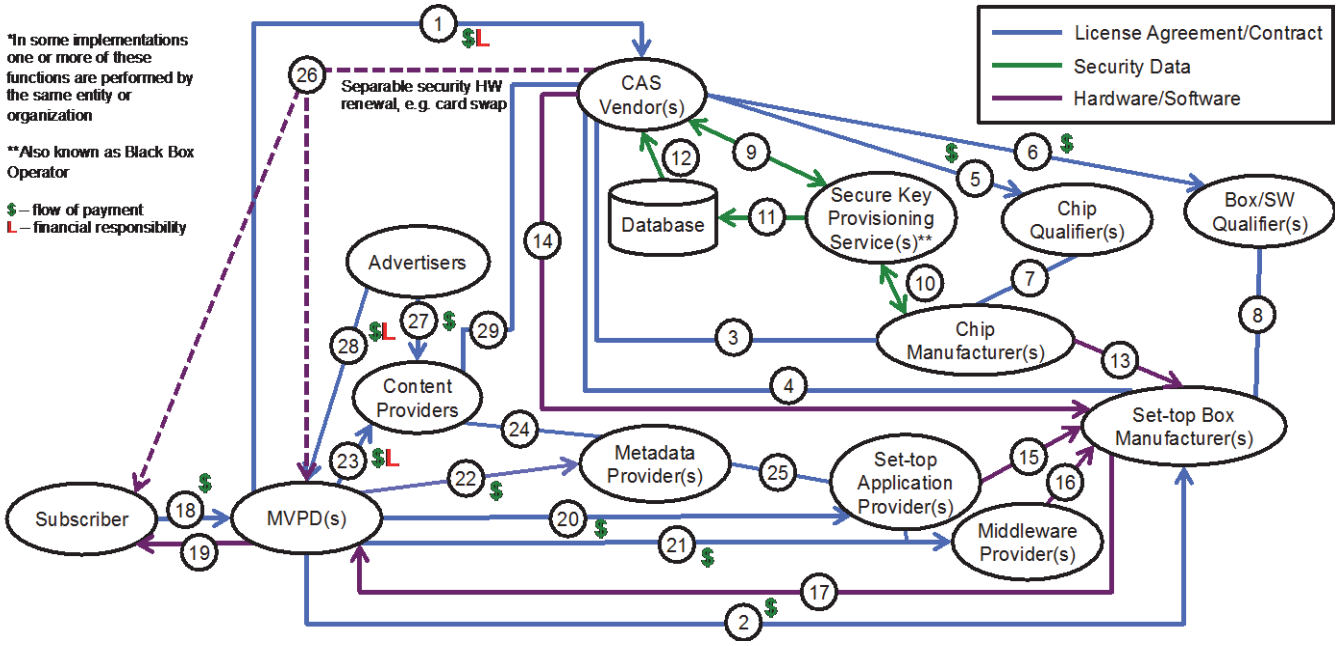


Figure 1 - Example MVPD Trust Infrastructure

For purposes of illustration, Figure 1 is not intended to be exhaustive or complete, but simply representative of the typical relationships that are involved in the MVPD trust infrastructure.

An MVPD licenses content from multiple content providers to create an aggregate retail service (23). These content licenses include terms that cover breach resolution, liability, warranty, as well as geographic, differentiated device, differentiated output, differentiated resolutions, and potentially other restrictions. In addition the MVPD agreements with the content providers include advertising opportunities (avails) to sell local advertising. In general,

the MVPD incurs a financial responsibility for compromises that result in theft of content. Content Providers may include language regarding specific security systems and platforms in their content agreements.

The MVPD also contracts with multiple parties to implement a complete solution including: CAS vendors, set-top box manufacturers, set-top box application providers, and set-top box middleware providers (1, 2, 20, 21, 22). These include breach resolution, warranty, and indemnification against IPR infringement, service level agreement (SLA), and other terms that are frequently derived from content licenses. A number of other relationships cascade from these licenses.

The CAS vendor will disclose details of its security solutions content providers under NDA to demonstrate the solutions' robustness (29). The CAS vendor may license IPR, such as custom logic blocks that have roots of trust, key ladders, and some recovery/countermeasure logic, to a chip vendor for use in their SoC (3) to provide differentiated capabilities in support of the CAS system requirements. They may also license IPR to a set-top box manufacturer for requirements that are not fully captured in the SoC (4). The CAS vendor may also contract with chip and set-top box/software qualifiers (5, 6) to validate designs for robustness. The chip vendor and set-top box manufacturer will have agreements with the chip and set-top box/software qualifiers respectively to enable them to perform this validation (7, 8). The CAS vendor and Secure Key Provisioning Service (also known as Black Box Operator) may exchange security data (keys and identifiers), which is stored in a secure database (9, 11, 12). The secure key provisioning service will inject security data into the SoC and set-top box at the time of manufacture (10). The chip vendor sells appropriate SoCs to the set-top box vendor (13). The CAS vendor may provide a separable security element, e.g. SmartCard to the set-top box vendor (14). In instances of system breach, one form of breach resolution is the issuance of new separable security elements, e.g. SmartCard sent either to the MVPD or to the subscriber directly (26).

The MVPD will also contract with set-top box application providers, set-top box middleware providers, and metadata providers to develop the set-top box application and supply it with content metadata (20, 21, 22). The content provider licenses content metadata to multiple metadata providers (24) and the metadata provider licenses aggregate metadata to the set-top application provider (25). The set-top box application provider and set-top box middleware provider will deliver their software to the set-top box vendor for integration (15, 16). The application implements portions of the overall service security. The set-top box manufacturer sells set-tops to the MVPD in accordance with their contract with the MVPD (17).

Advertisers contract with content providers and MVPDs to carry advertising specific to programming, time slot and geographic distribution and audit them for to validate their performance (27, 28).

When a subscriber signs up for service the MVPD executes an agreement with the subscriber specifying services provided, the subscription fee, and acceptable use policies (18). The MVPD then provides, installs, and provisions the set-top box at the subscribers' premises (19).

Not shown in this diagram are third-party piracy-monitoring services that may be retained by CAS vendors, MVPDs, or content providers to notify them of instances of pirated content, which

they can use to activate their own breach detection and response activities, or into joint action in some cases. Downloadable Conditional Access System (DCAS) architectures add another layer of trust hierarchy (an independent Trust Authority or federation of Trust Authorities above the individual CAS systems) to this diagram.

B. Example DRM Trust Infrastructure

Figure 2 is an example diagram of a DRM trust infrastructure. It is intended to show many of the various relationships, whether they are through license, contract, transfer of security data, or transfer of hardware/software. This is just an example of a trust infrastructure. Each implementation in a deployed system is likely to be different. Further, multiple functions can be performed or provided by the same organization depending on the implementation. For example, the DRM Vendor could also develop the Web Browser player plug-in or the DRM vendor could choose not to outsource the chip qualification function.

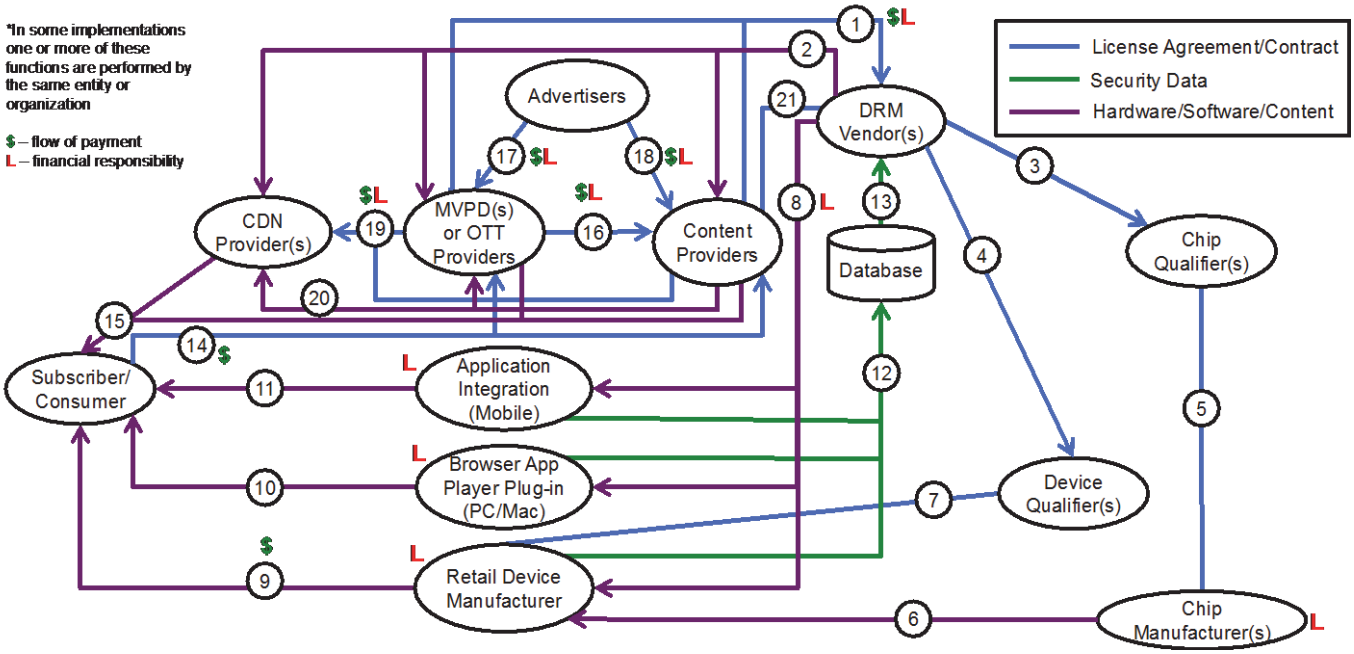


Figure 2 - Example DRM Trust Infrastructure

For purposes of illustration, Figure 2 is not intended to be exhaustive or complete, but simply representative of the typical relationships that are involved in the DRM trust infrastructure.

The MVPD, OTT Provider, or Content Provider will contract with one or more DRM vendors to provide a content protection solution for their network, including breach resolution, warranty, and indemnification against IPR infringement, SLA, and other terms that are frequently derived from content licenses (1).

As in the case of the MVPD CAS trust infrastructure, a number of other relationships cascade from these licenses. The DRM vendor may contract with a third-party chip and device/software qualifier to validate robustness against attack (3, 4). The chip vendor and device manufacturer

will have agreements with the chip and device/software qualifiers respectively to enable them to perform this validation (5, 7). The chip vendor sells appropriate SoCs to the device manufacture (6). The DRM vendor supplies a DRM client together with robustness and compliance requirements to application developers to integrate the DRM into their application, browser app player plug-in developers to integrate into the player plug-in, and retail device manufacturers to integrate into their retail device (8). The DRM client implementations report security data to the DRM database personalizing the specific instance of the DRM client to the specific device on which it is installed (12). The DRM vendor extracts security data from the secure database for purposes of provisioning and management of the DRM clients (13). The DRM vendor supplies a DRM license server to the CDN Provider, MVPD, OTT Provider, or Content Provider for use in protecting the content they deliver. The license server provides the content license, which includes the rights conveyed to the subscriber and the keys necessary to decrypt the content (2). As in the case of the MVPD CAS trust infrastructure, content providers will review DRM vendors' security solutions under NDA to understand the robustness of the implementation (21).

The MVPD, or OTT Provider licenses content from multiple content providers under terms that include breach resolution, liability, warranty, as well as geographic, differentiated device, differentiated output, differentiated resolutions, and potentially other restrictions (16). The consumer/subscriber purchases content from the MVPD, OTT Provider, or Content Provider, either on a subscription or transactional basis (14).

Advertisers contract with content providers, OTT Providers, and MVPDs to carry advertising specific to programming, time slot and geographic distribution and audit them for to validate their performance (17, 18).

MVPDs, OTT Providers, or Content Providers may contract with CDN Providers for content distribution and optionally DRM management services and provide content to the CDN provider for distribution and optionally DRM management services (19, 20).

The consumer purchases a retail device, download a browser DRM plug-in for their browser or download a browser with a pre-installed DRM or CDM, or download a mobile app onto their tablet or smart phone (9, 10, 11). The consumer/subscriber then purchases content from the MVPD, OTT Provider, or Content Provider, either on a subscription or transactional basis (14). The CDN Provider, MVPD, OTT Provider, or Content Provider delivers the appropriate content and DRM license to enable the consumer/subscriber to view the content they purchased (15). The DRM license will convey the specific rights the consumer/subscriber has purchased.

Not shown in this diagram are third-party piracy-monitoring services that may be retained by DRM vendors, MVPDs, or content providers to notify them of instances of pirated content, which they can use to activate their own breach detection and response activities, or into joint action in some cases.

C. CableCARD CAS Trust Infrastructure

In the CableCARD version of the CAS trust infrastructure, the CAS (1-12, 15, 21-25) is separable from the rest of the retail device (Host), and DFAST encryption is used across the CableCARD-Host interface. A DFAST license agreement between CableLabs and the Retail

Device Manufacturer includes robustness and compliance rules, approved output rules, warranties and indemnification, liability for security breach, rules for handling DFAST secrets, and other terms addressing service and security. (13) Content Providers and Cable Operators are third-party beneficiaries of the DFAST agreement. (19, 20) CableLabs acts as the verifier across multiple retail devices and multiple CableCARD manufacturers. (7, 8, 14) Some Retail Device Manufacturers also have business agreements with Cable Operators addressing additional services and terms. (19)

The Subscriber purchases a retail CableCARD device from the third party Retail Device Manufacturer. (16) The retail CableCARD device manufacturer has an end-user license agreement (EULA) for use of the software in the device and in some instances may also have a contract for a service provided to the subscriber by the retail CableCARD device manufacturer. (27) The Subscriber then signs up for cable service from their Cable Operator, and obtains a CableCARD from their Cable Operator to be used in their retail device. The Cable Operator activates that CableCARD and enables the Subscriber to view their subscribed content. (17, 18)

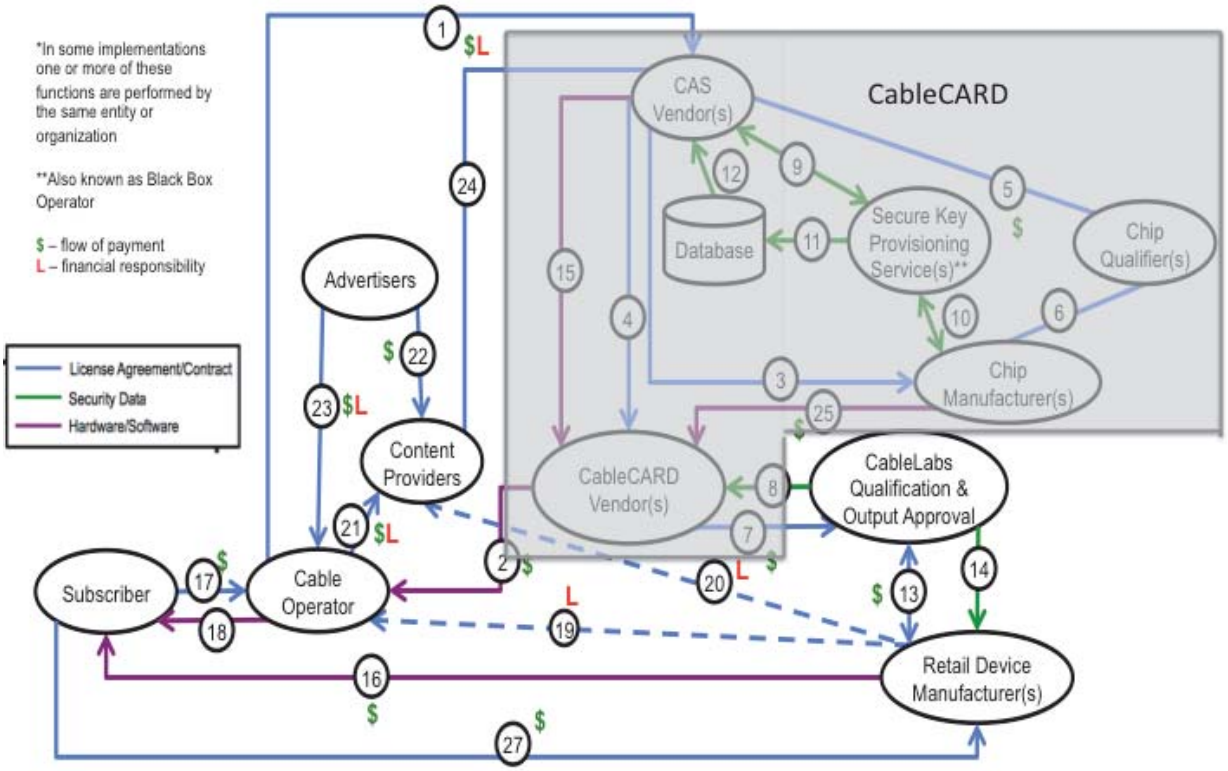


Figure 3 - Example CableCARD CAS Trust Infrastructure

References

[1] Jim Alexander, Charter DCAS Environment, Presentation to DSTAC WG2, March 12, 2015

[2] Ahmad Ansari, AT&T U-verse Overview, Presentation to DSTAC WG2, March 12, 2015

[3] Ralph Brown, Current Cable Technologies and Architectures, Presentation to DSTAC WG2, March 12, 2015

[4] Ralph Brown, Tackling the US Cable Set-top Legacy: Middleware in a Sea of Proprietary Systems, IEEE, January 2011.

[5] John Card II & Steve Dulac, DBS Architecture Overview, Presentation to DSTAC WG2, March 12, 2015

[6] John Card II, Sling TV Specifics, Presentation to DSTAC WG2, March 12, 2015

[7] Jeff Chen, Bright House Overview, Presentation to DSTAC WG2, March 12, 2015

[8] Steve Dulac, DirecTV Specifics, Presentation to DSTAC WG2, March 12, 2015

[9] Dan O'Callaghan, FiOS-TV, Overview, Presentation to DSTAC WG2, March 12, 2015

[10] Mark Hess, Comments at DSTAC WG2, March 12, 2015

[11] Shalini Ramachandran and Mike Shields, Web-Video Newcomers Undercut YouTube, Wall Street Journal, March 8, 2015

[12] George Sarosi, TWC IP Video Architecture, Presentation to DSTAC WG2, March 12, 2015

[13] Ken Silver, OMS and Optimum Services, Presentation to DSTAC WG2, March 12, 2015

[14] Mark Vickers, Current Cable Technologies and Architectures (Comcast example), Presentation to DSTAC WG2, March 12, 2015

[15] Eric Pfanner and Takashi Mochizuki, Sony to Roll Out New Internet TV Service This Year, Wall Street Journal, March 11, 2015

[16] About RDK, http://rdkcentral.com/about-rdk/

[17] Jeff Baumgartner, Comcast, TWC to Co-Manage Set-Top-Focused RDK Project, Multichannel News, Aug. 15, 2013, available at http://www.multichannel.com/distribution/comcast-twc-co-manage-set-top-focused-rdk-project/144963

[18] Steve Watkins, Presentation to DSTAC WG2, March 12, 2015

[19] MovieLabs Specification for Next Generation Video and MovieLabs Specification for Enhanced Content Protection, available at http://www.movielabs.com/ngvideo

[20] First Panasonic Tru2way TVs hit stores in Chicago, Denver, CNET (October 16, 2008), available at http://www.cnet.com/news/first-panasonic-tru2way-tvs-hit-stores-in-chicago-denver/.

[21] Petr Peterka & Jim Williams, MVPD Security Architectures, Presentation to DSTAC WG2, March 19, 2015.

[22] Brad Love, CableCARD TV receivers: Brief history of innovations**,** Presentation to DSTAC WG2, March 31, 2015

[23] Joe Weber, Retail CableCARD Set-tops, Presentation to DSTAC WG2, March 31, 2015

[24] Jim Williams, Submission to DSTAC WG2 on smaller cable and telco systems, April 3, 2015

[25] John Card II & Fred Ellis, Sling Television, Presentation to DSTAC WG2, April 9, 2015

[26] Matthew Chaboud, Amazon Video Playback Device Content Security, Presentation to DSTAC WG2, April 2, 2015

[27] Mark Vickers, The IP Video Transition, Presentation to DSTAC WG2, April 9, 2015

[28] FCC Second Report and Order

[29] Ralph Brown, MVPD CAS and DRM Trust Infrastructures, Presentation to DSTAC WG2, April 14, 2015.

DSTAC WG3 Report

I. Introduction

A. DSTAC Mission

The DSTAC's mission is "to identify, report, and recommend performance objectives, technical capabilities, and technical standards of a not unduly burdensome, uniform, and technology- and platform-neutral software-based downloadable security system" to promote the competitive availability of navigation devices (e.g., set-top boxes and television sets) in furtherance of Section 629 of the Communications Act. The DSTAC must file a report with the Commission by September 4, 2015 to detail findings and recommendations. [DSTAC Mission, www.fcc.gov/dstac]

B. DSTAC Scope

See *Scope of the DSTAC Report*, FCC, April 27, 2015 [DSTAC Scope, https://transition.fcc.gov/dstac/fcc-staff-guidance-04272015.docx]

C. Working Group 3 Description

The working group will identify performance objectives, technical capabilities, and technical standards that relate to the security elements of the downloadable security system. The working group will also identify minimum requirements needed to support the security elements of the downloadable security system. [*WG 3 & 4 Descriptions*, FCC, April 27, 2015]

D. Working Group 3 Product

The working group will deliver a written functional description its performance objectives, technical capabilities, and technical standards, and minimum requirements to the full DSTAC. It will present an outline of its work at the May 13, 2015 meeting, a first draft of its report at the July 7, 2015 meeting, and a final report for full DSTAC discussion and consideration at the August 4, 2015 meeting. [*WG 3 & 4 Descriptions*, FCC, April 27, 2015]

II. Downloadable Security System - Common Framework

A. Downloadable Security System – Common Definitions

In order to meet its goal of creating a functional description of performance objectives, technical capabilities, technical standards, and minimum requirements of a Downloadable Security System (DSS), WG3 worked to define common or alternate definitions of what a downloadable security system is, what functions it performs and what components it is comprised of. This effort aims to fulfill the DSTAC Mission of identifying "a not unduly burdensome, uniform, and technology- and platform-neutral software-based downloadable security system".

Objectives, capabilities, standards and requirements are measured against this set of definitions in subsequent sections of this report.

Definition of a Downloadable Security System:

Downloadable Security System (DSS) is a software based security system selected or supported by the media provider that is capable of being transferred from a download server and installed onto a navigation device to securely receive the services offered by the media provider. The DSS download server may be operated by the media provider, the device maker or a DSS vendor. A DSS may be downloaded as part of a client application or downloaded as part of the client OS or downloaded as part of the client TEE or pre-installed on the navigation device at manufacture time. (Note: As in the latter case, while the DSS is always download*able* it may not always be download*ed*.)

The DSS performs the required **functions** necessary to protect the media provider's service from a variety of attacks. A DSS relies on a number of common **components** within the navigation device. These common components may preferably support one or more DSS's from multiple media providers and one or more DSS vendors. A DSS may rely on a hardware root of trust capable of multiple hardware implementations.

"Modern computing devices consist of various hardware, firmware, and software components at multiple layers of abstraction. Many security and protection mechanisms are currently rooted in software that, along with all underlying components, must be trustworthy. A vulnerability in any of those components could compromise the trustworthiness of the security mechanisms that rely upon those components. Stronger security assurances may be possible by grounding security mechanisms in roots of trust. Roots of trust are highly reliable hardware, firmware, and software components that perform specific, critical security functions. Because roots of trust are inherently trusted, they must be secure by design. As such, many roots of trust are implemented in hardware so that malware cannot tamper with the functions they provide. Roots of trust provide a firm foundation from which to build security and trust."[1]

[1] http://csrc.nist.gov/projects/root-trust/

In the context of Downloadable Security, it is envisioned that **Hardware Roots of Trust** will be utilized for functions such as: the primary point of storage of consumption device secure identities, device key lists, key lists used for dissemination of information to intermediary security infrastructure, and revocation lists.

A common requirement within the hardware root of trust is a mechanism that allows the hardware to be uniquely identified explicitly or implicitly, giving each manufactured silicon chip its own "personality" (or unique number). Since no two chips are alike, the embedded secret key provides unique strength in how that device can be addressed by a secure ecosystem.

Additionally, it is important to understand the concept of service and user Authentication and Entitlement. Unless explicitly indicated, these terms represent concepts and functions, but not actual instantiations. For example Entitlements refers to the range of service states available from a pay service and not to specific implementations of license and entitlement distribution, such as entitlement management messages (EMMs). The functions may be part of a conditional access system, a DRM system, or another system that is part of the MVPD network.

Authentication – confirming a device or user is a subscriber of the MVPD service and authorized for service, and is typically encrypted. Examples of the authentication process could include the user entering a username and password, geo-location of the IP address, hardware device id, or the device presenting a certificate that is validated by a MVPD network component. Re-authentication may occur at different time intervals depending on authentication type.

Entitlements – refers to the control plane metadata indicating what services are available to the authenticated device and/or user, and is typically encrypted. For example a user may be entitled to a certain set of linear broadcast video channels, a pay per view (PPV) event, or a subscription VOD service. These may be functions of subscription level, time, device type and location. Entitlements are expected to change with time. The method by which entitlements are expressed and communicated have typically been an area where security solution providers (CAS or DRM) have differentiated their products in a competitive market.

Usage Rights – an authenticated device and/or user that is entitled to a service may have certain usage rights associated with the content they receive from the service. For example Copy Control Information (CCI) indicates if copies of the content can be made, plus any restrictions on those copies such as how many copies can be made. Usage Rights are usually expressed using a Right Expression Language (REL) which "is a machine-processable language used to express copyright or similar status of data."[2] Specific Usage Rights may be functions of subscription level, time, device type and location.

[2] https://en.wikipedia.org/wiki/Rights_Expression_Language

These concepts can also be seen as a process performed by the DSS or other component of the MVPD's network. Devices and their user interfaces utilize these processes to enable the user to access content services.

Further detail on how these processes are currently implemented in the MVPD network can be found in Section VIII.

B. Downloadable Security System – Common Requirements

1. DSS Functions, Core Components, Technical Capabilities, and Supported Services

*a) **Functions** of a Downloadable Security System*

Some of the main functions that a DSS performs:

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.[3]
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.
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.
4) Provides to the navigation device secure and verifiable information on the authorized services available to the device and user.
5) Enables descrambling of the authorized services available to the device.
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.
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.
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.
9) In the network, distributes entitlement information in various forms, using either one way or two way protocols, depending on the delivery network type.

---

[3] A DSS itself cannot independently verify that a device has met or supports all required robustness rules, hardware requirements or compliance requirements. These are typically done in a design audit, self-verification or other process (such as a legal agreement) to a set of Compliance Rules. The DSS and associated security servers verify, via a certificate or other highly secure mechanism, that a device reports such compliance. In typical implementations, any failure in this type of validation will deactivate the DSS and its associated device. In order to achieve this level of security, a DSS must be considered as part of a broadly defined security infrastructure which includes key management, secure manufacturing, audit, testing, standards development, etc. The level of the robustness and compliance will impact the content available, determined by the content licenses between content owner and distributor.

10) The DSS fulfills the commercial and/or regulatory obligations of an MVPD to protect content from content sources/owners. As an example, the Encoding Rules for CableCARD limited scope of MVPD obligations when applied to retail devices.

Optional Functions that may be required to enable a 3rd party User Interface to display and manage some or all of the media provider service:

1) Method to provide a 3rd party User Interface application knowledge of:
   a) Device Authorization status
   b) Media provider's Service Authorization status
   c) License rights for media provider content

b) Components of a Downloadable Security System

The definition and functions of a DSS imply a set of core components that a DSS must contain. The components include:

1) One or more software components that are provided by the MVPD/OVD and downloadable to devices
2) Common methods for a navigation device to securely discover and obtain the software components from a media provider.
3) A method of determining the robustness of the platform and execution environment that runs the software components.
4) A set of device requirements to provide a hardware and software execution environment such as a hardware root of trust, software libraries and trusted operating environment that meet the required robustness and compliance requirements.
5) A system for replacing or upgrading the software components.
6) A system for validating and/ or revoking the validation of the software components.
7) Network elements to support secure code download, content encryption, and entitlement distribution functions.

Optional Components that may be required to enable a 3rd party User Interface to display and manage some or all of the media provider service:

1) Method to provide a 3rd party User Interface application the ability to:
   a) Request a list of video services available to the device and user
   b) Request a video service to be decrypted
   c) Request license rights for media provider content
      i. Make local recordings of content if permitted by the license rights

c) Technical capabilities of a Downloadable Security System

1) Makes use of a hardware root of trust, or other framework, if available, that can be utilized to support secure code download of the DSS software.
2) Can decrypt standard encryption algorithms including DES, CSA, AES with suitable performance for the target device.
3) Optionally provide support for software downloadable non-standard encryption schemes equal in computational complexity to AES, to support download of system-specific countermeasures.
4) Can decrypt content packetized in a variety of formats, including MPEG transport streams, HLS, MPEG-DASH.
5) Supports software implementation, or access to hardware implementation, of standard cryptographic functions such as decryption ciphers, check-sums, hashes, and other one-way functions.
6) Protects and delivers content protection key(s) to the navigation device in a way that meets the conformance and robustness rules of the whole DSS system.

d) Services provided to the rest of the Navigation Device

1) Decrypts content, and may copy protect content or validate copy protection for delivery to either a player app or hardware decoder.
2) Interprets copy control information provided by the DSS management system and securely applies relevant copy control to digital outputs.
3) Supports some secure mechanisms such as secure boot, secure download, decryption, and signature verification services.
4) Optionally authenticates credentials presented by the navigation device with respect to relevant license regimes.
5) Provides authorization status with respect to a specified class of content to client-resident applications.
6) Optionally supports session-based security services to other applications in the client device.

2. System Requirements

a) System components (an application environment, a communication path, a secure execution environment, secure hardware elements, trust model, etc.)

A DSS must support the ability to download sufficient code and data to renew the security system – to download different keys, certificates, code, configuration parameters, etc., such that the renewed system is secure.

A DSS must have hardware resources to (1) uniquely identify the hardware, (2) store cryptographic keys securely, (3) enable secure updating of the securely-stored cryptographic keys, and (4) support a segregated execution environment for security operations (either by a separate CPU or by strong hardware segregation features, or equivalent).

Security without trust is impossible. We suggest that a DSS should (1) try to minimize the amount of trust placed in personnel, facilities and operations and (2) explicitly state what level of trust is required for the downloadable system to operate securely. Beyond these requirements, specification of a trusted registrar for keys may be necessary in some architectures.

b) Interfaces between system components

A CAS or DRM system is typically split into two main subsystems, (1) a “server” in the head-end or cloud that originates the viewing rights or licenses, and (2) a “client” subsystem located in the viewing device that securely applies the rights or license to descrambler to decrypt the content.

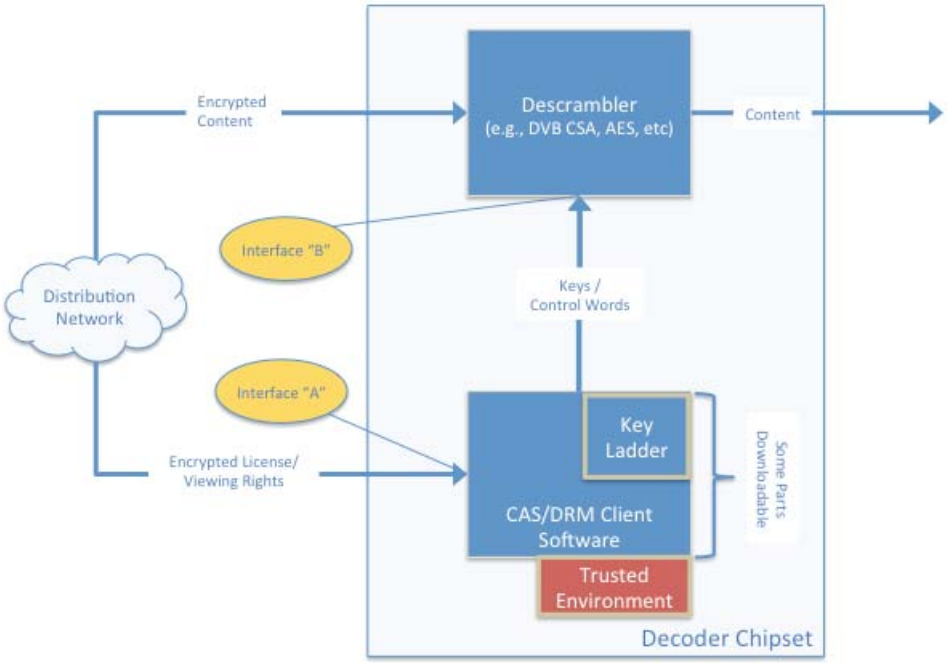


Figure 1 – Typical Communication Path Interfaces for Security Sub-system

The server head-end or cloud components also interface with subscriber management and in turn billing systems. These interfaces are outside the scope of this document.

The server system communicates viewing rights to the client in a one way broadcast CAS system through broadcast messages. If the system can be relied upon to be two-way, the rights can much more efficiently be requested via an IP call using traditional IP techniques. (Interface A in the graphic above)

For a DRM system, an IP channel is used by the client to request the viewing rights.

Within the client device, the rights are securely decrypted and a content or working key is securely connected to the content descrambler which forms part of the secure video path. (Interface B in the graphic above)

c) Compliance Rules

Devices implementing the downloadable security system need to be required to follow compliance rules. Generally, compliance rules describe things that the platform is required to do, and things that the platform is required not to do. For example, some of the compliance rules necessary may include:

- No Circumvention – A device shall not directly or indirectly provide access to content except as permitted in the compliance rules.
- Outputs – A device shall not emit the digital plaintext of encrypted audiovisual content on any interface that is not protected by a content protection system (such as DTCP-IP, HDCP, etc.). A device shall not emit unprotected audiovisual content on any output at a resolution higher than "standard definition" (720x480x60i or less).
- Watermark – A device shall not knowingly or intentionally disrupt, remove or interfere with a watermark that is widely used to enforce or track copy controls or copy control circumvention.

However, compliance rules are typically applied to a *product* – including both the hardware platform, and the firmware and software that runs on it. Compliance rules will need to be developed that are applied to the hardware platform; separately, compliance rules will need to be developed that are applied to the firmware and software.

d) Robustness Rules

Devices implementing the downloadable security system need to be required to have a certain level of robustness to attack. Generally, robustness rules describe how the hardware must be constructed so as to provide a certain level of resistance to attack.

Robustness rules have typically been an area where security solution providers (CAS or DRM) have differentiated their products in a competitive market. In general, content owners will refuse to license content to less robust solutions and MVPDs or OVDs will refuse to make use of them.

For a system to be secure it needs to preserve and maintain three basic properties: (1) confidentiality – secret data and secret operations are kept secure from unauthorized parties, (2) integrity – secret data and secret operations are kept secure from modification by unauthorized parties, and (3) availability – unauthorized parties are kept from disrupting or limiting access to the secured system. Whatever components (hardware, software) are used to build a downloadable system should ensure that these properties are not violated.

For example, some of the robustness rules necessary may include:

- Preservation of Secret Data – Devices shall be designed and manufactured such that they resist attempts to discover, revel and/or

use without authority any secret keys (including without limitation content keys, entitlements, or other authentication and decryption keys). Some attacks that chip designers should resist include: invasive imaging using powerful state-of-the-art microscopes, access to the keys using unsecured JTAG ports, attacks that use side-channel information such as power consumption, electromagnetic emissions, temperature difference, acoustic outputs, optical side-channel information or digital side-channels through on- and off-chip microarchitectural structures.

- Secure Content Path – Devices shall be designed and manufactured such that unencrypted digital audiovisual data is never transmitted or observable using standard board-level hardware debugging tools such as logic analyzers, JTAG debuggers.
- Unique Identification – The device and system shall be designed, implemented and manufactured to prevent an adversary from emulating the hardware platform in software to violate the security properties of the system. The device shall be required to provide an unforgeable proof to the software about the authenticity of the device.
- Software Attestation – The downloadable system shall be designed and implemented to provide an unforgeable proof of the authenticity of the software portion of the downloadable system. Specifically the adversary should not be able to modify the computer instructions of the downloadable system before or during the operation of the downloadable system. For maximum security, the attestation must be provided during the life-time of the software but one time attestation, i.e., when the system is rebooted each time, is acceptable if the device fulfills the non-interference robustness requirement.
- Non-Interference – The downloadable system shall be designed, implemented and manufactured to ensure that the execution of trusted components shall be not be influenced by the execution or presence of untrusted components executing on the system for the entire life-time of the downloadable software.
- Preservation of secret operations – The downloadable system shall be designed, implemented and manufactured to ensure to operations based on secret data cannot be subverted by the adversary to produce incorrect results. Further such subversion should be reported in an unforgeable manner to the provider.
- Forward Revisioning – The downloadable system shall be designed, implemented and manufactured such that the system can never be rolled back to an older version of the system than what exists in the system as identified by an unforgeable revision number associated with a system.

e) (if you do assume IP connectivity) DBS STB must act like DCAS server device – robustness, capabilities, etc.

Unique system requirements for a one-way environment (ie. DBS).

DBS services are inherently one way in nature, but must interface over 2-way IP networks to other devices in the home. It is unclear whether anchoring a DSS system on an adjunct and unmanaged IP connection is in harmony with the overall mission of designing a "uniform" and "platform-neutral" system. Because DBS devices have no a priori knowledge about reliability, bandwidth, cost, or other factors in any broadband-like connection they find, DBS CPE does not rely on this path for enabling two-way communications as part of the conditional access system. Existing DBS security and business practices assume that IP connectivity is intermittent or non-existent, and function effectively absent such communications. Broadband-like IP connectivity can be used to enhance the available content for a particular subscriber, but the basic system must function without IP connectivity.

Specifications would need to be developed to address how this intermittent, unreliable communications path would function in a standard way. Would there be one box with IP connectivity that would proxy for other boxes in the home? Would each box have its own IP connection through a customer-provided gateway? How would IP connectivity be established and maintained in a secure or reliable manner? These would be important factors that would need to be decided upon for the design of such a DBS gateway.

f) Countermeasures must be supported

Once a security compromise has been detected (through inline monitoring mechanisms or out-of-band mechanisms) it shall be possible for the security system to be refreshed the systems in the field to protect against future compromises.

For some compromises (e.g., key extraction using hardware reverse engineering, or deep probing into the hardware, or through other hardware means) the cure for the breach requires changing the hardware itself, and may not be cured without hardware change. For other compromises (including, but not limited to, software compromises or software vulnerability), cure may be effected by downloading different software.

g) Device and system testing by multiple parties must be supported

In the same way that stronger robustness and compliance rules provide greater levels of assurance that content licenses will be enforced, stronger and more thorough testing regimes provide greater levels of confidence that the functionality and, indirectly, robustness is compliant as well. The traditional MVPD CAS trust ecosystem, for example, implements a more thorough level of testing. Multiple parties are involved in this testing and validation regime. The SoC and set-top are validated from the robustness and compliance perspective in addition to functional testing to insure the MVPD service is appropriately supported.

The security system must support multiple testing parties. The device and system testing process should be designed in a way that a particular tested component (e.g., a retail navigation device) can be tested by any one of a set of testing entities, without any compromise in security or functionality.

For devices that attach directly to the MVPD network, the retail device would have to be designed to meet the required testing for each MVPD, focused on protecting the integrity of the MVPD physical network. Recognizing that testing against each and every MVPD would be a significant task, a solution would be needed to consolidate the test requirements to reduce the effort.

An example of how device and system testing processes work today is described in Section 0~~VIII~~.

h) Registrar for keys

A single entity, or a federated registrar consisting of multiple entities with secure exchange of credentials, should span all MVPDs and manage keys. Care has to be taken in the governance of this body or bodies with perhaps a board consisting of a wide cross section of stakeholders. The complexities and challenges of systems like this are outlined in the Working Group #2 Report, Section XII: Summary of MVPD CAS and DRM Trust Infrastructures [https://transition.fcc.gov/dstac/wg2-report-01-04212015.docx].

i) Devices need to support multiple MVPD simultaneous subscriptions

As a general rule most subscribers only subscribe to one MVPD at a time. However, there are instances where a subscriber may subscribe to multiple MVPDs simultaneously. The downloadable security system must not prevent a single device from supporting simultaneous subscriptions to more than one MVPD.

This use case could be handled in the following ways for the models referenced above:

- MVPD TV Apps – This solution enables multiple concurrent MVPD subscriptions. Each MVPD provides its own App, and the subscriber chooses which App to use at any point in time.
- HTML5 Web Apps – This solution enables multiple concurrent MVPD subscriptions. Each MVPD provides its own website and Web App, and the subscriber chooses which web site to visit at any point in time.
- VidiPath/RVU – The subscriber would have to have at least one VidiPath or RVU server from each MVPD and all of his devices connected to the home network. In this case the subscriber chooses which VidiPath or RVU server he wishes to use at any given point in time.
- Two Contexts – This solution would enable a device to have two (or more) distinct DSS instances, one per each MVPD.

For devices that attach directly to the MVPD network, the retail device would have to be designed to connect to multiple MVPD networks concurrently.

j) Devices need to support portability across MVPD subscription services

Retail navigation devices must be portable to other networks (e.g., when a consumer changes MVPD or moves into another cable operator's footprint). To support this, the downloadable security solution must support normal network registration, device authentication, device provisioning, secure download of the security software, and secure provisioning of service entitlements, as well as transitions from one MVPD network to another. The transition from one MVPD to another may involve an overlap of service (both services active) or a gap in service (neither service is active) and may involve a disruption of power to the device or may not, depending on the specific transition scenario. The activation of the new MVPD service may or may not involve an installation visit by an installer from the new MVPD. Regardless, a confirmation that the subscriber is receiving the desired service from the new MVPD is required. A retail device must support all of these transition scenarios.

3. Performance Objectives

The WG2 report captures several high level requirements regarding Scalability, Latency, and Addressability (see e.g. S13, S14, S15). A commercially viable DSS solution will need to fully address a broad set of performance objectives. Additionally, it is recognized that there are unique requirements for operating in one-way and two-way distribution architectures.

4. Technical Standards

See Annex C for relevant Standards references.

5. Representative devices to be considered

- Standard/High Definition/Ultra High Definition STB
- High Definition and 4K Ultra HD TV – for IP and other delivery paths
- RVU certified TV
- VidiPath certified TV
- Home Media Server
- Home Video Gateway from MVPD, Residential Gateways (RG)
- Digital Transport Adapter (DTA)
- Simple Digital Video Recorder
- Whole Home DVR Ecosystem
- Media Player Box from Retail (e.g. Roku, Apple TV, Amazon, WD)
- Media Player Sticks (e.g. USB, HDMI)
- Connected Tablet with Data Plan
- Connected Tablet with Wi-Fi
- Connected Smart Phone with Data Plan
- Connected Smart Phone with Wi-Fi
- Broadband Connected Blu-Ray Players
- Notebook or Laptop Computer (e.g. Apple, Windows, Linux)
- All-in-One or Desktop Computer (e.g. Apple, Windows, Linux)
- Gaming Consoles (e.g. PS4, Xbox)
- Connected AV Receivers
- Internal/External Tuners (e.g. Hauppauge, Silicon Dust, Sat-IP)

C. Existing Downloadable Security System Solutions

DSTAC Working Group 3 conducted a review of 16 existing security system solutions and components including both hardware (SoC) and software. The review included both a presentation of the technology to DSTAC members and, where relevant, a detailed response to survey of questions developed by Working Group 3 regarding the technical details of the respective security system solutions. The 16 security solutions and technologies reviewed were:

- Broadcom SoC
- PolyCipher
- W3C HTML5 Encrypted Media Extensions (EME)
- Open Media Security (OMS)
- Cisco VideoGuard
- Digital Transport Adaptor (DTA) Security
- Adobe Primetime
- Verimatrix VCAS
- Arris SecureMedia
- Nagra anyCast Connect
- RVU Alliance
- DLNA VidiPath
- Alticast XCAS
- MStar SoC
- Intel SGX Technology SoC
- Microsoft PlayReady

The presentations of the solutions reviewed are included in Appendix A, the survey questions developed by Working Group 3 in Appendix B, and the survey responses received in Appendix C.

A table summarizing all of the responses can be found in **Error! Reference source not found.**~~Table 1~~ of Annex D. The following section provides a shorter summary of this information.

1. Description of existing solutions

The downloadable security solutions that were reviewed ranged from the hardware technologies employed in current or next generation SoCs, to CAS and DRM solutions, to standards based solutions. The SoC vendors reviewed were: Broadcom, MStar, and Intel. The CAS and DRM solutions reviewed were: PolyCipher, OMS,

VideoGuard, DTA Security, Adobe Primetime, VCAS, SecureMedia, anyCast Connect, XCAS, and PlayReady. The standards based solutions reviewed were: HTML5 EME, RVU Alliance, and VidiPath.

There are several key observations that can be drawn from this review:

- Many of the solutions presented noted that CAS and DRM solutions are beginning to converge, blurring the line between the two. Several solutions presented an integrated CAS and DRM solution.
- Most of the solutions reviewed identified a hardware root of trust, secure boot, secure software download, and a trusted execution environment as important elements of a downloadable solution.
- The market supports and encourages a diversity of solutions that compete, driving innovation and cost reduction. All of the SoC, CAS, and DRM vendors have developed successful businesses providing security solutions to the market. SoC vendors have integrated security features into their chips to reduce costs, meet content providers' requirements, and compete in the market for hardware components. CAS and DRM vendors introduce new features into their systems to address evolving business models and content license requirements in the content distribution market. Standards are developed to provide scale for these systems, whether over the Internet or within home networks.
- A diversity of trust infrastructures including different robustness and compliance rules has developed to address different market opportunities. One presentation explicitly stated, "Permissions and security expectations vary widely and no one size fits all."
- Some of the solutions indicated support for both 1-way and 2-way networks, other solutions indicated that they were designed for 2-way networks only.
- There were strong recommendations to avoid rigid and/or single implementations (one-size-fits-all) that significantly limits innovation, competition, or increases security risk.
- Standards are carefully developed to allow for different, even proprietary, implementations to meet the requirements enabling differentiation among the implementations.

2. Existing applicable or related specifications

- UPnP and DLNA Guidelines
- W3C HTML5 Specification, *A vocabulary and associated APIs for HTML and XHTML*. http://dev.w3.org/html5/spec/
- W3C WOFF File Format 1.0. http://www.w3.org/TR/WOFF/

- W3C MSE, *Media Source Extensions*. http://www.w3.org/TR/media-source/
- W3C EME, *Encrypted Media Extensions*. http://www.w3.org/TR/encrypted-media/
- W3C Crypto, *Web Cryptography API*. http://www.w3.org/TR/WebCryptoAPI/
- RVU Alliance Specifications

III. Download Security System Threat Models

A Threat Model describes the level of tools available to the attacker, combined with a description of the amount of power or influence that the attacker has on the content delivery network.

Some examples of "level of tools" are:

- ***Widely Available Tools*** means tools or equipment that are widely available at a reasonable price, including items such as screwdrivers, jumpers, chip clips, file editors, and soldering irons.
- ***Semi-Professional Tools*** means specialized electronic tools that are widely available at higher prices than Widely Available Tools, but still affordable by a broad spectrum of the population. Within this category are tools such as memory readers and writers, debuggers, decompilers, or similar software development products.
- ***Professional Software Tools*** means professional tools, such as the software equivalent of in-circuit emulators, disassemblers, loaders, or patchers, implemented in software, that require professional skill and training to utilize.
- ***Professional Hardware Tools*** means tools or equipment, such as logic analyzers, chip disassembly systems, or in-circuit emulators, implemented in hardware, that require professional skill and training to utilize.
- ***Highly Sophisticated Tools*** means tools or equipment such as scanning electron microscopes, black box programming equipment and other equipment that might be available to an inside attacker, that require very specialized professional skill and training to utilize.

Some examples of "amount of power" are:

- **Level 0** – This least-powerful attacker has no control over any computer in the content delivery network.
- **Level 1** – This class of attacker has knowledge of the network infrastructure and can observe and manipulate everything in the network environment of the consumer
- **Level 2** – This class of attacker has knowledge of the network infrastructure, can observe and manipulate everything in the network environment of the consumer, and also has resources and ability to fake services, falsify authorization levels, manipulate service provider databases, and disable encryption systems as example capabilities. This would equate to a sophisticated inside attacker.

The threat model considered is described below.

A. Level of attacker capability

The attacker is a well-organized, well-funded organized crime syndicate, with significant technical, monetary and personnel available to devote to attacking the security system. Such an attacker can be expected to have access to Highly Sophisticated Tools with the skill and expertise to use them, and Level 1 access to the content delivery network.

B. Describe robustness from attackers

It is desirable for the DSS (at the highest level of capability) to be able to withstand and repel an attack assuming a combination of Level 1 access to the network, along with access to both Professional Hardware Tools, and Professional Software tools.

C. Threats not in scope

Bribery and corruption are outside the scope of threats to be considered.

We are assuming that threats corresponding to rogue network operator employees who grant service authorizations using the official systems, then proceed to hide their tracks via actions such as deletion or editing of transaction logs, are not within the scope of DSS to deal with. Similarly, attackers with Level 2 access to the system, along with Highly Sophisticated Tools, are also considered to be out-of-scope.

D. Diversity

It is anticipated that various levels of DSS capability will continue to be implemented on different device classes, as is the case today. Some implementations will not be sufficiently robust to withstand the highest level of attack identified above. We assume that in such cases, the type of content enabled on the weaker platforms will be limited to exclude content whose value is deemed to warrant the higher level of protection.

An additional level of diversification will occur through commercial competition in a future DCAS market. The output of the DSTAC group, and/or any subsequent groups may result in a broad definition or set of definitions, or a recommendation in DSS implementation specifications. However many areas that relate to security will still be open for innovation and hence differentiation. Thus by its very nature, competitive implementations will offer a degree of diversification.

Finally, deliberate diversification is a well-known technique used in obfuscated software components of a security system. Here the software is compiled or assembled in a way that makes reverse engineering very difficult AND it is done is such a way that there are multiple versions of the same or similar products deployed simultaneously. In this way a commercial hacker has a much larger challenge in deploying hacks to a wide enough population to make his criminal enterprise sustainable.

IV. Download Security Systems

The DSTAC WG3 has prepared two proposals for implementing a software-based downloadable security system. Proposal 1: HTML5 Security API's, was authored by Mark Vickers, Comcast and Proposal 2: Virtual Headend System was authored by Adam Goldberg, representing Public Knowledge. There are a number of commonalities between the two proposals that are important to highlight:

- Both proposals acknowledge the diversity of technologies across MVPDs and even within MVPDs of a similar type,[4]
- Neither proposal recommends a solution based on common reliance,[5]
- Both proposals acknowledge that it is unreasonable to expect that retail devices connect directly to the various MVPDs' access networks and rather connect via an IP connection with specified APIs/protocols,[6]
- Both proposals acknowledge that is unreasonable to expect that MVPDs will modify their access networks to converge on a single common security solution,[7]
- Both proposals acknowledge that the downloaded security components need to remain in the control of the MVPD.[8]

These commonalities represent significant agreement on the underlying principles involved.

---

[4] "Each of these systems and permutations have specifics which make them different even from others of a similar type. For example, among direct broadcast satellite systems, there are different conditional access systems in use with different signaling protocols, and different content encryption mechanisms."

[5] *Proposal 2: Virtual Headend System*, "It should not be necessary to disturb the potentially multiple present and future DCAS and other network technology choices made by cable, DBS and IPTV systems, which leave in place several proprietary systems for delivering digital video programming and services across MVPDs, while still supporting competitive navigation devices."

[6] *Proposal 2: Virtual Headend System*, "It would not be a step forward to return to an environment in which, to offer access comparable to that of MVPD-sourced devices, across all MVPD programs and services, a competitive manufacturer would have to equip a device with RF tuners for cable and satellite, varied semiconductor platforms to support the dozen-plus proprietary DCAS technologies that may be used, and IP connections for IPTV implementation, and provide for all associated application and field testing."

[7] *Proposal 2: Virtual Headend System*, "Nor is it reasonable to expect that all operators will radically re-architect their networks, and converge on a common solution in order to avoid the obstacles to competitive solutions."

[8] *Proposal 2: Virtual Headend System*, "The downloaded security components of the Virtual Headend System do not need to be standardized to a particular hardware platform or CPU architecture, as these aspects remain in the MVPD's control."

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

1. Summary

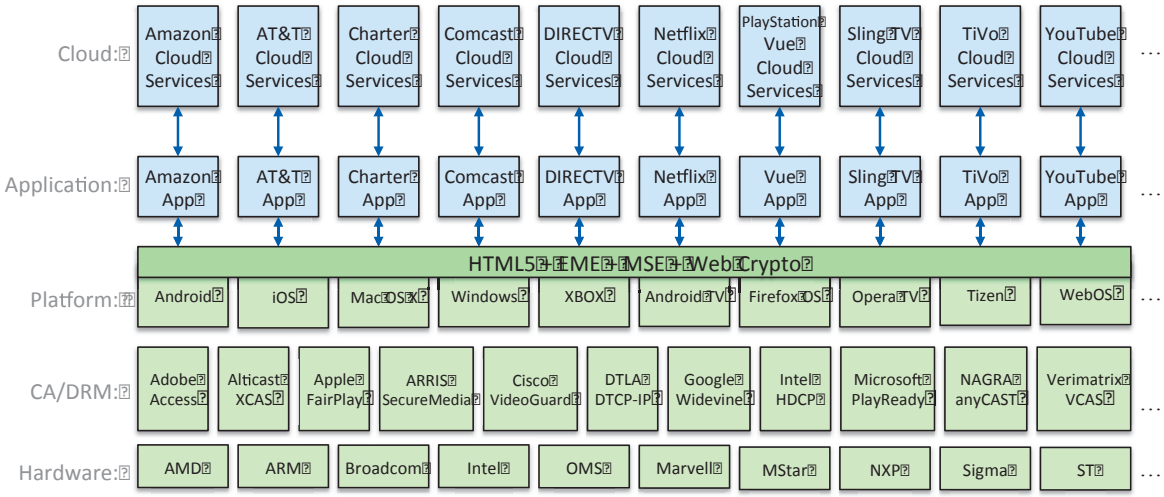


Figure 1 HTML5, EME, MSE & Web Crypto

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.

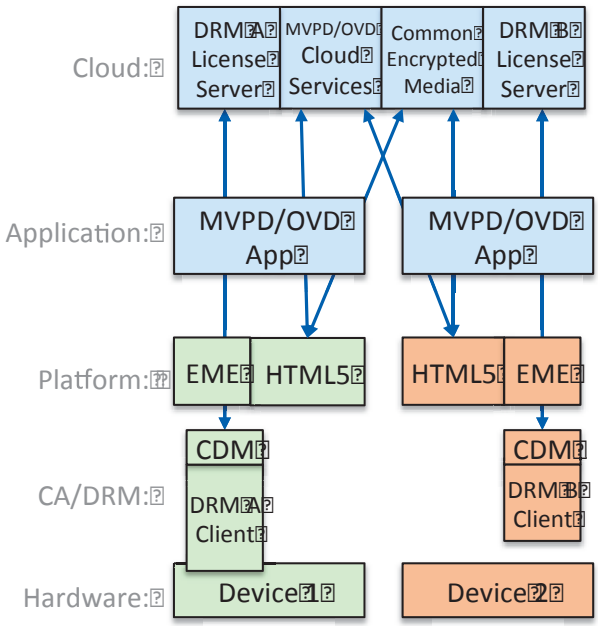


Figure 2 HTML5 EME Common Encryption

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

B. Proposal 2: Virtual Headend System

As is documented in the working group 2 and working group 4 reports, there is a wide variety of network architectures, delivery networks, and security systems in use by MVPDs today. These include both "mostly" one-way systems, like direct broadcast satellite, traditional cable HFC/QAM systems, IP-centric telco systems, and combinations thereof (e.g., Verizon FiOS). Within these, there are security systems rooted in Smartcard conditional access technologies, traditional embedded conditional access security technologies, and various permutations based on DRM-style security controls.

Each of these systems and permutations have specifics which make them different even from others of a similar type. For example, among direct broadcast satellite systems, there are different conditional access systems in use with different signaling protocols, and different content encryption mechanisms. Unless all MVPDs replace or upgrade these proprietary solutions with some common and interoperable means of network termination using a downloadable conditional access system (DCAS) or other technology however, only such devices as are designed for these proprietary systems and authorized by the specific MVPD can connect directly to the MVPD network to achieve full access. It should not be necessary to disturb the potentially multiple present and future DCAS and other network technology choices made by cable, DBS and IPTV systems, which leave in place several proprietary systems for delivering digital video programming and services across MVPDs, while still supporting competitive navigation devices.

Because there is such a wide variety of network technologies in use, the best solution which is both not technically burdensome, and supports retail devices which are both portable across MVPDs and geographically, is to create a technical solution that abstracts the network differences of MVPDs away. Such a solution will support the operation of commercial competitive devices to receive all MVPD content on all MVPD systems, as required by Section 629[9] and as a congressionally directed task.[10]

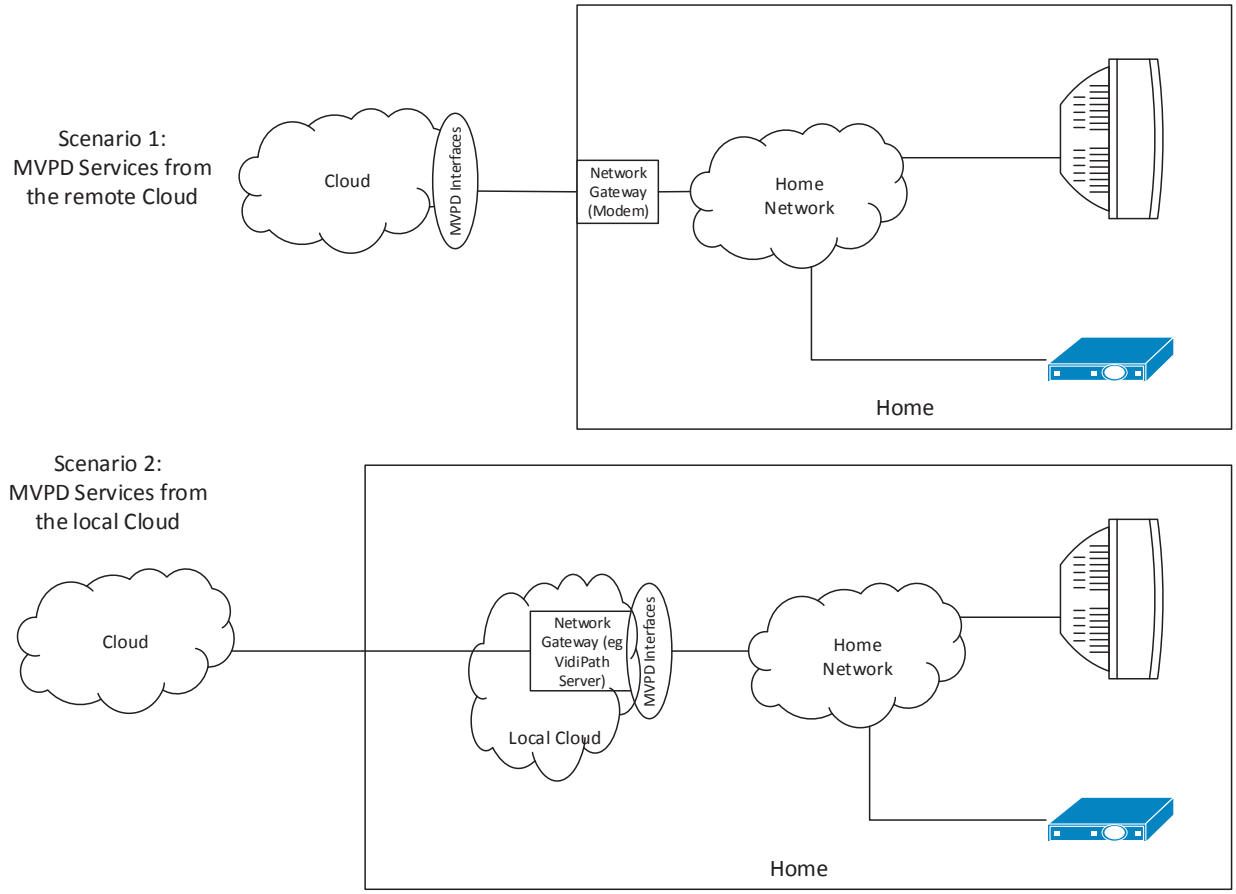
It would not be a step forward to return to an environment in which, to offer access comparable to that of MVPD-sourced devices, across all MVPD programs and services, a competitive manufacturer would have to equip a device with RF tuners for cable and satellite, varied semiconductor platforms to support the dozen-plus proprietary DCAS technologies that may be used, and IP connections for IPTV implementation, and provide for all associated application and field testing. Nor is it reasonable to expect that all operators will radically re-architect their networks, and converge on a common solution in order to avoid the obstacles to competitive solutions.

Instead a Virtual Headend System is a cloud-based security system. Network security and conditional access are performed in the cloud, and the security between the cloud and retail

[9] 47 U.S.C. § 549(a).

[10] DSTAC Charter, Dec 2014.

navigation devices is a well-defined, widely used link protection mechanism such as DTCP-IP. A MVPD may choose a system architecture for a Virtual Headend System that includes a device located at a consumer's location (e.g., home), which provides a "local cloud" which has security system components downloaded to it as necessary, or the entire solution may be in their network "cloud" and offered as IP services directly to devices in the home. The downloaded security components of the Virtual Headend System do not need to be standardized to a particular hardware platform or CPU architecture, as these aspects remain in the MVPD's control. The Virtual Headend System's interface to the home network (and retail devices) is standardized across MVPDs and thereby enables nationally-portable retail navigation devices without imposing an undue burden on MVPDs or retail device manufacturers. Furthermore, this link-protection mechanism can be extended to account for end-to-end IP systems, providing a clear path to purely protocol-based service integration in modern MVPD networks.



DBS providers currently provide devices with functionally similar to a Virtual Headend solution with a "local cloud" device. Dish's Hopper and DirecTV's Genie are currently-distributed devices that serve as Virtual Headend Systems via mixes of standard and proprietary protocols, and provide services to a range of consumer devices connected to the home network "cloud". In order to provide a uniform mechanism for competitive navigation device integration, some form of gateway device will continue to remain a practical necessity for unidirectional distribution networks under any security scheme suggested that complies with the DSTAC's charter.

Comcast and other Cable MVPDs have announced both a “local cloud” solution using VidiPath enabled server devices[11], as well as a true virtual cloud solution such as “Comcast Stream.”[12] These solutions provide content services to unmanaged devices without requiring the implementation or download of MVPD network-specific technologies.

These current efforts from MVPDs demonstrate that operators are working towards Virtual Headend System technology that abstracts legacy network systems into common IP network protocols that serve non-proprietary navigation devices.

[11] “XFINITY for VidiPath enables customers with XFINITY on the X1 Entertainment Operating System to stream video content, including live TV and recorded DVR programs, directly to a VidiPath-compatible device (e.g., smart TV) without the need for an additional set-top box.” http://customer.xfinity.com/help-and-support/cable-tv/vidipath-overview/

[12] “No extra device or additional equipment required…or even a TV. And it’s called Stream”, http://corporate.comcast.com/comcast-voices/a-new-streaming-tv-service-from-comcast; “an IP-based cable service that offers live, on demand and cloud DVR delivered over our managed network in the home”, http://www.engadget.com/2015/07/12/comcast-xfinity-internet-stream/.

V. Annexes

A. MVPD Security System Validation Process

For traditional MVPD deployed set-tops, SoC and set-top box validation is normally done at the direction of the CAS or DRM provider, in response to requirements from content providers and MVPDs. This testing includes a validation of both the SoC and the set-top box that is built using the SoC.

<u>SoC Validation Process</u>

The following is a typical validation process for the SoC:

1. The technical requirements of the CAS or DRM provider derived from requirements from content providers and service providers are made available under license to the SoC vendor. These technical requirements have two parts:
    a) Functional requirements – These are the capabilities and features of the SoC (e.g. cryptographic algorithms, codecs, graphics capabilities, etc.)
    b) Robustness rules – These rules relate to characteristics of the SoC that are not testable by functional testing. They describe what level of security protection is required, rather than how the security functions are to be implemented.
2. Once the SoC vendor has implemented the technical requirements, the vendor will bring in its device to the CAS or DRM provider for validation. This validation has two parts:
    a) Functional validation – This involves running functional tests on a reference or development platform that uses the SoC, to insure that it meets the functional requirements, e.g. properly process a video stream, clear appropriate registers when reset, properly implement cryptographic algorithms, etc. This testing is done independently of the SoC vendor, but will involve iterations with SoC vendor when issues are discovered.
    b) Robustness validation – Since these requirements are not addressed through functional testing, the SoC vendor provides documentation describing how it has met the robustness requirements. This may involve a design review with the SoC vendor or may be done through a third-party review process, e.g. a common criteria evaluation.
3. Once the SoC has cleared this validation testing, a record of this is communicated to the SoC vendor, for example a letter to the SoC vendor confirming validation of the specific SoC version. Device manufacturers can use this as confirmation that the CAS or DRM provider has validated the SoC.
4. If the SoC vendor makes changes to the device, either hardware or software, the vendor is required to notify the CAS or DRM provider of the changes. The CAS or DRM provider will review the changes or contract with a third-party to review the changes and will determine if the SOC needs to be retested. In addition, the CAS or

DRM provider will often monitor which SoC versions are in the market to ensure that they are aware of any SoC revisions of which the vendor may have failed to notify them.

5. In order for a SoC to go through this process with the CAS or DRM provider, the SoC vendor signs a support agreement that obliges it to notify the CAS or DRM provider of any changes or revisions.
6. This process typically takes a number weeks or months for a new SoC, based on any issues that may be discovered through the process. The robustness review is typically the longest portion.
7. The SoC vendor needs to have a Black Box vendor approved by the CAS or DRM provider to inject the right keys into the SoCs at manufacture.
8. Set-top box manufacturers request from the SoC vendor a list of validated parts and the CAS or DRM provider can also verify this. Often the device manufacturers and SoC vendors work closely together through the validation process.
9. The SoC vendor will typically include countermeasures in its implementations, either of its own design or that of the CAS or DRM provider, to support renewability and upgrades in the field if necessary.

Set-top Box Validation Process

The set-top box validation process is very similar to the SoC validation process:

1. Set-top boxes must use a validated SoC before they can be submitted for validation.
2. The set-top box manufacturers must also license functional requirements and robustness rules from the CAS or DRM provider.
3. Devices have a similar process for SOC validation, e.g. functional testing and robustness design reviews.
4. To avoid cloned set-top boxes, the CAS or DRM provider may maintain a database of all the SoCs that could possibly be in the field. Service providers can use this database to validate devices as they attach to their network.
5. CAS or DRM providers monitor hacker sites and any unusual activity, such as the same device being installed in two different locations (cloning).

System and Device Testing Regimes

In addition to the set-top box validation described above, there are various regimes that are used for device and system testing. MVPDs will conduct system testing through a series of phases beginning with lab testing to validate that the system functions in a controlled environment. This is followed by limited field-testing, usually with employees, to validate that the system functions on a production network, and then followed by more expanded field-testing with paying subscribers to validate that the system functions in real customer use scenarios. This process ultimately leads to full deployment once all of the bugs have been worked out in the system, the set-top box, the installation process, provisioning, and customer support.

Device testing by itself can fall into one of a number of different testing regimes:

1) Device testing is done as part of system testing described above.

a) Device testing is conducted through a third-party to test compliance with published specifications or standards; examples of third party testing organizations include DLNA, CableLabs, Wi-Fi Alliance, etc. The CableLabs certification process is an example of this type of test regime. The CableLabs certification is described through a set of publicly available guidelines (*http://www.cablelabs.com/wp-content/uploads/2014/01/CWGuidelines.pdf*). The test plans and test tools are available under NDA, and CableLabs offers development lab assistance under which device manufacturers can test their devices before certification submission. CableLabs staff conducts the device testing and reports test results to the device manufacturer. Test errors will be reproduced in the test lab if requested and there is a formal appeal process for pass/fail decisions.

b) Devices are self tested or self certified by the device manufacturer to be in compliance with either published specifications or standards or even proprietary systems.

As mentioned above, the stronger and more thorough the testing regime, the greater the level of confidence in the device's compliance with the functionality and robustness requirements. The testing regimes above move from strongest (device testing as part of system testing) to weakest (self testing). In the case of Uni-Directional Cable Products (UDCP), CableLabs permitted a process that moved from CableLabs validation to one of self-certification.

Testing in Existing Retail Systems

In existing retail systems that are supported by MVPDs today, there are several examples of how app/device testing is applied for these systems:

a) MVPD TV Apps – MVPD TV Apps place much of the burden of testing onto the MVPD and relieve the retail manufacturer of testing their device with every MVPD. The Apps are made available through an App store supported by the retail device manufacturer or their platform partner. These App stores have license conditions, guidelines, and limitations on Apps. The App platform provider reviews these Apps before they are released. Retail manufacturers may also test MVPD TV Apps on their devices to insure they meet platform guidelines.

b) HTML5 Web Apps – HTML5 implementations allow the retail manufacturer to self-test their browser or the browser vendor to self-test its browser on multiple devices. The MVPD can test its Web App on multiple devices. This approach splits the testing burden among all parties.

c) VidiPath/RVU – These make use of third party compliance testing for devices through DLNA and RVU Alliance. The MVPD can test its devices and RUI Apps against certified devices.

Renewability in these systems is achieved through updates to the App, the platform, the Web browser, or the DRM system.

If a retail device connects directly to the MVPD network, it must be tested to assure compliance with requirements similar to those discussed above for MVPD set-top boxes in the sections on SoC and set-top box validation. This verification testing must initially be conducted through an MVPD-approved certification test process. It may be possible to design a self-certification test process for subsequent devices.

B. MVPD Entitlements within the existing MVPD Service

Conditional Access Systems and subscriber Entitlements have always been inextricably intertwined by design. Typical conditional access systems encrypt video content via a 64 or 128 bit number known as a control word (CW). The control word is delivered to a STB as part of the video stream, but in an encrypted form known as an Entitlement Control Message (ECM). It is the principle job of a conditional access system to create these ECMs in a manner such that they cannot be opened by anyone who is not authorized to use them, and to provide the set top with a process to open them when they are authorized. The STB has a mechanism to retrieve the ECM from the video stream, but the STB will still need special authorizations enabling that STB to decrypt the ECM and thus decrypt the MPEG video. For this, the CAS system creates a unique message known as an Entitlement Management Message (EMM) which is targeted to a specific STB and typically delivered outside of the video stream. Every STB in a video network will be sent EMMs that only that box can open and use to decrypt video that has been purchased by that subscriber. The generation of an EMM for a specific STB begins with an authorization delivered from the billing system when a service, such as 'Discovery Channel', is purchased by a subscriber. When an EMM is received by the STB, it will open the EMM using its hardware Root of Trust as a decryption key. That will produce the key to decrypt the ECM, which is opened by the STB. That produces the CW that is used to decrypt the video.

Video is often delivered with certain information denoting rights to copy. Most commonly, this is via a convention known as Copy Control Information, or CCI for short. The CCI is a one byte flag included in video streams that allows content owners as well as distributors to specify how content can be duplicated. Some of the common settings for the CCI field include copy freely (content is not copy protected), copy no more (no more copies permitted), copy once, and copy never (may be recorded but is not transferable). This provides a high level, albeit weak mechanism to convey certain embedded entitlements that go along with content. Typical DRM (digital rights management) systems have an ability to provide more advanced entitlement mechanisms and a rich rights expression language that can convey more extensive and variable access, copying, distribution, and usage rights.

For compatibility with a legacy video system that utilizes QAM transmission and distribution, CPE devices must contain SoCs (system on a chip) that embody certain embedded functions. This includes the notion of a hardware root of trust, which is a unique identifier that is placed in a 'one time programmable' (OTP) location on the SoC. The unique number for each STB is generated by a Trust Authority and injected into the OTP slot using a process jointly defined by the Trust Authority and the SoC Vendor. These SoCs must also implement the current decryption algorithms used by US cable operators, which include the DVB Common Scrambling Algorithm (DVB CSA 2) and SCTE-52 with a MediaCipher IV (Initialization Vector).

C. Technical Standards

1. Security Standards

Standards relating to encryption, hashes, and related items

AES	Advanced Encryption Standard	http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf
TLS	Transport Layer Security	https://tools.ietf.org/html/rfc5246
CSA	Common Scrambling Algorithm	http://www.etsi.org/deliver/etsi_TS/103100_103199/103127/01.01.01_60/ts_103127v010101p.pdf
DVB SimulCrypt	Digital Video Broadcasting (DVB);	http://www.etsi.org/deliver/etsi_ts/103100_103199/103197/01.05.01_60/ts_103197v010501p.pdf
FIPS 180-1	Secure Hash Standard	http://csrc.nist.gov/publications/PubsFIPS.html#fips180-4
RSA	Public Key Encryption	http://www.emc.com/emc-plus/rsa-labs/standards-initiatives/public-key-cryptography-standards.htm
SCTE 201	Open Media Security (OMS) Root Key Derivation Profiles and Test Vectors	http://www.scte.org/documents/pdf/Standards/ANSI_SCTE%20201%202013.pdf
SCTE 52	Data Encryption Standard – Cipher Block Chaining Packet Encryption Specification	https://www.scte.org/documents/pdf/Standards/ANSI_SCTE%2052%202013.pdf
DES	DES encryption standard	http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf
ETSI TS 103 162 V1.1.1 (2010-10)	Access, Terminals, Transmission and Multiplexing (ATTM); Integrated Broadband Cable and Television Networks; K-LAD Functional Specification	http://www.etsi.org/deliver/etsi_TS/103100_103199/103162/01.01.01_60/ts_103162v010101p.pdf
DTCP/IP	DTCP/IP	http://www.dtcp.com/specifications.aspx

2. Networking and Communication Standards

Standards relating to communication and transmission to and inside homes.

_802.11	Wireless LAN Standards	http://standards.ieee.org/about/get/802/802.11.html
ATSC for OTA tune	Off the Air	http://atsc.org/standard/a72-parts-1-2-and-3/
Bluetooth	Bluetooth Core Version 4.2	https://www.bluetooth.org/DocMan/handlers/DownloadDoc.ashx?doc_id=286439 https://www.bluetooth.org/en-us/specification/adopted-specifications
DTCP CVP-2	DTCP CVP-2	http://www.dtcp.com/documents/dtcp/20150309-dtla-cpv2-v1-rev-1-1.pdf
DIRECTV (legacy DSS) transport	International Telecommunications Union, Recommendation ITU-R BO.1516, 2001, "Digital multiprogramme television systems for use by satellite operating in the 11/12 GHz frequency range, System B"	https://www.itu.int/dms_pubrec/itu-r/rec/bo/R-REC-BO.1516-0-200104-S!!PDF-E.pdf
DLNA	DLNA	http://www.dlna.org/guidelines/
DSG	DOCSIS Set-top box gateway	http://www.scte.org/documents/pdf/standards/ANSI_SCTE%20106%202010.pdf
DVB-S, DVB-S2	Satellite broadcasting standard	https://www.dvb.org/standards/dvb-s2
Ethernet	Ethernet networks standards	https://standards.ieee.org/about/get/802/802.3.html
HDMI	HDMI	http://www.hdmi.org/manufacturer/specification.aspx
MoCA	Multimedia over Coax	http://www.mocalliance.org/
RVU	RVU Alliance	http://rvualliance.org/specification-availability
SCTE-55	Legacy Out of Band (OOB) communications	http://www.scte.org/documents/pdf/standards/SCTE%2055-1%202009.pdf
UHD Alliance	documents (available in a few months)	http://www.uhdalliance.org/
UPnP	Universal Plug and Play	http://upnp.org/specs/arch/UPnP-arch-DeviceArchitecture-v1.1.pdf
USB	Universal Serial Bus	http://www.usb.org/developers/docs/

3. Encoding Standards

Standards used for digitally encoding audio and video

AAC	Information technology -- Generic coding of moving pictures and associated audio information -- Part 7: Advanced Audio Coding (AAC)	http://www.iso.org/iso/iso_catalogue/catalogue_ics/catalogue_detail_ics.htm?csnumber=25040
DASH	MPEG-DASH Profile for Transport of ISO BMFF Based DVB Services over IP Based Networks	https://www.dvb.org/resources/public/standards/a168_dvb-dash.pdf
Dolby Digital	Audio format	http://www.dolby.com/us/en/technologies/dolby-digital-plus.html
H.264/AVC	H.264	http://www.itu.int/rec/T-REC-H.264-201402-I/en
H.265/HEVC.	HEVC	http://www.itu.int/rec/T-REC-H.265-201504-P/en
HLS	Apple adaptive bit rate streaming	https://github.com/winlinvip/simple-rtmp-server/blob/master/trunk/doc/hls-m3u8-draft-pantos-http-live-streaming-12.txt
ISO/IEC 13818-1:2015	Information technology, Generic coding of moving pictures and associated audio information: Systems	http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=67331
MPEG-1,2, DASH, TS	MPEG Specifications	http://mpeg.chiariglione.org/standards
MPEG-2 Transport	Specification for the MPEG Transport format	http://www.etsi.org/deliver/etsi_ts/103100_103199/103197/01.05.01_60/ts_103197v010501p.pdf
HTTP Live Streaming	HTTP Live Streaming, IETF Internet-Draft	https://tools.ietf.org/html/draft-pantos-http-live-streaming-16
Microsoft DLNA Extensions	Digital Living Network Alliance (DLNA) Networked Device Interoperability Guidelines: Microsoft Extensions	http://download.microsoft.com/download/9/5/E/95EF66AF-9026-4BB0-A41D-A4F81802D92C/[MS-DLNHND].pdf

4. Service Standards

Standards used for the delivery of MVPD services, and to comply with regulatory requirements

RRT	U.S. Region Rating Table (RRT)	https://www.ce.org/Standards/Standard-Listings/R4-3-Television-Data-Systems-Subcommittee/CEA-766-C-(ANSI).aspx
VBI Data	VBI Data in Cable Digital Transport Streams	http://www.scte.org/documents/pdf/Standards/ANSI_SCTE%2021%202012.pdf
CALM act	ATSC Recommended Practice: Techniques for Establishing and Maintaining Audio Loudness for Digital Television (A/85:2013)	http://atsc.org/wp-content/uploads/2015/03/Techniques-for-establishing-and-maintaining-audio-loudness.pdf
CEA-608-E	Line 21 Extended Data Services, Closed captioning	http://www.ce.org/Standards/Standard-Listings/R4-3-Television-Data-Systems-Subcommittee/Line-21-Data-Service.aspx
CEA-708-E	Digital Television (DTV) Closed Captioning	http://www.ce.org/Standards/Standard-Listings/R4-3-Television-Data-Systems-Subcommittee/CEA-708-D.aspx
EME	Encrypted Media Extensions	http://www.w3.org/TR/encrypted-media
PSIP	ATSC A/65 Program and System Information Protocol (PSIP) for Terrestrial Broadcast and Cable	http://atsc.org/wp-content/uploads/2015/03/Program-System-Information-Protocol-for-Terrestrial-Broadcast-and-Cable.pdf

5. Other

Miscellaneous Standards

OATC	"Open Authentication Technology Committee"	?
PNG	Portable Network Graphics (PNG) Specification	http://www.w3.org/TR/PNG/
RF4CE	ZigBee RF4CE Specification	https://docs.zigbee.org/zigbee-docs/dcn/09/docs-09-5262-01-0rsc-zigbee-rf4ce-specification-public.pdf

D. Existing Security Solutions Survey Results

Survey Question	AltiCast	ARRIS	Broadcom	Cisco	DTA Security	Intel	Nagra	OMS	Verimatrix
1. Name of the solution and brief overview	AltiProtect	SecureMedia™ Encryptonite	Broadcom	VideoGuard™	DTA Security	Intel SGX Technology	NAGRA anyCAS	Open Media Security	VCAS
2. Features/functions of the downloadable security solution:									
2.a. Security functions:									
2.a.i. Does the solution provide conditional access functions (e.g. this service not authorized for this user)?	Yes	Yes	Yes	Yes	Yes	Supports the trusted implementation of conditional access systems, but it is not itself a conditional access system.	Yes Supports complex MVPD marketing rules & needs	Yes	Yes

Survey Question	AltiCast	ARRIS	Broadcom	Cisco	DTA Security	Intel	Nagra	OMS	Verimatrix
2.a.ii. Does it provide DRM services (e.g. this content can be viewed for 90 days)?	Yes	Yes	Yes	Yes	No	Supports DRM systems but is not itself a DRM system.	Yes Supports complex Content Use Cases	currently being developed in labs.	Yes
2.a.iii. Does it provide link protection across digital interfaces between separate devices?	Yes	Yes	Yes	Yes	Passes CCI	Can support link protection technologi es but does not itself provide link protection . iv. Does it provide watermar king or fingerprint ing, device and user authentica tion, or system	Yes DRM, PRM, DTCP-IP and others	as defined by the MPVD's content and technolog y license	Yes

Survey Question	AltiCast	ARRIS	Broadcom	Cisco	DTA Security	Intel	Nagra	OMS	Verimatrix
						renewability? ISVs can include these functions in their own applications.			
2.a.iv. Does it provide watermarking or fingerprinting, device and user authentication, or system renewability?	Yes	third party watermarking systems	Yes	Finger printing supported, work with 3rd-party watermarking	Device Auth & System Renewability - Yes, all others No	ISVs can include these functions in their own applications.	Watermarking is implemented using outsourced technology however standards are not agreed and no one wants to pay. Nagra supports user authentication and	no specific watermarking or fingerprinting	Yes, Verimatrix is a pioneer in forensic watermarking; Verimatrix performs device authentication, supports user authentication by the MW or App, and supports

Survey Question	AltiCast	ARRIS	Broadcom	Cisco	DTA Security	Intel	Nagra	OMS	Verimatrix
							renewability		system renewability in a final integrated system
2.b. Network support:									
2.b.i. What kinds of networks (DBS, HFC, FTTH) are supported?	1-way & 2-way	2-way	support satellite, cable and IP	All major MVPD delivery networks	1-way HFC only	SGX is network agnostic.	All Plus terrestrial ATSC M/H, DVB-H, DMB….	2-way	All major networks and more (e.g., existing worldwide DBS, cable, and telco 1- & 2-way networks, unmanaged IP (OTT), and adaptable to new networks)
2.c. Services and Device Functions:									

Survey Question	AltiCast	ARRIS	Broadcom	Cisco	DTA Security	Intel	Nagra	OMS	Verimatrix
2.c.i. What content services are supported (e.g., live TV streams, file based VOD, progressive download VOD, pay per view, or download-rental)?	All	All	All types	All types	Linear only	Depends on the ISV application, but all can be supported.	Yes to all listed use cases and many more	All	All types (as specified by content distribution agreements)
2.c.ii. What consumer device features are supported (e.g., local recording, digital output control, whole-home streaming, out of home streaming of content)?	A full suite of consumer device features	NPVR, local PVR in home and out of home streaming	All types	All types	CCI and DTCP-IP only	Depends on the ISV application, but all can be supported.	Yes including secure removable storage, place shifting, download to go or sideloading, transcoding, expiration enforcement, Enforcement of	All	All types

Survey Question	AltiCast	ARRIS	Broadcom	Cisco	DTA Security	Intel	Nagra	OMS	Verimatrix
							number of streams or copies…		
2.d. Device support:									
2.d.i. What are the target consumption devices? Does the system work only on special-purpose, operator managed devices like set-top boxes, or on generic consumer devices like tablets?	both operator-managed devices and consumer devices	both operator-managed devices and consumer devices	Broadcom chipsets have been designed so that they can technically serve a wide variety of devices	Popular devices including Windows PCs, Macs, Apple iOS devices, Android devices, Windows 8 RT/Phone devices, HDMI Dongles, Samsung Smart TV, Roku, PS3/4 and Xbox One	Various DTAs only	Devices with Intel processors including set top boxes, residential gateways, PCs, tablets, and smart phones.	All Devices: STB, Tablet, Phone, USB/HDMI dongles, SmartTV Regular TV Managed, Unmanaged PC. iOS, Windows, Android, MacOS	OMS defines SoC and keying requirements	All device types, including both operator-managed devices and consumer devices. MultiRights approach provides full flexibility in this regard.
2.e. Application support:									

Survey Question	AltiCast	ARRIS	Broadcom	Cisco	DTA Security	Intel	Nagra	OMS	Verimatrix
2.e.i. Does the system present APIs to independent (i.e., not from or controlled by the security provider) applications, for example APIs for service information, authentication status, emergency alert messages, closed captioning information, copy control information?	APIs to verify authorization and enable purchases	API's vary by system	support various APIs	Open APIs (e.g., authentication and authorization copy control) are available for integration of Video Guard with TV Applications	No APIs are presented from the system	Can support whatever the ISV application presents.	Yes, many different API's depending on system and needs	OMS defines APIs that are required to deliver the service provider's service	Client and server-side APIs are published and licensable.
3. Components of the solution									
3.a. Software									

Survey Question	AltiCast	ARRIS	Broadcom	Cisco	DTA Security	Intel	Nagra	OMS	Verimatrix
3.a.i. What parts of the solution are downloadable as software?	CAS and DRM client modules	Entirely software solution	All other than first stage bootloader and loader	Supports fully downloadable security solutions where both DRM and CA components are implemented as downloadable software	The conditional access client is downloaded as software	ISVs build their own SGX enabled applications using an SGX SDK.	All of the software components	software environment, HTML5 applications, and a CAS client	Both CAS and DRM clients are downloadable.
3.a.ii. What is the secure software execution environment (execution environment framework, OS, etc.)	a variety of Trusted Execution Environments, including TrustZone	Work with whatever is available	a separate, self-contained, security processor is required to meet all the security requirements and	iOS (5.1 and above), Android (4.X and above), Windows 8 RT, Windows XP SP3 and above (XP SP3 /	secure portion of the SOC	SGX creates HW level robust trusted execution environment.	Various, Depends on device/processor and available resources	OMS does not define a full software environment	TrustZone/ TEE or dedicated security processors, or hardened OS.

Survey Question	AltiCast	ARRIS	Broadcom	Cisco	DTA Security	Intel	Nagra	OMS	Verimatrix
			robustness rules	Vista / 7 / 8 / 8.1), Windows 8, Mac OS 10.6 and above, IE 9.0 and above, Firefox 17.0 and above, Chrome 24.0 and above, Safari 5.1.7.					
3.a.iii. How is code verified, updated? Structure of signing keys and of download images	using Application upgrade protocol	Custom protocol makes use of a SW authentication key which is verified in the first steps of registration and	Security processor is used to verify and renew the SW and FW	All client device software is validated before being run using asymmetric cryptography for	authenticated according to CAL and Cisco licensing materials	Structure of signing keys and of download images SGX verifies the integrity of code to be	Code verified using classical authentication procedures	OMS defines the OTP hardware root of trust	SW is signed (and encrypted) and verified during secure boot process. OTA upgrades

Survey Question	AltiCast	ARRIS	Broadcom	Cisco	DTA Security	Intel	Nagra	OMS	Verimatrix
		authorisation. Additionally code signing is employed on platforms where it is supported. As an example, iOS and Android products load images via their respective store in accordance with their required protocol		security		executed in its trusted execution environment and is able to attest to its validity to remote servers.			are also signed and optionally encrypted.
3.a.iv. Software Roll back support? Roll back	Yes	Yes	Security processor is used	Software download and rollback	Yes	This depends on the ISV applicatio	Yes	Not currently	Yes. client-based or enforced

Survey Question	AltiCast	ARRIS	Broadcom	Cisco	DTA Security	Intel	Nagra	OMS	Verimatrix
management				infrastructure are dictated by the specific application download environment		n.			by the head-end.
3.a.v. In what format are Application interfaces provided?	APIs to verify authorization and enable purchases	http / XML or C or JNI or JAVA or objective C	provide specification/tools to help the security partners and/or OEMs to verify, renew and revoke SW and FW	C, Java, JS, Objective C, http/JSON SDKs are available for application integration partners.	APIs are defined by the SOC vendor	Not applicable.	XML, HTML, JAVA, C and other	set of APIs that allow support of the MVPD HTML5 application	C/C++ APIs on the client side; SOAP and HTTPS server interfaces.
3.b. Hardware									

Survey Question	AltiCast	ARRIS	Broadcom	Cisco	DTA Security	Intel	Nagra	OMS	Verimatrix
3.b.i. What is required on the physical platform (e.g. secure key bundle at manufacturing, Trusted Execution Environment, one-time programmable memory, cryptographic functions in hardware)?	dependent on target security requirements	No specific hardware or CPU architecture required	10 Specific HW features	The Key Ladder in the SoC forms the core of the content security system in the set-top box.	The SOC must support specified key ladders.	Intel processor with SGX support.	All listed are preferred by Nagra and typically mandated by most content owners for high value content. Also Secure Key Ladder	OMS requires the implementation of a SoC with a secure processer that conforms to robustness rules defined by OMS	Personalized SOCs (including 3rd party Trust Authority), certified TEE, code/app signature verification, etc. (Depends on device type)
3.b.ii. Process description of how devices, SoCs, and CAS gain access to secure key elements	Access to secure elements is provided through low-level APIs.	implemented on a case by case basis, hw support where available	1) Non-Modifiable OTP key/IDs 2) Root Key Derivation 3) Content key derivation /Key	Leverages the standard OMS ecosystem for acquisition of all secure key elements.	Robustness rules and compliance requirements are specified in CAL and Cisco licensing materials.	See intel presentation	Via secure key ladder	OMS allows for a Trust Authority to create keys	Verimatrix-provisioned/personalized SOCs using Verimatrix or 3rd party TA blackbox; or access to TEE keys.

Survey Question	AltiCast	ARRIS	Broadcom	Cisco	DTA Security	Intel	Nagra	OMS	Verimatrix
			ladder						
3.b.iii. Is there a specific CPU or CPU architecture required? If so, which one(s)?	No	No	No, should be left up to the SOC designers	DRM system works across a wide range of CPUs include x86 and ARM.	No specific CPU or CPU architecture is required.	Intel Architecture.	MANY, DEPENDS ON DEVICE, The more secure the better but can be made to work at some level of security on most	No specific CPU or SoC architecture is defined by OMS	No specialized CPUs are required

Survey Question	AltiCast	ARRIS	Broadcom	Cisco	DTA Security	Intel	Nagra	OMS	Verimatrix
3.b.iv. What happens if some physical elements are not present?	A subset of services can be provided depending on robustness of device.	Dependent on content license	It will depend on the content protection policy	Designed in a modular fashion to support and where necessary to compensate for varying degrees of physical hardware security.	They may not receive certain content if they do not have certain capabilities.	Trusted Execution Environment using SGX is not possible.	Can be Emulated in SW, BUT may have significant reduction in security guarantees and may require waivers from content owners	The full security chain is required for use of OMS solutions	Some critical security features must always be present. Different levels of protection available depending on content type (e.g. HD vs. UHD).
3.b.v. How are robustness rules and compliance rules on hardware defined? Who defines them? What are these rules? How are they enforced?	dependent on service and content provider requirements	Robustness rules are defined in the content license.	defined by security architects, like CA/DRM vendors	Cisco security experts are responsible for identifying threat criteria and dynamically updating	The SOC and DTA device go through a validation process to ensure they comply with the license and robustnes	SGX is a technology that ISVs use to meet various robustness rules. With respect to SGX itself, Intel defines	Very Stringent Defined by Nagra in conjunction with content owners Enforced by Nagra and third party	OMS defines the Robustness and Compliance rules	Compliance and Robustness Rules are published by Verimatrix in collaboration with content owners

Survey Question	AltiCast	ARRIS	Broadcom	Cisco	DTA Security	Intel	Nagra	OMS	Verimatrix
				Cisco's own internal robustness and compliance criteria for hardware, software, networks, and operating environments.	s rules.	rules for keeping secrets. They are enforced through bilateral contracts.	audit		
3.b.vi. Are there any execution environment restrictions (e.g., any other applications must be tested and/or signed by the security solution or operator).	Execution environment must meet robustness requirement.	Robustness rules are defined in the content license.	all SW/FW should be verified. All platform and 3rd party code should be HW isolated from critical security code, and	Downloadable CA should be signed by Cisco or operator	This is covered under the CAL and Cisco licensing materials.	There are some memory usage limitations in the current version of SGX.	Yes, Code run in TEE or secure processor is fully vetted. Depending on processor architecture other processes may need to be	OMS requires the validation of the CAS Client APIs as well as the Application APIs.	Dependent on client device type, a certified TEE is desirable.

Survey Question	AltiCast	ARRIS	Broadcom	Cisco	DTA Security	Intel	Nagra	OMS	Verimatrix
			not rely on SW isolation mechanis ms				vetted		
3.b.vii. Are independent third-party applications supported, that don't require verifications/ce rtification from the CAS supplier?	Yes	Platform specific.	a secure scheme that can separate the trusted applicatio ns from the non-trusted applicatio ns should be required based on fully isolated hardware	The entity that controls or manages a device is responsibl e for certificati on of third-party applicatio ns download ed to a device.	Independ ent, third-party applicatio ns are not supported .	YES	Depends on processor architectu re and partitionin g	The full security chain is required for use of OMS solutions	Application s must abide by integration complianc e and robustness rules or must be completely sand-boxed away from CA/DRM.

Survey Question	AltiCast	ARRIS	Broadcom	Cisco	DTA Security	Intel	Nagra	OMS	Verimatrix
3.b.viii. Are there third party, independent lab testing and certification options?	No	Yes	Yes	Technology is periodically subject to third-party audits and evaluations, as requested or required by commercial agreement.	DTA SOCs and DTAs are validated by Arris/CCAD and Cisco/Itaas	Not applicable.	Yes	OMS validates solutions.	Yes, e.g. Riscure for SOCs and TEE certification by GlobalPlatform approved test labs.
3.c. Device identification and Keying									
3.c.i. Secure mechanisms for identification of devices in the network.	Yes	Platform dependent	This is a MUST for anti-cloning.	Utilizes a common secure channel for identification of all VideoGuard clients	The DTA's network identity is created at time of SOC manufacture as part of the	SGX uses provisioning and attestation (see presentation) to verify genuine	Yes Essential	The OMS defined Root of Trust is a key residing on the SoC, and is	Immutable SOC IDs; MAC addresses, device ID, HW fingerprint, and unique device

Survey Question	AltiCast	ARRIS	Broadcom	Cisco	DTA Security	Intel	Nagra	OMS	Verimatrix
				on the network	keying process	Intel processor and SGX enclave.		accessible by the KLAD key ladder.	certificates .
3.c.ii. Serial number/unique identification requirements	Yes	not required, but may be used if present	Non-Modifiable OTP IDs can be readable by host ACPU	There are no specific identification requirements dictated by VideoGuard	Serial number is added at device manufacture time.	Requires genuine Intel processor with SGX technology. These properties are remotely attestable .	Yes	OMS defines the specification for serialization and keying of SoCs.	Unique SOC IDs, typically programmed in OTP during the SOC personalization process, or unique device ID (and optionally keys) accessible in TEE.

Survey Question	AltiCast	ARRIS	Broadcom	Cisco	DTA Security	Intel	Nagra	OMS	Verimatrix
3.c.iii. Keys, key storage capabilities	Yes	WBC or secure storage or simply encrypted storage if secure environment	Non-Modifiable OTP keys cannot be readable by host ACPU.	Downloadable clients work with device OS to ensure reliable access to persistent memory	APIs are provided by the SOC vendor	SGX can securely store an Application's keys by cryptographically sealing them to the processor.	Yes Essential	OMS defines OTP keys to use with the KLAD mechanism	Asymmetric verification keys (secure boot); Device unique symmetric OTP keys
3.c.iv. Is there a standardized mechanism for communication with SoC and other hardware elements?	Yes	No	We are not aware of any standardized scheme.	ETSI, SCTE and OMS all provide standards		SGX uses provisioning and attestation to enable ISV application to set up trusted execution environment.	No Only frameworks	OMS defines a CAS Client API	Verimatrix-defined HW Key Ladder abstraction layer implemented by many SOC vendors; or OMS/KLAD APIs.
3.d. Key server/client communication path and network									

Survey Question	AltiCast	ARRIS	Broadcom	Cisco	DTA Security	Intel	Nagra	OMS	Verimatrix
3.d.i. Is a two-way communication path required? Does it need to be full-time connectivity?	Two-way comm path required, but full-time connectivity not mandatory	Intermittent 2 way connectivity required	Certain STB features may require bi-directional communication	Provides multiple solutions for one-way and two-way environments	The DTA is a one-way device per FCC requirements	Setting up a trusted execution environment using SGX requires provisioning and attestation, which can be performed one time using bi-directional communication with a server via the Internet.	No, Helps security of present	OMS requires two-way connectivity at any time that a digital device is attached to the network	No, adapted to network type (1-way or 2-way)

Survey Question	AltiCast	ARRIS	Broadcom	Cisco	DTA Security	Intel	Nagra	OMS	Verimatrix
3.d.ii. Must it be a secure channel or is an open unsecure channel supported (e.g., by encryption that is part of the system)? Does the channel use IP or proprietary protocols? DSG or other network specific technologies?	Secure channel is needed and is used on IP or proprietary network protocols.	ESAM protocol is application level protocol	Require secure channel to perform authentication and key exchange, defined by CAS/DRM vendor	Operates within completely managed as well as completely unmanaged networks	in-band proprietary messaging	This is up to the ISV application. SGX provisioning and attestation requires an internet connection on set up.	The channel runs over a potentially open network using well known IP and RF protocols. Where necessary the messaging is secured	Defined by CAS provider	VCAS provides its own secure key management protocol based on standards such as TLS and X.509.
4. Technical Capabilities									
4.a. What media transport formats supported (e.g., MPEG-2 Transport Streams, ABR/HLS, ISO BMFF)?	All	MPEG2-TS for IPTV, HLS for OTT, mp4 offline playback, ISO-BMFF being added	can support a lot of container formats and codecs	MPEG-2 Transport Streams, ABR/HLS, HSS and MPEG DASH	MPEG-2 and MPEG-4	SGX is format agnostic. Intel graphics support a wide range of media formats.	All	OMS is agnostic to the transport stream	All; VCAS is as video encoding and file/transport format independent

Survey Question	AltiCast	ARRIS	Broadcom	Cisco	DTA Security	Intel	Nagra	OMS	Verimatrix
4.b. What content delivery networks are supported (e.g., HFC QAM, DBS, IP unicast, IP multicast)?	1-way & 2-way	All two way networks.	Different BRCM STB chipsets can support satellite, cable and IP markets.	HFC QAM, DBS, IP unicast, IP multicast	Only HFC is supported.	Network agnostic.	ALL Plus Terrestrial Broadcast ATSC M/H, DVB-H, DMB etc	OMS can support any two way network	All are supported.
4.c. Is Network information conveyed and required (e.g. DVB-SI, SCTE 65, etc.)?	Yes	Not for decrypt	STB chipsets can filter different network information	Network and System information are not conveyed or required	SCTE-65 on the in-band channel	Not required. Depends on specific ISV application.	DVB-SI and SCTE 65 helpful on broadcast networks. Not needed for DRM use cases	Yes	Yes, a minimal subset of SI information is required for use by VCAS
4.d. What encryption standards used (e.g., which ciphers, and is there support for legacy deployed systems such as DVB-CA, SCTE	A range of ciphers and key lengths are supported	System dependent	DVB-CSA2, DVB-CSA3, AES, 3DES and DES	including, but not limited to: DVB-CSA2, AES-CBC, DVB-CSA3, DVB-CPCM,	DES-CBC as defined in SCTE-52 or proprietary DES-CTS or DVB-CSA	SGX is not an encryption technology. Can support whatever the ISV applicatio	All, Relatively agnostic - encryption and decryption typically done by secure processor	OMS can be deployed on CSA and SCTE-52 networks	All can be used; typically AES128 is used, however, specific content encryption is not

Survey Question	AltiCast	ARRIS	Broadcom	Cisco	DTA Security	Intel	Nagra	OMS	Verimatrix
55, etc.)?				ATIS-ISSA, ARIB, SCTE-55 and MPEG CENC		n supports.	in CAS and some DRM deployments		required by VCAS
4.e. What are the application APIs to the CAS/DRM client? (e.g., what are the API interfaces between the device software and the CAS/DRM software for requesting content decryption, and querying entitlements defining the associated content such as DVR recording, home streaming, and	Basic APIs for requesting content decryption and querying entitlements	API's vary by system	ECM/EMM or DRM license filtering/parsing	Open APIs for querying viewer rights and activation content decryption	The APIs to the CA client are supplied by the SOC vendor.	These are determined by the application.	Many	OMS APIs define the interfaces used by the CAS client	Verimatrix publishes a CAS/DRM client API for 3rd party middleware/application/player integrations.

Survey Question	AltiCast	ARRIS	Broadcom	Cisco	DTA Security	Intel	Nagra	OMS	Verimatrix
for how long or how many copies.)									
4.f. Network identification, access and attachment requirements APIs?	Authentication APIs are supported.	no dependence on network identification	Depend on each security partners.	Network attachment APIs are defined by the MVPD	Host requirements are via SOC-defined APIs	These are determined by the application.	-	OMS defines these	Provisioning APIs are provided by the CAS client.
5. Standards Used in the System									

Survey Question	AltiCast	ARRIS	Broadcom	Cisco	DTA Security	Intel	Nagra	OMS	Verimatrix
5.a. What standards (i.e., non-proprietary technical standards promulgated by government or private standards defining organizations) are used in the system?	JCAS, NCAS, XCAS/iCAS, and others	Pantos/AES for OTT, MPEG2-TS AES/CSA, TLS, RSA, SCTE-52	DTCP-IP, HDCP1.4, HDCP2.2, MPEG CAS, etc.	DVB SimulCrypt, DVB CSA and CPCM encryption ciphers, ATIS encryption ciphers, ETSI and SCTE OMS key ladder	• ATSC A/53, MPEG-2 and MPEG-4: Video Transport • SCTE-65: Network Information • SCTE-18: Emergency Alert Messages • SCTE-20, CEA-608 and CEA-708: Closed Captioning • OpenCable Common Download Specification:	SGX is an Intel proprietary technology.	SCTE, DVB, ETSI, MPEG, ATSC, DLNA, AES	SCTE-52, DVB Simulcrypt, DVB CSA, KLAD (ETSI and SCTE 201)	MPEG, DVB, SCTE, ETSI, OIPF, EITF, W3C, DLNA, OMS, GlobalPlatform, DASH-IF, etc.

Survey Question	AltiCast	ARRIS	Broadcom	Cisco	DTA Security	Intel	Nagra	OMS	Verimatrix
					firmware download				
5.b. Describe plans (if any) related to how the security system works with W3C	Alticast HTML5 Browser supports EME.	Active program underway	Different DRM technologies with EME	Working with a number of browser vendors to	There are no current plans to use DTA with W3C EME	SGX can support any application, including	In Development	No	W3C EME is supported where applicable.

Survey Question	AltiCast	ARRIS	Broadcom	Cisco	DTA Security	Intel	Nagra	OMS	Verimatrix
Encrypted Media Extensions (EME).				implement the VG Everywhere CDM (Content Decryption Module) in support of EME		those with EME.			
6. Deployment Model									
6.a. Does the solution require the operator to deploy a new transmission network or leverage existing ones?	Leverage existing.	Use existing.	N/A	Should not require the deployment of new transmission networks	Existing HFC Networks	Up to the operator/ISV. Can leverage existing ones.	EITHER	OMS is designed to work with legacy cable deployments that have been enhanced to support DVB Simulcrypt	Existing networks supported.

Survey Question	AltiCast	ARRIS	Broadcom	Cisco	DTA Security	Intel	Nagra	OMS	Verimatrix
6.b. What are the largest cost elements for an operator to deploy (new equipment, upgrades, network changes, swap out older equipment)	Highly operator-dependent.	No special hardware necessary	N/A	Cost of operating the new security solution alongside the legacy ones	The operator will have to modify or install new systems		Deploying a new security system. This assumes existing STB 's can be re-used or continue to co-exist	replacement or upgrade of all encryption devices, conversion to DOCSIS out-of-band, new CAS system and CAS controller, integration with legacy CAS Controllers, and integration with Billing	Highly operator dependent, however Verimatrix strives to provide standards-based solutions to minimize such costs.
6.c. Co-existence with legacy CAS systems, or modification required, or	Completely independent, coexists with	SimulCrypt	N/A	SimulCrypt and Simulcast modes, Sony Passage	coexist with both the ARRIS and Cisco	Can be whatever the ISV wants its application to be.	Either, Have deployed simulcast and simulcryt	The OMS system can exist with legacy CAS Systems.	Simulcrypt with legacy CAS systems is supported. Simulcast

Survey Question	AltiCast	ARRIS	Broadcom	Cisco	DTA Security	Intel	Nagra	OMS	Verimatrix
completely independent (simulcast) solution?	legacy CAS (Simulcrypt)			(partial encryption modes), MultiCrypt modes					is also an option.
7. Intellectual property and licensing regime									
7.a. What elements of the system are currently licensed/licensable on Fair, Reasonable and Non-Discriminatory (FRAND) terms?	Proprietary license.	FRAND to service providers	N/A	Where IP Hooks are recommended for security reasons, such as use of DVB-CSA, intellectual property licenses are generally available from third-parties on FRAND terms.	negotiated between the licensors -- CAL and Cisco -- and their licensees.	Intel will license SGX technology on FRAND terms.	All with exception of proprietary recovery logic used against persistent attack modes	Under development	Both server-side and client-side components are licensed to operators and device manufacturers.

Survey Question	AltiCast	ARRIS	Broadcom	Cisco	DTA Security	Intel	Nagra	OMS	Verimatrix
7.b. What elements (if any) of the system are not currently licensed/licensable under FRAND terms?	None.	Not licensing IP separately	N/A		N/A	SGX is an Intel microprocessor feature and is not licensed for implementation on non-Intel processors.	Recovery Logic included in Nagra NOCS3 key Ladder implementations		Specific elements that should be kept proprietary to diversify security.
7.b.i. Are there any elements that will never be licensed under FRAND terms?	Yes	Not licensing IP separately	N/A	Licensable to Cisco's MVPD customers as Cisco product licenses	N/A	Licensing is limited to applications for Intel processors.		Under development	Certain elements should remain proprietary to diversify security.
8. Porting Issues & Liability									

Survey Question	AltiCast	ARRIS	Broadcom	Cisco	DTA Security	Intel	Nagra	OMS	Verimatrix
8.a. Who does the port?	Alticast.	ARRIS SecureMedia	Either security partner, OEM or Middleware vendor.	Cisco provides support for all ports of the VideoGuard Everywhere clients	The SOC vendor	ISVs license SGX and build their own SGX applications.	Varies Mostly Nagra	device manufacturer	Verimatrix and SOC vendors or 3rd party integration labs.
8.b. How's the port validated?	Trusted Authority.	tested with over 150 different device and OS combinations	May require some forms of certification to validate the end–to-end system.	Cisco provides device and application certification services as dictated by MVPD commercial requirements.	CCAD and Cisco validate SOC requirements, then CCAD and Itaas validate DTA requirements.	Intel uses provisioning and attestation to validate creation of an SGX trusted execution environment.	By Nagra	OMS will define validation procedures	Verimatrix.

Survey Question	AltiCast	ARRIS	Broadcom	Cisco	DTA Security	Intel	Nagra	OMS	Verimatrix
8.c. Who provides indemnification for the ported implementation ?	Dependent on commercial contract terms.	Depends on business arrangement	Whoever is acting as an insurance company in the ecosystem.	Indemnification is a term that is governed by commercial agreement between entities	Indemnification terms are negotiated.	Intel does not indemnify ISVs for use of SGX.	Nagra to MVPD	business agreement between the CAS and Device vendors.	Indemnification is typically negotiated between operators and vendors

Table 21 - Summary of Survey Responses

REPORT OF WORKING GROUP 4 TO DSTAC

Introduction

Working Group 4 (WG4) was formed out of the larger DSTAC to address the topic of device platforms, variability, and interfaces.

Guidance Description

(Part I) The working group will identify existing devices and technologies that receive MVPD and OTT service, such as DVRs, HDTVs, personal computers, tablets in home, connected mobile devices, take-and-go mobile devices, etc., and identify the salient differences important to implementation of the non-security elements of a system to promote the competitive availability of such devices based on downloadable security.

(Part II) For each category of existing device identified above, the working group will identify a system comprising minimum standards, protocols, and information other than security elements to enable competitive availability of devices that receive MVPD services.

(Part III) The working group may identify alternative systems as appropriate to promote the availability of different categories of navigation devices, consistent with the Commission's instruction to recommend an approach that would allow consumer electronics manufactures to build devices with competitive interfaces and an approach under which MVPDs would maintain control of the user interface.

Product

The working group will deliver and present its findings to the full DSTAC.

Table of Contents

Part I: Existing Devices and Technologies 6
Section I: Devices that receive MVPD or OTT service 6
Section II: Technologies (Network) that enable the reception of MVPD or OTT service 6
Operator Network Technologies 6
Home Network Technologies 27
Section III: Technologies (Functional) that enable the reception of MVPD or OTT service: 36
Gateways and MVPD Provided Devices and Environments 36
Application on Retail Device 38
Standalone Retail Devices 40
Section IV: Technologies that enable the reception of MVPD or OTT service: 41
Google Fiber IPTV System Overview 41
Slingbox 42
Mediaroom 42
Section V: OTT Services 42
Section VI: Essential Customer Experiences 43
PURPOSE 43
INTRODUCTION 43
END-USER Precondition: 44
USE CASE #1 - Tuning and Viewing a Linear Channel 44
USE CASE #2 - Viewing On-Demand Content 54
USE CASE #3 - Tuning and Viewing Pay Per View (PPV) events 55
USE CASE #4 - Navigation 56
USE CASE #5 - Recording Linear Content 57
USE CASE #6 - Remote Management by Consumer 57
USE CASE #7 - Set-Top Box set-up 58
USE CASE #8 - Customer Support and Remote Management by Service Provider 59
USE CASE #9 - Installation and Provisioning 59
USE CASE #10 - Device Operation Requirements 60
USE CASE #11 – User Authentication 61
USE CASE #12 – Renewability (DELETED DURING DELIBERATIONS) 62

USE CASE #13 - Cloud VOD Delivery 62
USE CASE #14 - Cloud Live Streaming 63
USE CASE #15 – Cloud DVR Recording and Streaming 63
USE CASE #16 - Cloud Content Downloading for Mobile Devices 64
Part II: Systems that Enable Competitive Availability of Devices 66
Section I: SAT-IP 66
Description 66
Protocols 66
Security 66
Information 66
Section II: CableCARD 67
Description 67
Standards 68
Information 68
Applicable Devices 68
Section III: DRI and OpenCable interfaces (and specifications) 69
Description 69
Protocols 69
Security 69
Information 70
Applicable Devices 70
Section IV: Android/iOS Store Device Architectures from DEVELOPER Point of View 70
Standards 72
Protocols 73
Information 74
Applicable Devices 78
Section V: VidiPath 78
Summary 79
VidiPath Deployment Scenarios 91
Standards 93
Protocols 94

Information 94
Applicable Devices 95
Section VI: W3C HTML5 Web Browser 95
World Wide Web Consortium (W3C) Standards 98
Protocols 99
Information 99
Applicable Devices 99
Section VII: RVU™ 99
Standards 100
Protocols 100
Information 101
Applicable Devices 101
Section VIII: Passage 101
Description 101
Passage Headend Encoding 102
Passage Technology 103
System Architecture 105
Managing Bandwidth 105
Implementations 106
Security 106
Protocols 106
Part III: Alternative Systems that Enable New Categories of Navigation Devices 107
Section I: *"Competitive Navigation"* System 107
Competitive Navigation Device Executive Summary 107
Diversity in Direct Connection Delivery Networks 109
Migration to IP Delivery Underway 110
Limitations of Architectures Thus Far 111
Limitations Where User Experience Is Too Closely Controlled 112
Interfaces Necessary to Enable Competitive Interoperability 113
Physical Interconnection and Basic Networking 115
Service Discovery Interface 116

Entitlement Information Interface 119
Content Delivery Interface 120
Use Case Analysis 122
Closing and Summary 126
Section II: "Application-Based Service with Operator Provided User-Interface" System 127
Introduction 127
Device Specific Apps 130
HTML5 Web Apps 135
DLNA VidiPath™ 138
RVU™ 139
Virtual Joey 139
Sling Media Technology Clients 140
Use Cases Supported 140
Section III: Implementation Analysis 144
Evaluation of "Competitive Navigation" System Proposal by Proponents of Application-Based Service 144
Evaluation of "Application-Based Service with MVPD UI" ("Apps Approach") by Proponents of Application-Based Service 166
Passage to Facilitate Transition to All DRM Approach 174
Policy Analysis by Content Providers 177
Evaluation of Both Proposals by Proponents of "Competitive Navigation" Proposal 178
Part IV: Appendix A: Survey of Existing Devices 201

Part I: Existing Devices and Technologies

"The working group will identify existing devices and technologies that receive MVPD and OTT service, such as DVRs, HDTVs, personal computers, tablets in home, connected mobile devices, take-and-go mobile devices, etc., and identify the salient differences important to implementation of the non-security elements of a system to promote the competitive availability of such devices based on downloadable security."

As most members generally understand the functionality of the devices listed in Part I, it is expected that information would be provided as to how the devices discover and receive content.

As content is coming in on different input ports and through different applications running on the devices, the mechanisms for each are detailed.

Various points have been captured in the table in Appendix A: Survey of Existing Devices.

Section I: Devices that receive MVPD or OTT service

The table in Appendix A serves as a reference for retail and MVPD devices that will interact with content distribution networks, and provides basic descriptions of their functionality. Many of these devices will function as receivers for MVPD/OTT content, and it is important to understand their differences and capabilities for the purpose of establishing standards for the reception and control of video content. All of these devices may connect through disparate network architectures such that protocols for device management and stream management need to be considered and how these devices receive and display content.

Section II: Technologies (Network) that enable the reception of MVPD or OTT service

Discussion of important features of specific technologies

Operator Network Technologies

SUMMARY

As noted in WG2 Report Section III starting on page 3 [45], there is variation in current video providers' distribution technologies and platforms. Across all service providers, an approach that has developed for delivering video service to customer owned devices is through "apps."

Diversity of Access Network Technologies

As noted in WG2 Report in Section III starting on page 4 [45], the larger US Cable operators and Verizon mostly use one or both of two the two primary CAS (Conditional Access Systems) vendors, and all support CableCARD for limited services. Both US Cable and Verizon use Quadrature Amplitude Modulation (QAM) for broadcast signals while over Hybrid Fiber Coax (HFC) or B/GPON (Broadband-/Gigabit-capable Passive Optical Networks) fiber networks. Verizon adds hybrid QAM/IP for on-demand content and two-way services. Direct Broadcast Satellite (DBS) also has two major variants for transport

and CAS. AT&T uses IP unicast and multicast over DSL or B/GPON fiber, with a Digital Rights Management (DRM) approach instead of CAS.

Diversity Of Customer Equipment Installation, Provisioning, And Configuration Methods *Error! Reference source not found.*

The diversity of network technologies across and within MVPDs is associated with a diversity of Customer Premise Equipment (CPE) installation, provisioning, and configuration methods. Table 1 - Diversity of MVPD Customer Premise EquipmentTable 1 shows the equipment necessary for network termination at the premise, the CPE deployed for the Pay TV service and the technologies used for in-home distribution of the service.

MVPD	Network Termination	Customer Premise Equipment (CPE)	In-Home Distribution
Cable	Coax & RFoG Optical Network Termination (ONT)	DVR & Non-DVR set-tops, DTA and Cloud Based systems IPTV Set tops	Cable RF & MoCA Wi-Fi
Satellite	Out Door Unit (ODU) – Satellite Dish Low noise block down-converter (LNB) Multiswitch (RF switching unit)	Genie Server (DVR) & Genie Mini clients Hopper (DVR) & Joey clients	802.11 & MoCA MoCA Wi-Fi
Telco	VDSL Modem or Gateway B/GPON Optical Network Termination (ONT)	DVR & Non-DVR IPTV set-tops	802.11 Cable RF & MoCA Wi-Fi
Google Fiber TV	GPON Optical Network Termination (ONT)	Network Box, Storage Box, TV Box	802.11 & MoCA

Table 1 - Diversity of MVPD Customer Premise Equipment

Cable networks are typically terminated at the house at the point of entry with coax cabling. In some instances cable networks use RF over Glass (RFoG), an analog RF fiber to the premise technology. The

RFoG Optical Network Termination (ONT) converts the optical RF to an electrical RF signal over coax permitting the use of traditional cable QAM based CPE. Cable systems make use of both DVR and non-DVR set-top boxes that receive broadcast signals and use MoCA technology to link them together for a whole home DVR solution.

Satellite networks terminate in Out Door Units (ODU) satellite dishes. Low Noise Block down-converters shift the satellite signals to a frequency band that can be switched by a Multiswitch unit and distributed via coax cables to the various satellite CPE. Satellite systems make use of both DVR and non-DVR set-tops and use both MoCA and 802.11 Wi-Fi for distribution in the home for a whole home DVR solution. The satellite MVPDs also have client software available in some LG, Samsung, Sony and Toshiba TVs that allow them to access services through their home network either using RVU or Virtual Joey technology.

Telco networks are typically either traditional telephone twisted-pair copper or B/GPON FTTP networks. In the case of twisted-pair, the network is terminated by a VDSL modem or gateway in an IPTV solution making use of both DVR and non-DVR IPTV set-tops and use 802.11 Wi-Fi for distribution in the home for a whole home DVR solution. Twisted-pair networks also need a filter installed to block the VDSL signal from telephones in the home. In the case of fiber networks, the network is terminated in an ONT and, in the case of FiOS, the optical RF spectrum is converted to electrical RF spectrum and distributed over coax, similar to the cable RFOG case. Fiber networks may use either Hybrid IP/QAM based set-tops (DVR and non-DVR) and MoCA for distribution in the home for a whole home DVR solution or the same IPTV based set-tops and 802.11 Wi-Fi distribution as in the twisted-pair case. In Hybrid IP/QAM based set-tops, each set-top box includes two interfaces: an interface to the overlay wavelength for linear services and certain control signaling; and an IP interface for IP VOD, widgets, guide data, gaming, and certain control plane signaling. All of these are integrated into a single service within the set-top box.

While all MVPDs would like for consumers to be able to self-install the necessary equipment to receive the MVPD service, this is not always a practical option for a number of reasons. First, if this is the first time a customer has subscribed to an MVPD service, it may be necessary to install the necessary network termination equipment, whether this is a cable drop, a fiber drop and an ONT, a VDSL modem/gateway and filters, or a satellite ODU, LNB, and Multiswitch. In addition to this, it may be necessary to wire the home with coax cable to distribute the signal from the point of entry to the various rooms in which service is desired. Even if the home has been previously wired for cable service, the need to insure that signal levels are appropriate or alignment of the satellite ODU is correct is still required.

Provisioning of set-top boxes also varies across and within MVPDs. There are two basic kinds of provisioning necessary in an MVPD system. The first is network provisioning so that the set-tops are properly connected to the network and can communicate properly. The second is provisioning of entitlements so that subscribers can access the services to which they are subscribed. Network provisioning is typically specific to the type of network and CAS system deployed, while provisioning of entitlements is exclusively the domain of the CAS system deployed. Configuration methods are also specific to the type of network and CAS system deployed.

Common Approaches to Retail Devices

As noted in WG2 Report in Section VI starting on page 12 [45], for some service providers an approach for delivering video service to customer owned devices is through service provider authored or authorized “apps.”

MVPDs are remarkably similar in their approach to supporting retail devices, following the successful model that OTT video distributors such as Netflix, Hulu, and others use.

Cable Technologies and Architectures [46]

Cable systems have evolved over the decades since the first cable systems in 1940s. Most cable operators have upgraded their networks to two-way, Hybrid Fiber Coax (HFC). However, this evolution was not uniform across the United States and there is diversity across cable operators. Figure 33 shows the typical HFC cable network architecture.

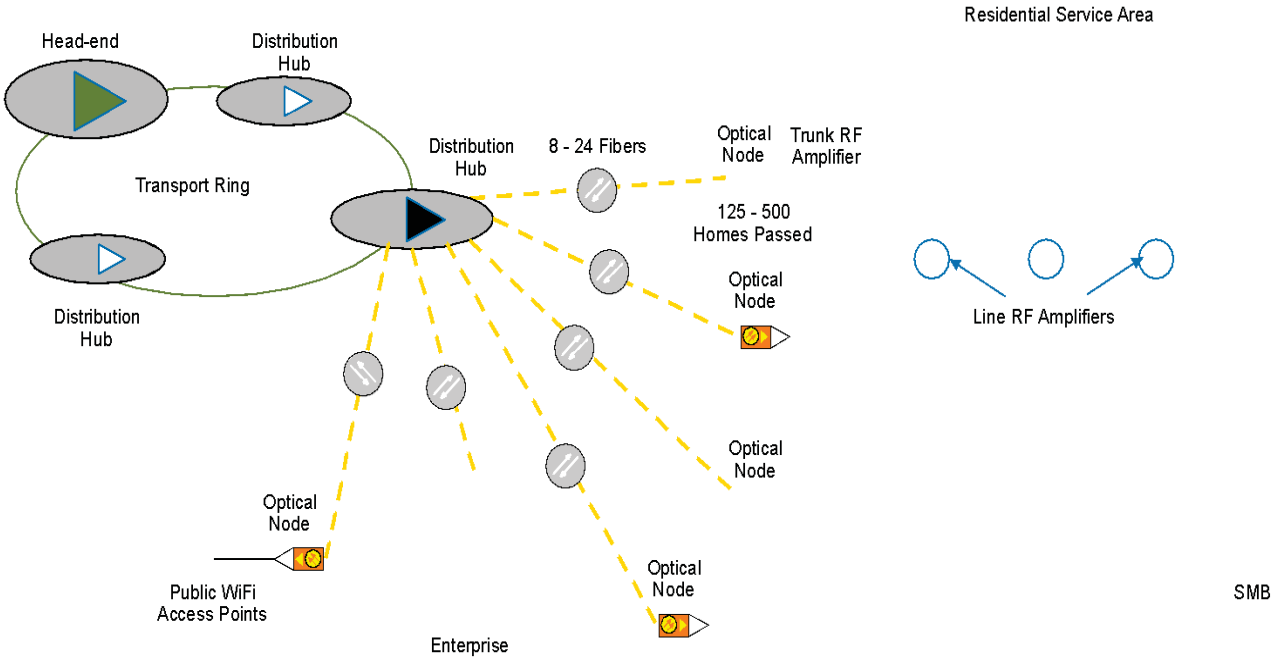


Figure 1 - Typical Cable System Network Architecture

Cable system architectures reflect fundamental differences dating from the original design goals based on different vendors and different owners. The General Instrument (now ARRIS) design was tailored primarily for the more rural and less clustered systems owned by Tele-Communications, Inc., with a focus on increased channel capacity, minimized head-end cost, and centralized set-top control and authorization. The Scientific-Atlanta (now Cisco) design was tailored primarily for the more urban and clustered systems primarily owned by Time Warner Cable, with a focus on two-way interactive services such as Video-on-Demand (VoD), the ability to add applications and services to set-top boxes over time, and local control and authorization. Thus, even though there are some shared elements, such as MPEG-2 video compression, there are fundamental differences in technologies for CAS, controllers, the out-of-band (OOB) communications channels used for command and control of the set-top box, network transports, QAM modulation, video codecs, core ciphers, advanced system information such as network configuration, session management, operating system, processor instruction set, interactive services, billing systems, applications necessary for presentation of services and in the set-top boxes. **Error! Reference source not found.**

The respective design objectives resulted in proprietary systems that had different system architectures and network configurations, as well as different CAS systems, as described above. Despite these different design goals there were also a significant number of common elements:

- The GI and SA systems used MPEG-2 video compression and Dolby® AC-3 audio compression [6][7].
- Both systems have added support for MPEG-4/AVC in the intervening years [8].
- Both systems used QAM modulation for transmission of MPEG-2 transport streams carrying the audio/video signal [9].
- Both systems used variants of Data Encryption Standard (DES-64) [10] encryption as the working cipher for their CA systems and in particular both were capable of supporting the SCTE 52 2008 DES-CBC variant [11].
- Both systems used a common Service Information format to communicate channel line-up information [12].

However, because of the different design goals, there were many proprietary components remaining in each system.

The proprietary aspects of the two systems largely lay in following areas:

- The CAS system (DigiCipher™ II in the case of GI and PowerKey™ in the case of SA) used to control subscriber entitlements and manage access to digital channels.
- Their out-of-band (OOB) communications channels used for command and control of the set-top box:
  - GI's system implemented the DigiCipher II OOB utilizing an MPEG structure for transporting OOB messaging downstream, standardized as ANSI/SCTE 55-1 2009 [13]. The GI OOB channel provided 2Mbps downstream bandwidth and 256Kbps upstream bandwidth through an Aloha, polled communication protocol.
  - SA's system implemented a DAVIC based OOB utilizing an ATM/IP structure for transporting OOB messaging downstream, standardized as ANSI/SCTE 55-2 2009 [14]. The SA OOB channel provided 1.5 Mbps bandwidth in both the downstream and upstream using a real-time, two-way protocol.
- Operating system (OS) and processor instruction set:
  - GI's system initially implemented a proprietary kernel on a Motorola 6800 processor instruction set.
  - SA's system initially implemented the PowerTV™ OS on a Sun SPARC™ processor instruction set.
  - Subsequently, both system providers have introduced other OS (e.g. Linux) and processor instruction sets (e.g. MIPS).
- Network control architecture in support of interactive applications, such as VoD and Switched Digital Video (SDV):
  - GI's network control architecture lacked the concept of an interactive session manager, requiring third-parties to provide this component when integrating session-based services, such as VoD.
  - Interactive network functions such as Switched Digital Video have been implemented using external controller platforms, available from 3rd parties or directly from ARRIS (Vertasent and BigBand implemented the most commonly deployed SDV controllers, and were subsequently acquired by ARRIS).

  - SA's network control architecture implemented an interactive session manager, supporting DSM-CC User-to-Network commands [5] for support of dynamic MPEG transport sessions.
- Electronic Program Guide (EPG) application and EPG metadata format.

Integration of interactive service components, such as a VoD application and corresponding video streaming servers, required tight integration with either GI or SA's network. This resulted in pair-wise integrations between VoD vendors, set-top applications vendors, and the digital video systems providers.

Existing cable systems have now evolved in ways that vary widely from the legacy system architectures that were just described. One major difference is the use of the Common Scrambling Algorithm (CSA) in some systems, rather than core ciphers based on DES. In addition, many systems incorporated content delivery components from multiple vendors, which has led to much more diversity in session control, bandwidth management, maintenance, commercial insertion, VOD and other critical system hardware and software.

To attempt to address the issue of interoperability across cable systems, CableLabs developed a set of specifications under the OpenCable program **Error! Reference source not found.**. These specifications isolate the proprietary system specific aspects of these systems into separable components. The systems specific aspects fall into two general categories:

- Hardware – These included, the core hardware components of the CA system (working cipher and key hierarchy) and the key components of the OOB communications network (e.g. forward error correction and MAC layer processing)
- Software – These included, Operating System (OS) and applications (both cable operator specific and potentially third-party applications)

Figure 2 - OpenCable/tru2way Interface DiagramFigure 2 provides a block diagram identifying the key interfaces in the OpenCable architecture.

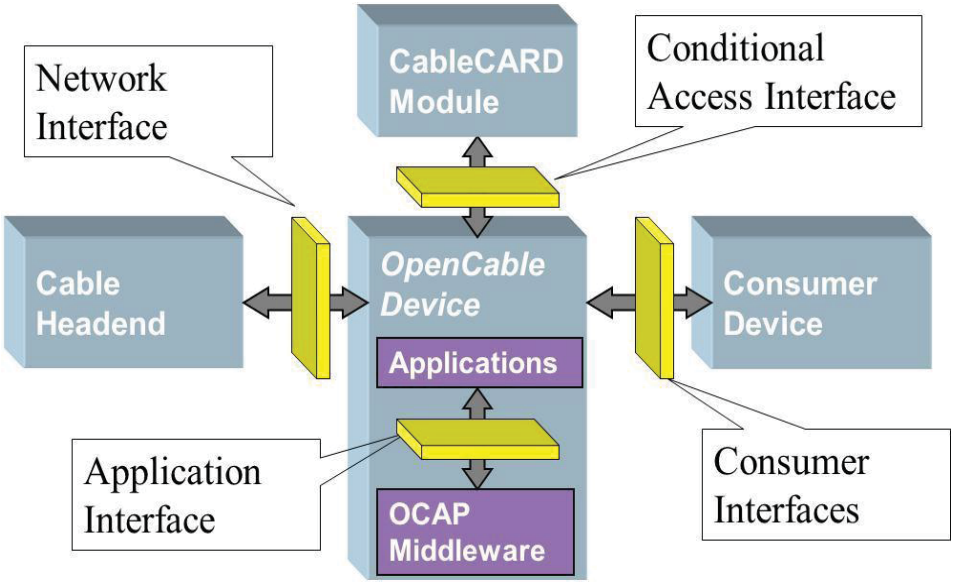


Figure 2 - OpenCable/tru2way Interface Diagram

The four interfaces specified by OpenCable:

- The Network Interface – This is the interface that connects to the cable network at the consumer's home and is specified as part of the OpenCable Host Specification [30].
- The Consumer Interfaces – These are the interfaces that connect to the consumer's TV or other entertainment devices (e.g. HDMI, component analog, composite analog, etc.) and are also specified as part of the OpenCable Host Specification **Error! Reference source not found.**.
- The Conditional Access Interface – This is the interface to the system-specific CA and OOB channel and is specified in the CableCARD™ Specifications.
- The Application Interface – These are the Application Program Interfaces (APIs) that applications use to perform the desired functions using the Host and CableCARD components and are specified by the Open Cable Application Platform (OCAP) specification [23].

In this architecture, an OpenCable Host device is enabled to connect to the cable network by providing a hardware component, the CableCARD, which is specific to the proprietary system deployed in that cable network. Originally, this would be either a GI or SA CableCARD; however other CA systems, such as NDS and Conax, have been added to this list over time. The CableCARD cryptographically binds to the Host for security and copy protection purposes and instructs the Host how to acquire the OOB communications channel, register on the network, and receive the OOB command and control signals appropriate for the CA system. The Host is then able to acquire the list of applications, for example the EPG, which are supported on the cable system, securely download them if necessary, and begin execution.

The CableCARD is the hardware module in the OpenCable system that achieves this isolation through a physical encapsulation of the cryptographic CA component and some portions of the OOB communications channel. The CableCARD by necessity had to be a separable or removable module that

could be delivered independently from the Host device. In practice, the local cable operator provides the CableCARD.

The only commonality the two proprietary OOB channels have is the use of QPSK modulation; they differed in the frequency band and bandwidth, the Forward Error Correction (FEC), the framing, and the transport protocol used. Consequently, the QPSK front-end (modulation and demodulation) was placed in the OpenCable Host and all of the higher layers of the proprietary OOB communications protocol stack were placed in the CableCARD. Raw QPSK symbols and their timing passed across the PCMCIA interface through the use of redefined pins in the physical interface. The CableCARD is responsible for instructing the Host what mode of operation the system requires. OpenCable also enabled the cable operator to migrate the proprietary messaging carried on these proprietary OOB channels to a standard two-way communications channel, such as Data-Over-Cable Service Interface Specification (DOCSIS®). This was accomplished through the DOCSIS Set-top Gateway (DSG) with the appropriate modifications to the CableCARD **Error! Reference source not found.**. Since DOCSIS provides an efficient two-way IP connection for devices, the DSG specification focused on extending the DOCSIS specification to perform two key functions:

- Encapsulate the downstream proprietary messaging in an IP transport using a broadcast or multicast transmission so that all set-tops could access it concurrently.
- Provide a one-way mode of operation so that the set-top could continue to function in a one-way mode in cases of network disruption.

EIA-679 Part B [17] only permitted the decryption and processing of a single MPEG Multi-Program Transport Stream (MPTS), equivalent to a single set-top tuner. The original CableCARD specification followed this model with single stream mode, or S-Mode, of operation. As Digital Video Recorders (DVRs), picture-in-picture, and other multi-tuner features were developed, it was realized that the original S-Mode CableCARD had inadequate bandwidth for these features. It would require multiple S-Mode CableCARDs to provide this capability and could not grow to support multi-tuner gateway scenarios. Subsequently, the M-Mode (or Multi-stream mode) CableCARD specification was developed and has its origin in SCTE 28 **Error! Reference source not found.**. M-Mode provides the higher transport data throughput rates that are required to support features, such as multiple-tuner Hosts, Hosts with DVRs, and Hosts with picture-in-picture capability as described in DSTAC Working Group 2 Report #1 **Error! Reference source not found.**.

Satellite Technologies and Architectures [52]

As was summarized in DSTAC Working Group 2 Report #1 [45], there are two primary Direct Broadcast Satellite (DBS) providers in the United States, DISH and DirecTV. While they use similar technologies and architectures to deliver the DBS portion of their service, there are still sufficient differences in the two systems as to prevent a set-top box designed for one system from working on the network of the other.

Figure 3 shows the general DBS architecture for distribution of the television signal from program source to the subscriber's home. The video programming is distributed from the program source via satellite (indicated by "a" in the diagram) or fiber (indicated by "c" in the diagram) to the satellite up-link facility where it may be re-encoded, multiplexed, and encrypted for transmission via the DBS satellite to the

subscriber's home. Local Receive Facilities (LRF) or Local Collection Facilities (LCF) are used to receive programming from local broadcast stations (indicated by "b" in the diagram), where these channels are then decoded, re-encoded, multiplexed, and transmitted via satellite or fiber to the satellite up-link facility. In some instances, an antenna at the subscriber's home receives local broadcast stations directly (indicated by "d" in the diagram).

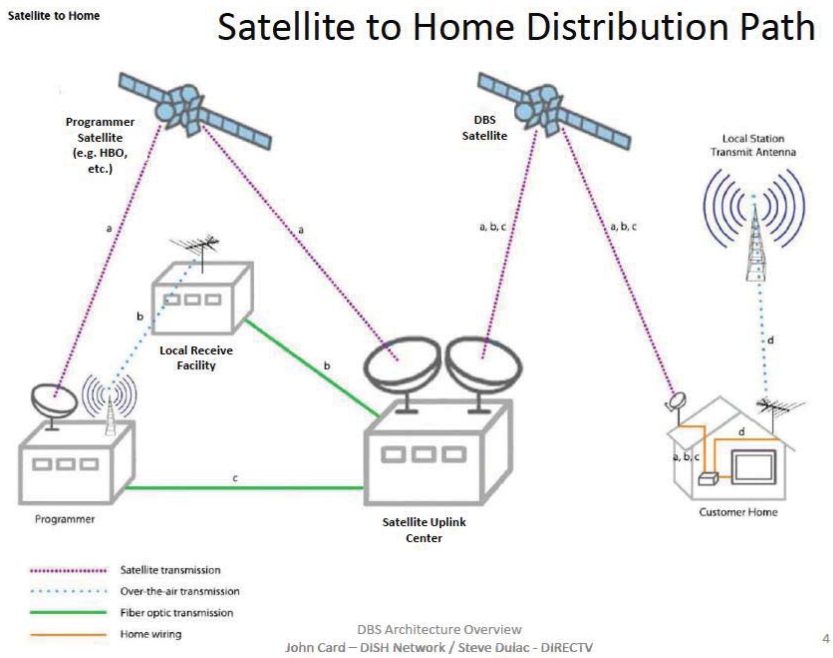


Figure 3 - DBS Architecture – Satellite to Home Distribution Path

Multiple satellites are used in each system to carry the diversity of programming offered by each provider. The Out Door Units (ODUs) and Low Noise Block (LNB) down-converters receive the satellite signals and down-convert the signal to a lower frequency for distribution over coax cable throughout the subscriber's home. Because there are multiple satellite signals received by the ODU and LNB and there are potentially multiple tuners and/or set-tops in the home, a Multiswitch unit is used to switch the specific signal source to the requesting tuner.

The two operators' systems differ in a number of respects, including:

- The number and location of up-link facilities
- The orbital positions of the satellites used by each
- The satellite frequency plans used
- The Out Door Units (ODUs), Low Noise Block (LNB) down-converters, and Multiswitch units used
- The Conditional Access Systems (CAS) used
- The whole home DVR architectures and technologies used

Figure 4 and Figure 5 show the number and location of the uplink facilities for the two DBS providers. As can be seen the number and location of uplink facilities differs significantly.

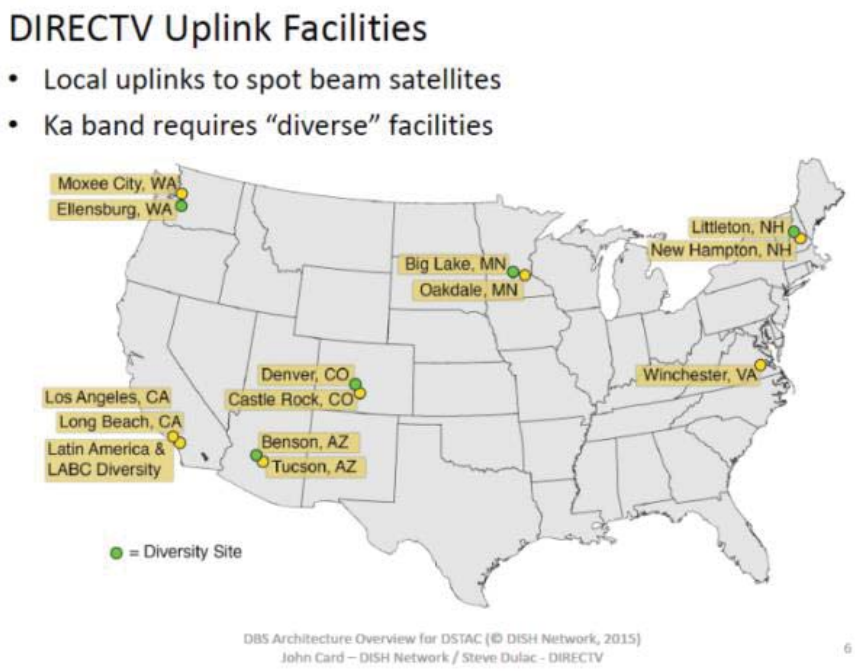


Figure 4 - DIRECTV Uplink Facilities

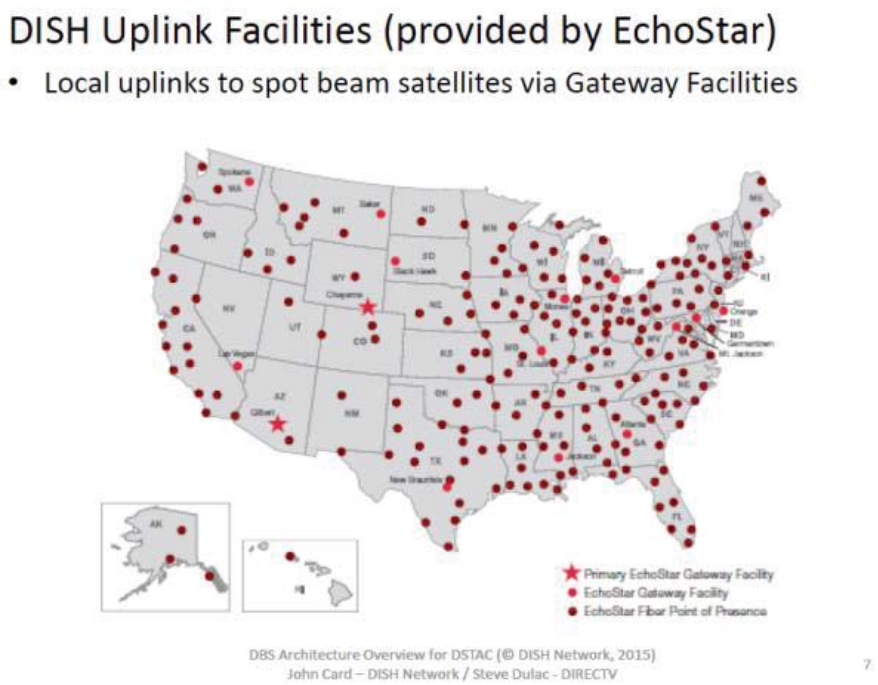


Figure 5 - DISH Uplink Facilities

The orbital positions for the two providers differ and this directly affects the orientation of the satellite dish and configuration of the ODU, LNB, and Multiswitch at the subscriber's home. The orbital positions for the two providers currently are:

- DirecTV – 99W, 101W, 103W as well as 110W, 119W & 95W
- DISH – Eastern US Arc – 61.5W, 72.7W, 77W, Western US Arc – 110W, 119W, 129W and shared 118.7W

The satellite frequency plans of the two providers differ as well. This impacts the configuration of the LNB and Multiswitch at the subscriber's home, as well as the implementation of the Integrated Receiver Decoder (IRD) or set-top box. Figure 6 and Figure 7 show the respective satellite and in-home frequency plans of the two providers.

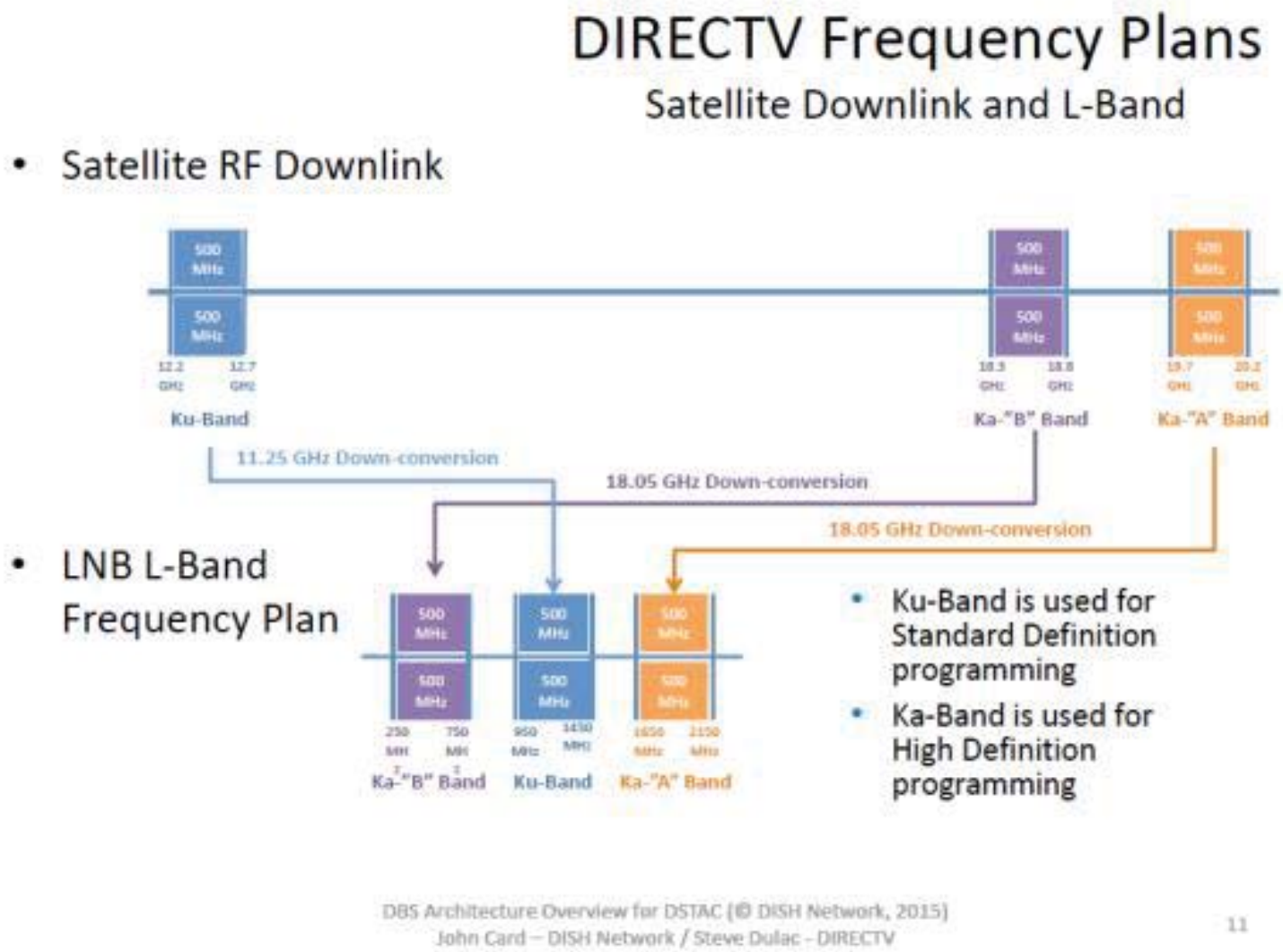


Figure 6 - DIRECTV Frequency Plan

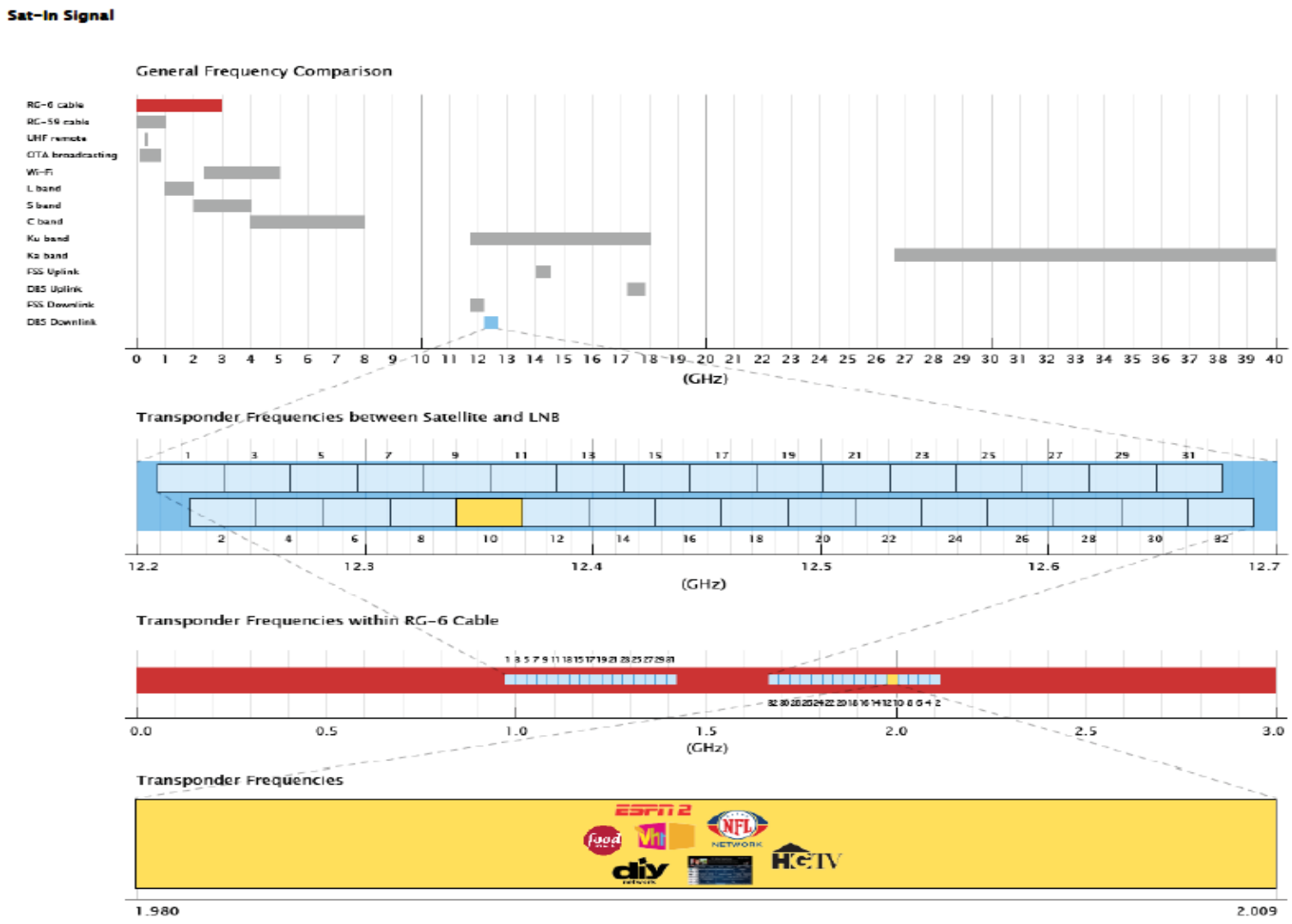


Figure 7 - DISH Frequency Plan

The ODUs and LNBs differ depending on the DBS operator and type of service being provided. For example, the current DirecTV ODUs include: an 18" Round (SD only), an 18x20" Triple-Sat (SD only), or a Slimline ODU (HD) which can be used with a Slimline-3 or a Slimline-5 LNB. The LNBs also differ in their powering. DISH LNBs are typically powered by one set-top in the home, while all DirecTV and some DISH LNBs have a dedicated external power supply. The Multiswitch unit allows a set-top to select between the multiple input signals received by the LNB. Because LNBs receive signals from multiple satellite transponders, it is necessary to switch the input signal for the requested channel to the requesting set-top tuner. The set-top sends a signal to the Multiswitch unit identifying the desired input and the Multiswitch unit switches the input signal onto the coax cable to the requesting set-top.

The two DBS providers differ in their implementations of their respective Multiswitch units. The control signaling between the two systems differs. Specifically, DIRECTV uses a Pulse-Width Modulated (PWM) control scheme; with simple 3-byte messages to identify desired input port, which does not strictly conform to the DiSEqC (Digital Satellite Equipment Control) standard. DISH uses system based on and conforming to DiSEqC but extending the standard with additional commands. There are Single Wire Multiswitch units, which allow multiple, independent set-tops to share a single coaxial cable and multi-wire switch units that use separate coax cables for each set-top. Set-tops, Multiswitch units, ODUs and LNBs from the two providers do not interoperate.

The DIRECTV set-top boxes receive SD satellite signals using the 130-byte "DSS" transport format, while DISH uses the 188-byte MPEG transport format for its SD satellite signals. Both MVPDs use MPEG transport format for HD satellite signals. The two DBS providers utilize Digital Video Recorders (DVR) in the home to deliver a more interactive and personalized experience to subscribers: each have proprietary implementations that leverage MVPD-controlled content storage to deliver features including VOD and targeted Dynamic Ad Insertion (DAI). Each implementation "pushes" VOD and DAI content through the DBS broadcast system to pre-allocated storage areas of the DVR. As an example of use of this capability, the two providers jointly offer targeted DAI that was used during the 2014 election cycle by local and national candidates to reach their constituents. Each proprietary implementation required the providers to modify the headend transport and video stream encoding to offer seamless merging of broadcast and from-DVR content. The set-top boxes from both providers offer common television outputs (e.g. analog component and composite, digital HDMI), but have deployed non-interoperable approaches for IP-networked outputs. Software updates to set-top boxes happen independently on each DBS system as new features of the service are released, and typically range in frequency from quarterly for legacy devices to more than once per month for newly deployed set-top boxes or critical bug fixes. The two DBS providers also differ in the CAS and DRM solutions used in their respective DBS systems. DirecTV uses NDS CAS/DRM systems and DISH uses Nagra CAS/DRM systems. Both providers support additional DRM systems for their internet-delivered services.

While both DBS providers use a client-server architecture and MoCA for in-home distribution of their whole home DVR solutions, they differ in their specific implementations. Figure 8 and Figure 9 show the two whole home DVR server-client solutions. DirecTV uses the RVU Remote User Interface technology, which has been integrated into a number of retail televisions (see rvualliance.org/products). Like other MVPDs, both providers participate in the Digital Living Network Alliance (DLNA) and make use of some DLNA protocols in their whole home DVR solutions.

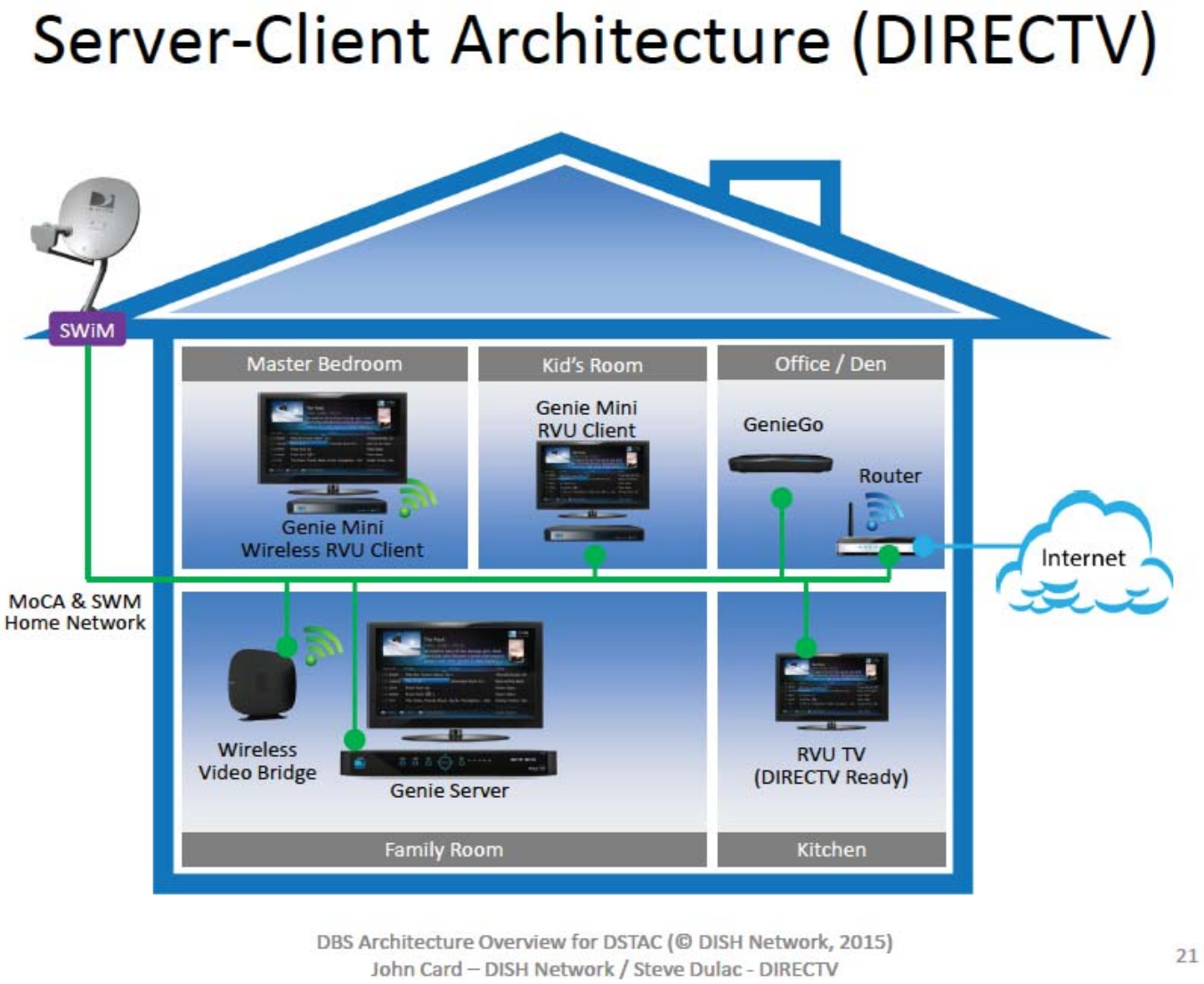


Figure 8 - DIRECTV Server-Client Architecture

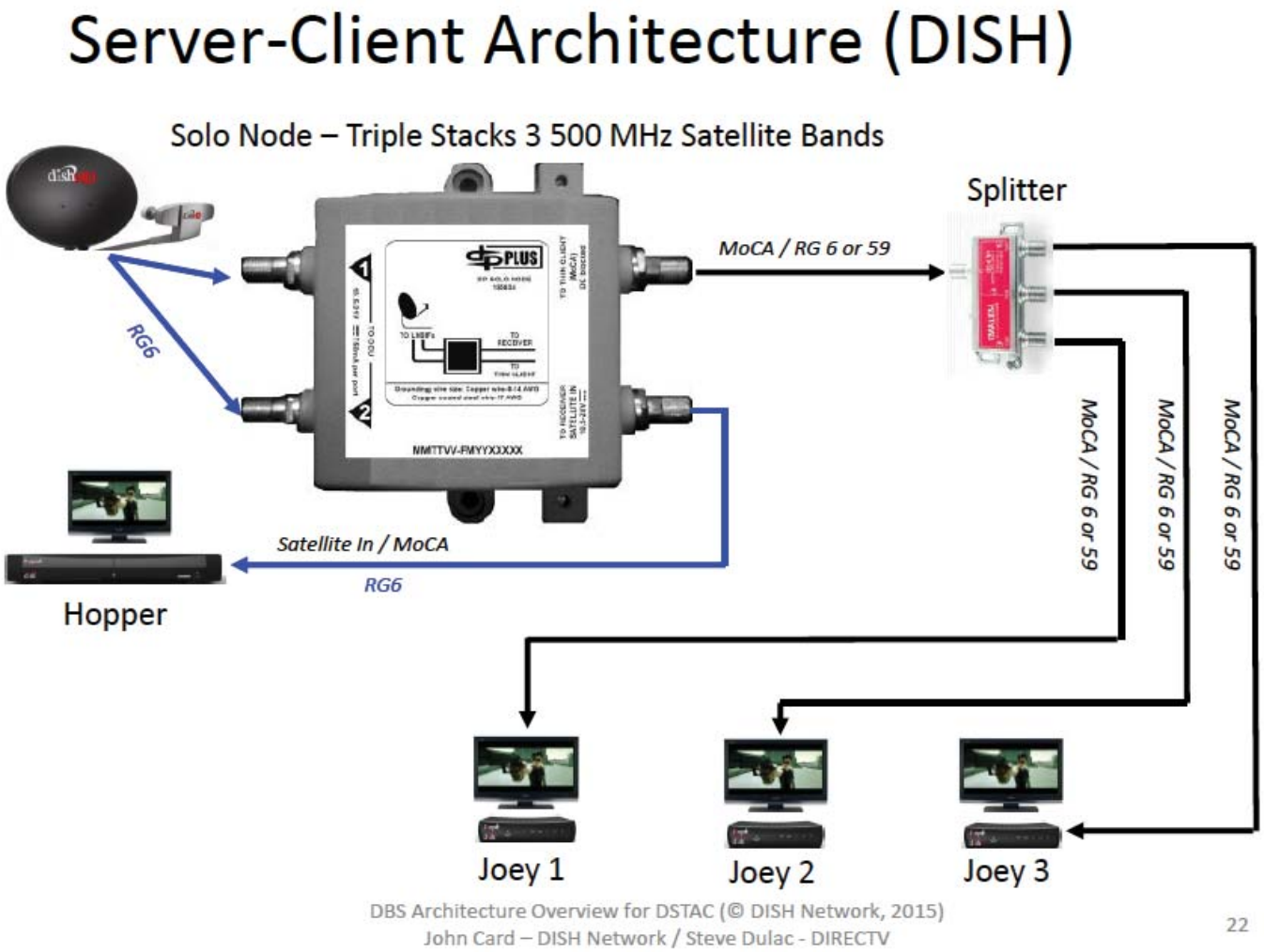


Figure 9 - DISH Server-Client Architecture

Telco Technologies and Architectures

Telephone companies have used a number of different technologies and architectures for delivery of their MVPD service. Some have partnered with satellite providers to deliver an MVPD service, others have deployed fiber with an RF overlay network, and others have deployed IPTV systems over VDSL and fiber networks. This section covers the systems deployed by AT&T and Verizon.

AT&T and Verizon have taken different approaches to deploying an MVPD service. AT&T largely leveraged its twisted pair network using VDSL technology to deliver an IP-based TV service. AT&T has also deployed an FTTP PON network to carry this IPTV service. Verizon deployed a PON fiber network (FiOS) from the start, but chose to leverage cable technology to deliver its MVPD service to the point that they also make use of CableCARD in their set-top boxes as well as in support of retail devices. To accomplish this, Verizon used a separate wavelength to carry an RF spectrum with broadcast TV channels. The two-way PON network is used to carry two-way services, including VoD. This is sometimes referred to as a Hybrid QAM/IP implementation, as QAM is used to carry the broadcast channels and IP is used to carry VoD services.

AT&T Technologies and Architectures [43]

In 2004 SBC/AT&T participated in the Microsoft IPTV Early Adopters Program (EAP). The IPTV Mediaroom system was designed as an application platform to support the IPTV service and evolution of service features. The platform is now owned and maintained by Ericsson. AT&T offers this service over both copper (VDSL) and Fiber (FTTP) networks. The service is based on an all Internet Protocol (IP) delivery for Linear/Live, and VOD. The system encompasses a number of proprietary features such as Instant Channel Change (ICC), Multiview, and a large number of interactive applications, an EPG, search engine, recommendations, integrated service features such a caller-ID on the TV, etc. Applications such as Multiview are integrated within the Mediaroom software client. AT&T is a licensee of the Mediaroom proprietary IPTV system and additional implementation details has to be obtained directly through Ericsson. The Microsoft Mediaroom DRM is used for content protection on AT&T U-verse STBs with an embedded secure SOC. U-verse is offered to third party devices such as smart phones (iOS, Android), tablets, PCs and laptops through AT&T U-verse applications. PlayReady DRM is used for content protection on these devices.

Figure 10 is a diagram of the AT&T U-verse Architecture. U-verse content is acquired and gathered at a central location, the Super Hub Office (SHO), for national linear channels and VOD assets. Linear content is encoded to AT&T's unique specifications and distributed via multicast from the SHO to Video Hub Offices (VHOs). The content is then multicast to the end user, when requested. Local channels are acquired locally and encoded to AT&T's unique specifications at the VHOs. VOD assets are encoded to AT&T's unique specifications and transported to the SHO[1]. From there they are distributed to the VHOs via multicast, and stored locally at the VHOs. The assets are then streamed from the VHOs to the end user via unicast, when requested.

Linear channels are encoded using H.264 video compression and Dolby Digital Plus (DD+) converted to AC-3 by the STB or AAC audio, and contained within an MPEG-2 transport stream. When ingested into Mediaroom, the channels are encrypted and encapsulated as RTP streams via the Acquisition Servers (A-

[1] Note that AT&T does not use the CableLabs encoding specifications to encode content.

servers), and distributed via multicast to the local VHOs. Linear channels are also acquired by a Distribution Server (D-server), which is at the VHO and used for instant channel change. When a user switches to a live channel, a proprietary ICC enables a fast channel change implementation.

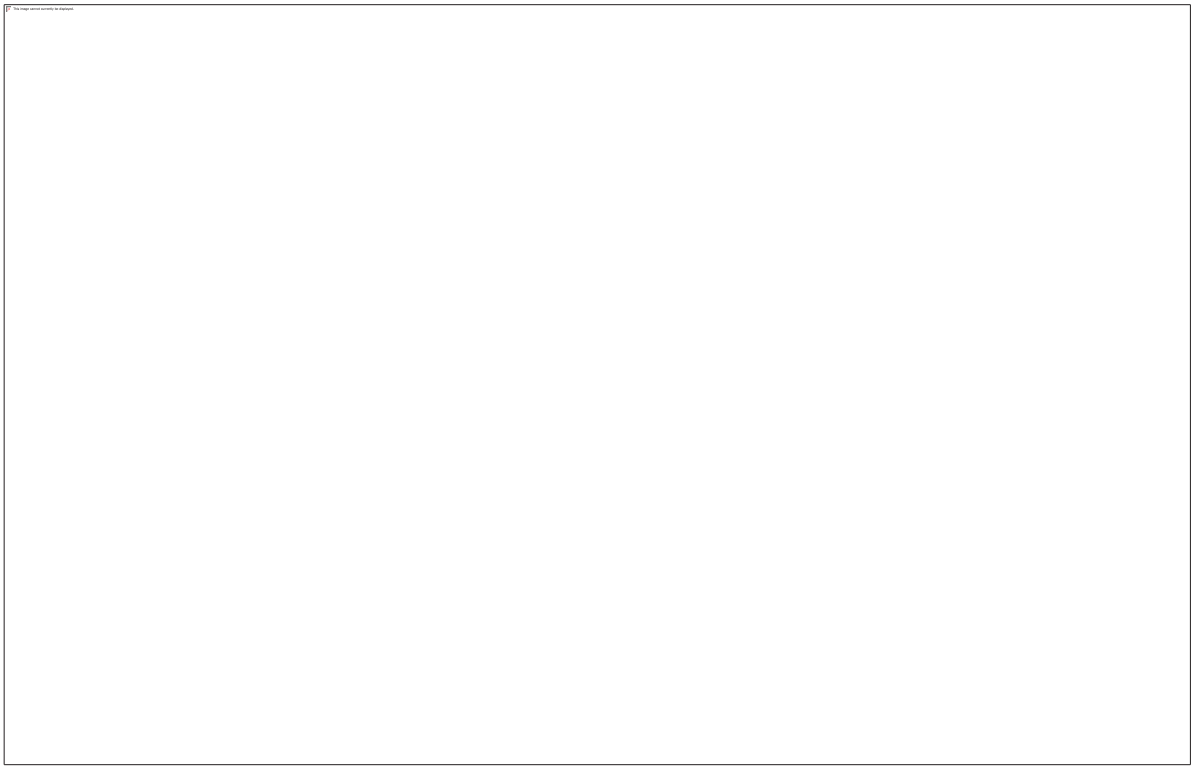


Figure 10 - AT&T U-verse Architecture

VOD assets are encoded using H.264 video and AC-3 audio, and contained within an MPEG-2 transport stream. When ingested into Mediaroom, the assets are encrypted, encapsulated as an RTP stream, then distributed and stored at the local VHOs on VOD Servers (V-servers). When initiated by the user, VOD assets are streamed from the VHO V-servers to the user's receiver over HTTP.

The U-verse Mediaroom DRM is used to enforce license restrictions from content agreements and provides overall content protection. The DRM is based on 128-bit AES and 2048-bit RSA encryption. Linear content is encrypted either at the SHO, or at the local VHO (for local channels). The encrypted channels are distributed to the end user's STB where they are decrypted using an embedded secure SOC. VOD assets are encrypted at the SHO after being acquired from the content provider. The encrypted assets are then distributed through the network and only decrypted once it is streamed to the end user's STB. Content outputs are also protected via HDCP, CGMS-A, and Macrovision. The output controls are implemented through the client application.

AT&T U-verse is also available online at uverse.com, and on tablets and smart phones via the U-verse mobile application. Uverse.com offers a web site where users can login and view services. Some content flows through an internal process and other content is hosted directly through third parties like Hulu, Turner, etc. Content is protected via PlayReady DRM. The U-verse mobile app for phones and tablets are developed internally and content is encoded and hosted using a third party. Content is protected via PlayReady DRM.

New updated U-verse Mediaroom software is pushed to U-verse STBs at least twice a year: offering new features, improved performance, security and protocol system updates and updated user experience. AT&T is planning to deploy 4K and HEVC, more advanced STBs to provide more value-added services to U-verse customers. Access bandwidth is improving with the provisioning of more bandwidth over VDSL and the deployment of more fiber (GigaPower). AT&T will be deploying more advanced Wi-Fi technologies (i.e. 802.11ac) for both video and data distribution and expanding U-verse applications to reach more and more third-party devices, and offering more interactive applications.

Verizon Technologies and Architectures [44]

Verizon took an alternate approach to AT&T by deploying a FTTP network known as FiOS. The Verizon FiOS network is a Passive Optical Network (PON) either B-PON or G-PON with the addition of an "overlay" wavelength (1550nm) to transmit broadcast video over RF. VOD is distributed over IP using data/voice wavelengths (1490nm & 1310nm). Figure 11 shows the Optical Spectrum on the PON network based on ITU G.98x PON standards. Figure 12 provides a diagram of the FiOS access network showing the B/G-PON OLT for two-way voice, data, and VoD traffic, the Erbium Doped Fiber Amplifier (EDFA) used to inject the broadcast RF on the fiber, and the ONT at the customer premise. This diagram also shows the optical wavelengths used for the FiOS service. This architecture provides full support for both cable style RF video as well as emerging IPTV video technologies. Moving the VOD traffic to the B/G-PON IP network freed up RF spectrum for broadcast HDTV growth and provides greater scale as demand for voice, data, and VoD increases. The network protocols used on the B/G-PON network are ATM AAL1&2 for Plain Old Telephone Service (POTS) and ATM AAL5 for Broadband Internet and VoD.

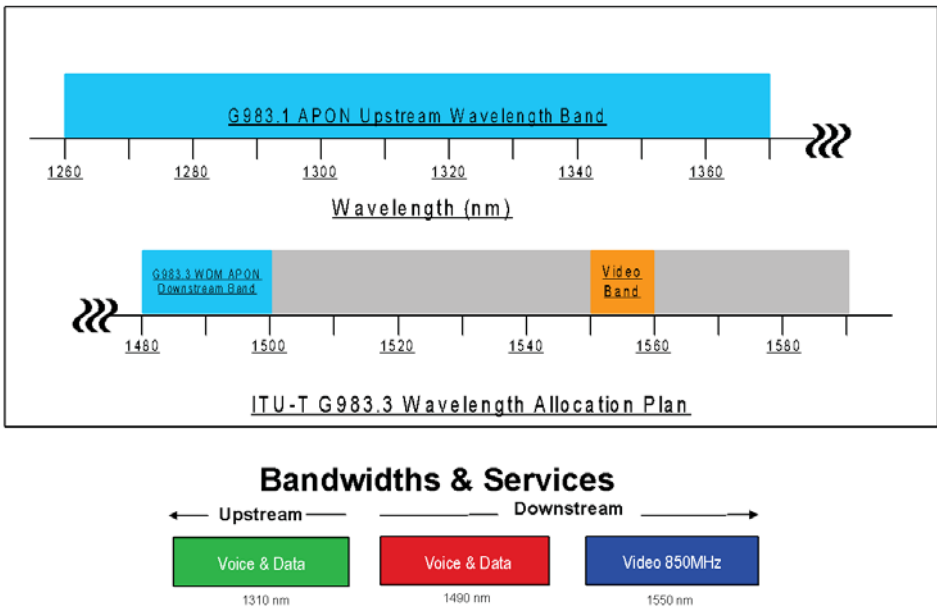


Figure 11 - ITU G.98x PON Optical Spectrum

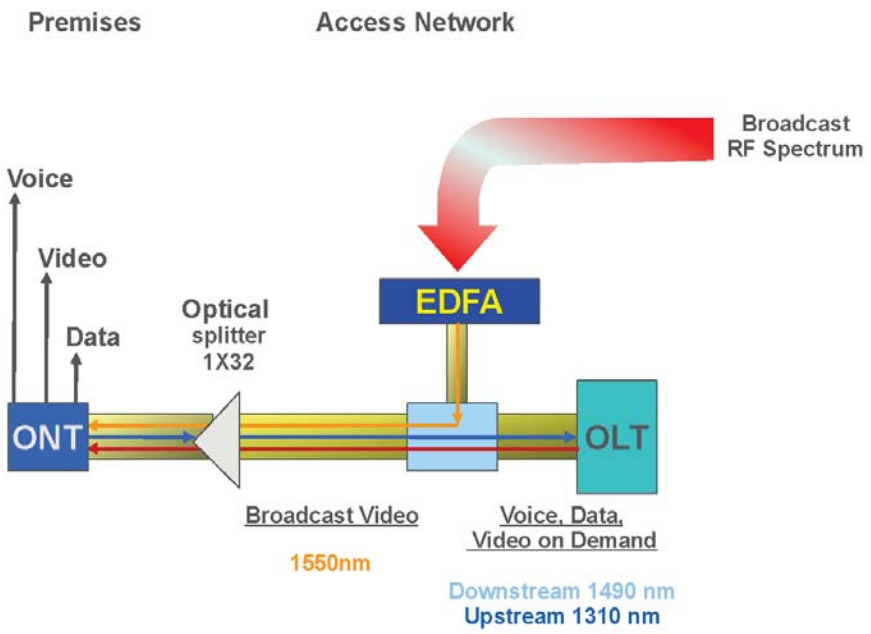


Figure 12 - Verizon FiOS Access Network

Figure 13 shows the high-level Verizon architecture. Content is received at two Super Head Ends (SHE) for purposes of redundancy. A Long Haul Network (LHN) is used for the National Video Distribution Network to carry the video traffic from a SHE to multiple Video Hub Offices (VHO), each of which serves a major metropolitan or franchise area. The Metro Video Distribution Network distributes the video traffic from a VHO to multiple Video Serving Offices (VSO) where it is then distributed over the PON access network to the customer premise. This diagram also shows which network protocols used at which points in the overall architecture.

Figure 14 shows the FiOS Hybrid QAM/IP set-top box and dual networks over which it connects to the VSO. First, there is the one-way overlay interface that carries broadcast video using 256 QAM and MPEG-2 Transport Streams (TS). In addition, there are two OOB downstream channels to support multiple encryption systems: SCTE-55-1 for the MediaCipher CAS system and SCTE-55-2 for the PowerKey CAS system, similar to that used by most US Cable operators after fiber termination. These OOB channels carry System Information (SI), Entitlement Management Messages (EMM) and other control plane signaling for box control and configuration. The IP Interface carries VOD content, duplicates some of the OOB signaling and carries additional application data including widgets, guide data, and gaming traffic.

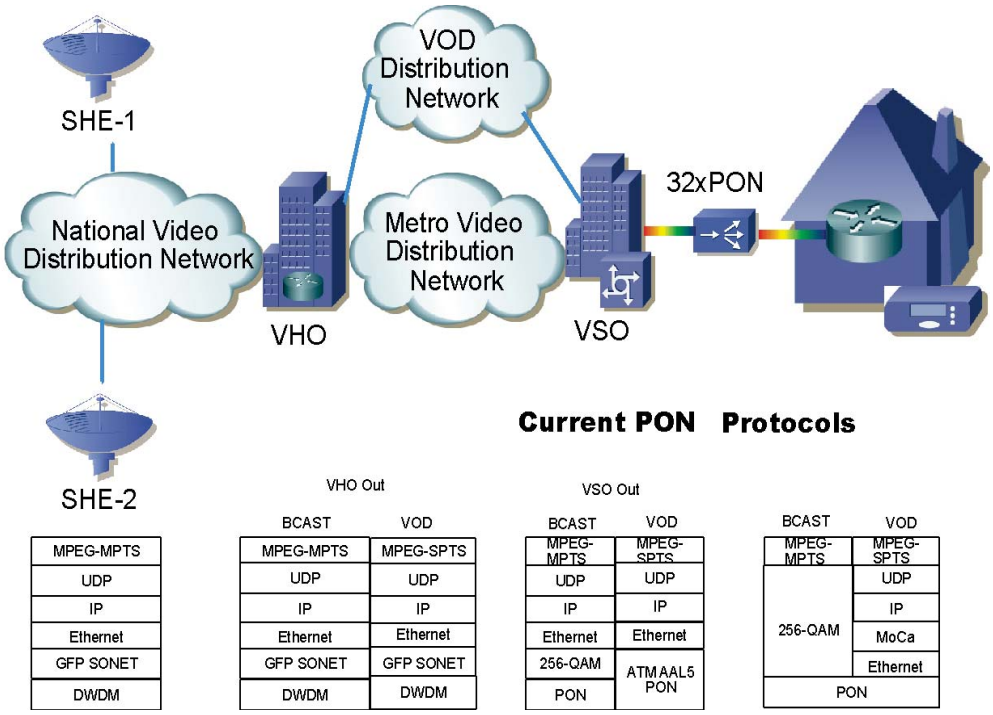


Figure 13 - Verizon FiOS High-Level Architecture

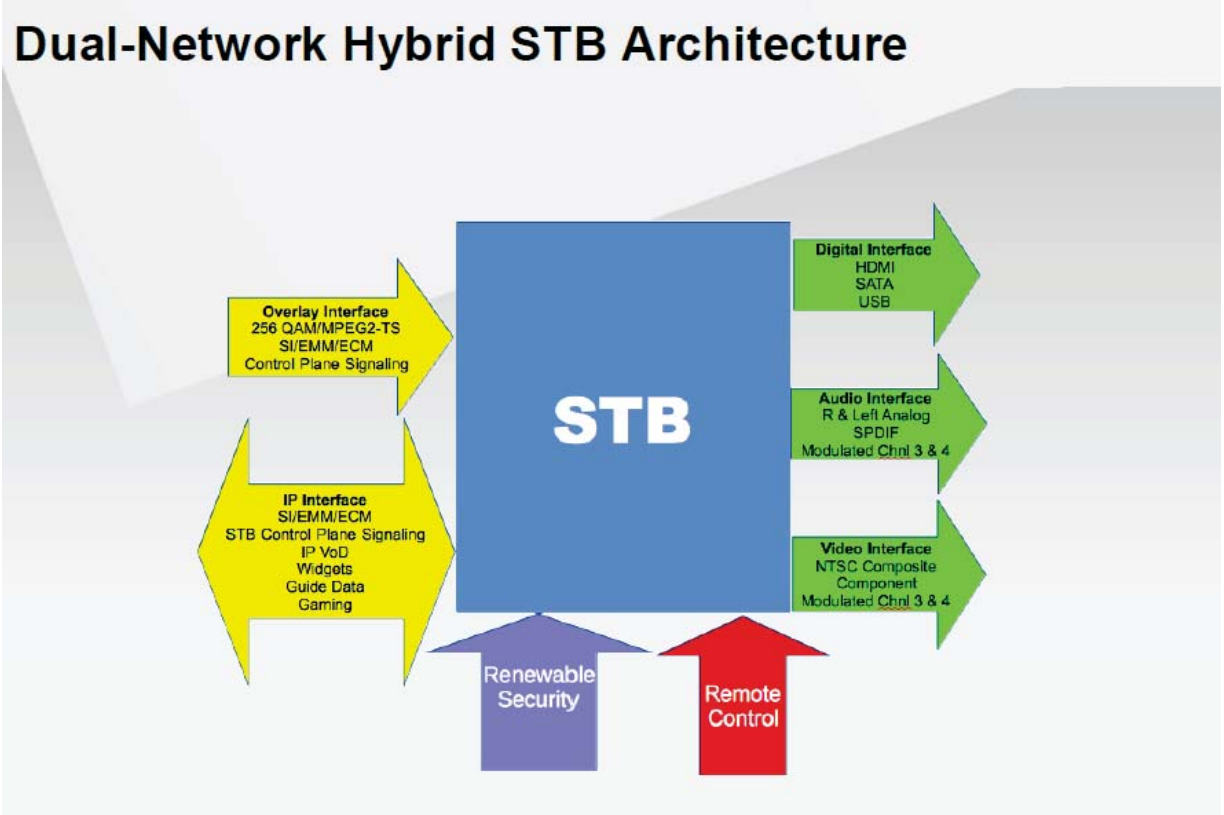


Figure 14- Verizon FiOS Dual-Network Hybrid STB Architecture

The Verizon FiOS system uses both MediaCipher and PowerKey CAS systems in all markets via a Simulcrypt compliant architecture. All channels and VOD are encrypted using the DVB Common Scrambling Algorithm (CSA) cipher. The system also fully supports the CableCARD interface with different CableCARDs provided for MediaCipher and PowerKey. To support CableCARD it was necessary to support the distribution of required Uni-Directional Cable Service information such as System Information and EMMs via the RF OOB channel. However for non-uni-directional services the IP network is used instead. See WG2 report section III D [45]. In order to support simulcrypt, the FiOS headends comply with the DVB Simulcrypt standard. In the FiOS simulcrypt implementation, the MediaCipher CAS has the sole Code Word Generator (CWG) function. Simulcrypt also increased the complexity of the system. Both the Mediacipher and PowerKey CAS systems are accessing the same commonly encrypted version of the content. In addition, many other channels and VoD content are available through alternate IP communications channels.

Verizon supports retail devices such as Smart Phones, Tablets, Smart-TVs, and Gaming Platforms. Non-FiOS access networks make use of DRM rather than CAS for content protection. The DRM solutions are based on 128 bit AES CBC cipher.

Direct-to-Home (DTH) Satellite Dish (small dish)

For customers in northern Alaska, the DBS satellite geometry coupled with the usual 1m dish does not provide enough signal strength for reliable operation. They will use larger dishes. Further, although the service delivered to customers in Alaska and Hawaii is comparable to the service delivered to the continental 48 states, the specific transponders and orbital locations used for delivery are likely to be different.

Over-the-Air Network Antenna Tuners (ATSC)

DBS receivers will commonly include ATSC tuners for local channel reception. The receiver integrates any off-air channels with DBS-carried HD and SD versions of the same.

Home Network Technologies

Home Networking Overview

AT&T U-verse supports both wired and wireless home networking for video distribution. In homes with structured wiring/Ethernet cable wiring (i.e. CAT-5 wiring), the Residential Gateway (RG) and STBs are connected using the available structured wiring. If structured wiring is not available, AT&T is using HPNA over coax for wired video distribution. AT&T is also offering a Wireless STBs (WSTBs) and a dedicated Wireless Access Point (WAP) using the 802.11n Wi-Fi technology for video distribution. Figure 15 shows an example of home networking diagram.

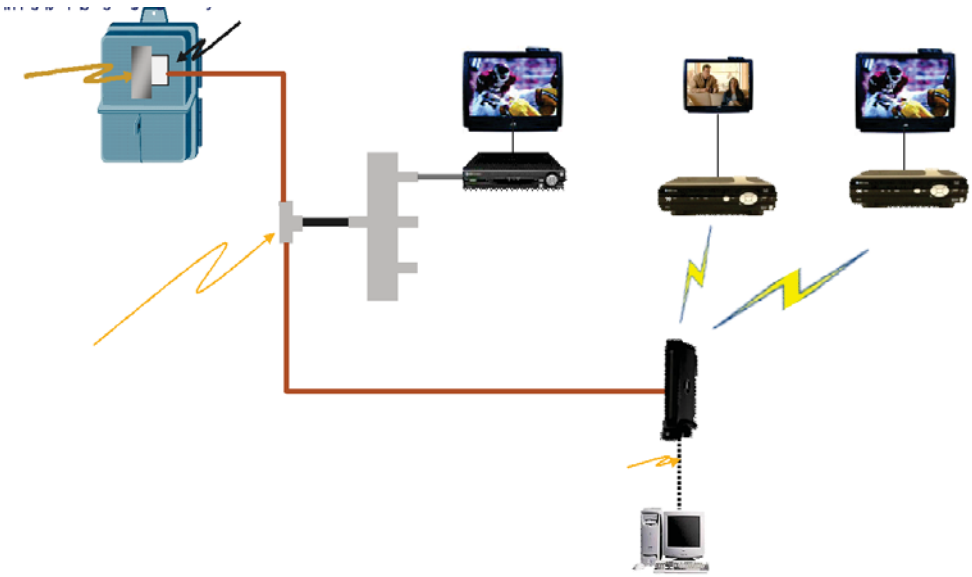


Figure 15 - Example Home Network

Typically, VDSL is terminated at the RG using a coaxial cable or a twisted pair copper cable. Content is distributed to wired STBs via either HPNA over coax, or standard Ethernet cables, or wireless networks. In terms of Access network technology, AT&T is offering broadband services over both copper and fiber to the home networks. For the U-verse copper-based customers, AT&T is using VDSL speeds of up to 100Mbps and for fiber-based customers, AT&T is offering broadband speeds of up to 1Gbps.

Wireless Network Connectivity

Over the last decade wireless performance has improved exponentially as a result of technologies and features such as Multiple Input Multiple Output (MIMO), Transmit Beamforming (TxBF) and availability of additional spectrum. A number of wireless vendors are working on optimizing Wi-Fi silicon for in-home high definition video streaming. Figure 16 shows some of the current in home wireless technologies.

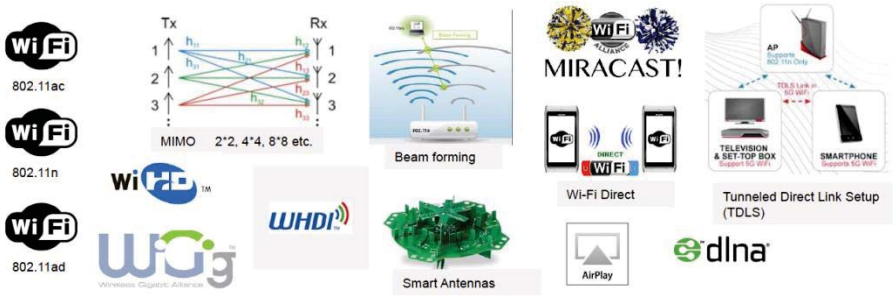


Figure 16 - Current in Home Wireless Technologies

Both 802.11ac and 802.11n claim enough capacity to support in-home video streaming. Many Wi-Fi products, including 802.11n, support Multiple Input Multiple Output (MIMO), digital Beamforming and operations in 5GHz spectrum. These technologies promise greater reliability and even better

performance than legacy Wi-Fi technologies. These technologies are application agnostic and allow operators to use device and service discovery technologies defined in DLNA.

Tunnel Direct Link Setup (TDLS) and Wi-Fi Direct are efficient methods for video streaming between two Wi-Fi clients. MSOs should consider these technologies for in-home video streaming if the cable video source (e.g. cable video gateway) in the home can be configured as a Wi-Fi client. The service discovery methods defined in Digital Life Living Alliance (DLNA) can be used while the TDLS clients are connected through an AP. A new Wi-Fi Direct Application Service Platform (ASP) to advertise and discover cable video services is required before Wi-Fi Direct can be used for in-home cable video streaming.

Miracast uses TDLS or Wi-Fi Direct as underlying transport. Unlike TDLS and Wi-Fi Direct, Miracast also defines application specific procedures such as content security methods and media streaming protocols to support screen mirroring and video streaming between two Wi-Fi clients. Miracast currently does not require support for High Definition video streaming using MPEG-2.

Use of Wi-Fi for in-home video streaming introduces a number of factors that influence the design of home network architecture. Some of these factors are:

- Does the customer subscribe to both video and Internet services from the same of different service provider?
- Is the video source (e.g. video gateway) connected to the home network LAN using wired or wireless network?
- Are there separate IP networks in the home for video and data services? An architecture using separate Wireless LAN for video and data can result in confusion for the customer since a device connected to the Wi-Fi AP for video services will not be able to access data services without first disconnecting from the video Wi-Fi network, and then connecting to the data Wi-Fi network. WiGig (802.11ad) supports data rate up to 7 Gbps using 60 GHz frequency band. The indoor coverage range for WiGig is about 10 meters, which is good for communication between two devices in the same or next room.

802.11ac versus 802.11n

802.11ac delivers higher throughput than 802.11n, as a result of the support for 80 MHz channels and 256 QAM. This advantage is more obvious when Wi-Fi clients are at close range to the Wi-Fi AP. The throughput performance of the two technologies is comparable at long range (e.g., < -70 dBm RSSI).

While either 802.11n or 802.11ac can be used for video streaming, 802.11ac is the current generation Wi-Fi technology, and it supports some features that were not part of the 802.11n standard. Table 2 below provides a highlight of some of the differences between 802.11n and 802.11ac.

Features	**802.11n**	**802.11ac**
Frequency Band	2.4 or 5 GHz	5 GHz only
Channel Bandwidth	20, 40 MHz	20, 40, 80, 160, 80+80 MHz
Modulation & Coding	64 QAM	256 QAM

Features	802.11n	802.11ac
Scheme		
Spatial Streams	Up to 4	Up to 8
Transmit Beamforming	Optional	Standardized
Max Throughput	600 Mbps	3.2 Gbps
MU-MIMO	No	Yes
Availability	Available for some time now	First generation available now

Table 2 - Comparison 802.11n and 802.11ac features

In addition to the features in Table 2, 802.11ac also includes support for features such as Dynamic Bandwidth Management, which can be very handy in mitigating interference and improving spectral efficiency. This feature allows an AP to dynamically choose channel bandwidth to each client on a frame-to-frame basis.

The first generation 802.11ac products support only 20, 40 and 80 MHz channel bandwidth. The current FCC spectrum rules do not allow for a 160 MHz channel. Channel bandwidth of 80 MHz+80 MHz and 160 MHz are expected in the second-generation 802.11ac products. Support for MU-MIMO and Dynamic Bandwidth Management are also expected in the second-generation 802.11ac products.

AT&T is deploying a dedicated video Wireless AP (WAP) that is based on 4x4 802.11n. The video WAP is strictly used for video distribution to wireless standalone STBs that are based on 802.11n Wi-Fi standard.

TUNNEL DIRECT LINK SETUP (TDLS)

TDLS allows network-connected client devices to create a secure, direct link to transfer data more efficiently. The client devices first establish a control channel between them through the AP. The control channel is then used to negotiate parameters (e.g., channel) for the direct link. APs are not required to support any new functionality for two TDLS compliant devices to negotiate a direct link.

TDLS offers multiple benefits, including efficient data transmission between client devices by removing the AP from the communication link. Use of direct communication channel also allows the client to negotiate capabilities independent of the AP. For example, clients can choose a wider channel, efficient modulation scheme, security and channel that are more suitable for direct link between the client devices.

TDLS devices, communicating with each other over a direct link, are also allowed to maintain full access to the Wi-Fi network simultaneously, which for example, allows the client device to stream video to another device in the home over the direct link; and at the same time allow user to surf Internet via connectivity to the AP. If the TDLS direct link is switched to another channel, the stations periodically switch back to the home channel to maintain connectivity with the Wi-Fi network.

The WFA has certified multiple products for TDLS, including Broadcom and Marvel. TDLS is based on IEEE 802.11z, and is one of the optional features of Miracast (Wi-Fi Display).

WI-FI DIRECT

Wi-Fi Direct allows Wi-Fi client devices to connect directly without use of an AP. Unlike TDLS, Wi-Fi client devices are not required to be connected to an AP to establish a Wi-Fi Direct link. Wi-Fi Direct also includes support for device and service discovery. Wi-Fi Direct devices can establish a one-to-one connection, or a group of several Wi-Fi Direct devices can connect simultaneously.

Wi-Fi Direct offers multiple benefits, including ease of use and immediate utility and enables applications such as printing by establishing a peer to peer connection between the Wi-Fi Direct enabled printer and client device, content sharing between two Wi-Fi Direct enabled devices, and displaying content from one Wi-Fi Direct device to another without requiring any Wi-Fi network infrastructure.

Wi-Fi Direct certifies products, which implement technology defined in the WFA Peer-to-Peer Technical Specification. The WFA has certified multiple products for Wi-Fi Direct. As of 2012, there are over 1100 Wi-Fi Direct certified products.

Wi-Fi Direct is the core transport mechanism for Miracast (Wi-Fi Display).

MIRACAST

Miracast provides seamless display of content between devices using Wi-Fi Direct as the transport mechanism. Miracast also includes optional support TDLS as a transport mechanism.

The key features supported in Miracast include device and service discovery, connection establishment and management, security and content protection, and content transmission optimization. Similar to Wi-Fi Direct and TDLS, Miracast is client functionality and does not require updates to AP devices.

Primary use cases for Miracast are screen mirroring and video streaming.

Miracast certifies products, which implement technology defined in the Wi-Fi Display Technical Specification. As of this writing many devices (e.g., Smart phones) have been certified for Miracast.

WIRELESS GIGABIT (WIGIG)

WiGig was originally developed in WiGig Alliance. In 2013, WiGig Alliance and Wi-Fi Alliance united, consolidating WiGig technology and certification development in Wi-Fi Alliance. The WiGig technology offers short-range multi-gigabit connections for wide variety of applications including video, audio and data. The following is a list of applications that WFA is focusing on:

- WiGig Display Extension
- WiGig Serial Extension
- WiGig Bus Extension
- WiGig SD Extension

The WiGig technology is the basis of IEEE 802.11ad amendment and supports Beamforming and data rates up to 7 Gbps in 60 GHz frequency band. Many WiGig products are also expected to support Wi-Fi, along with mechanisms for smooth handovers from 60 GHz to 2.4 GHz and 5 GHz band. The indoor coverage range is about 10 meters, which is adequate for communication between two devices in the same or next room. A number of vendors, including Atheros, Marvell and Broadcom, Dell, Intel,

Panasonic and Samsung are working with the WFA in the development of technology and certification testing program. The WFA currently expects to launch WiGig certification program in 2016.

Ethernet Network Connectivity

Some MVPD provided STB also have wired Ethernet connectivity. All U-verse STBs are equipped with a Fast Ethernet connector enabling the 10/100-base fast Ethernet home networking. This enables consumers with Ethernet wired homes to directly connect the STBs to the network termination units or RGs inside the home without the need for extensive rewiring or setup of high-fidelity wireless networks.

Bluetooth

Increasingly Bluetooth networking is being utilized by many CE devices and applications to extend their functionality to support new features and capabilities. These include (among others) remote controls, game controllers, and audio streamers.

ZigBee® RF4CE Remote Control Specification

Traditionally, remote controls for set-top boxes and CE devices have made use of InfraRed (IR) protocols that have relied on line of sight between the remote control and the device itself. Increasingly, these devices have been installed in entertainment centers or equipment closets that preclude line of sight use by IR remote controls. As a result the use of RF protocols like ZigBee RF4CE are being used in remote controls for set-top boxes. The cable industry has adopted a profile of RF4CE that is published by CableLabs[2].

HPNA Network Connectivity

AT&T is using the HPNA V3 over Coax that is based on the ITU G.9954-2006 standard. HPNA operates in the 12-44 MHz frequency band and offers a data throughput of up to 320 Mbps. The HPNA technology also supports Quality of Service (QoS), Differentiated Services Code Point (DSCP) with 8 priority queues. The technology also supports dynamic bandwidth allocation and coexists with VDSL.

MoCA 2.0 Technology Overview

Used for whole-home DVR, IP networking (IPVOD, CAS call-home for PPV/VOD purchase reporting, diagnostics, application data, diagnostics), software download and client control

Please refer to http://www.mocalliance.org/ for more information.

A typical in-home coaxial cable architecture consists of a tree-and-branch network topology using RF splitters and coaxial RG-6 or RG-59 cables. The multimedia signal enters the home via an Optical Network Unit (ONU) or via Cable gateway, Digital Subscriber Line (DSL) gateway, or via a satellite dish. Multimedia content is distributed to each room in the home using the in-home coaxial network. The home must support multiple simultaneous HDTV, SDTV, audio, data, voice-over IP, gaming, and other multimedia usages both from the broadcast network and from the in-home DVR or storage devices. Each wired room and device may be either, or both, a source or sink of multimedia content both to and

[2] Cable Profile for the ZigBee® RF4CE Remote Control Specification, OC-SP-RF4CE-I01-120924, September 24, 2012.

from multiple simultaneous entertainment devices in the home. Although the in-home coax is a relatively static channel, the presence of coaxial splitters creates a highly dispersive multipath channel that can cause significant echoes in addition to high signal attenuation when communicating between various networking devices.

The in-home coaxial network connectivity must provide a reliable room-to-room, peer-to-peer, full-mesh connectivity among all sources and sinks in the home. In order to support at least three simultaneous HDTV and SDTV multimedia streams, the in-home network is required to have at least 60 Mb/s, and in many cases greater than 100 Mb/s data throughput with low packet error rate and low average latency. These network performance requirements, adopted by MoCA, must be satisfied when other services are added or when a neighbor or a family member runs services in the home.

The initial MoCA technology using the existing in-home coaxial cables was based on the MoCA 1.1 standard ratified in 2007. It uses bit-loaded Orthogonal Frequency Division Multiplexing (OFDM) modulation with 224 subcarriers in a 50 MHz channel. Bit-loaded OFDM was selected for MoCA because it is robust against static or slowly changing multipath and optimizes the modulation between every pair of devices. When bit loading, each MoCA device probes the channel between itself and every other MoCA device in the network and selects the modulation on each of the 224 subcarriers based on the probe results: the better the signal-to-noise ratio (SNR) on a subcarrier, the higher the modulation assigned to that subcarrier. MoCA 1.1 uses a maximum subcarrier modulation of 256 QAM. Since the MoCA PHY layer adapts each link between node pairs independently, the channel capacity can be different between different nodes, as well as between the forward and reverse directions of the same node. The bit-loading parameters for a particular path are called a PHY profile. It enables a maximum PHY rate of 275 Mbps, and network throughput rate of 175 Mbps at low Packet Error Rate (PER ≤ 10^{-5}) and low average one-way latency (≤ 3.5 milliseconds) in defined frequency bands from 475 MHz to 1550 MHz. The latest MoCA 2.0 standard, which was ratified in June 2010, includes the following key features:

- Increased channel bandwidth from 50 MHz to 100 MHz (225 MHz) for bonded channels with increased maximum modulation density from 256-QAM to 1024-QAM
- Forward-Error-Correction (FEC) was changed from Reed-Solomon (RS) to Quasi-Cyclic (QC)-LDPC
- Expanded MoCA channel plan from 400 MHz to 1675 MHz in defined frequency bands to support bonded channels operation, and two simultaneous independent networks
- Total MAC network throughput of 430 Mbps, and 860 Mbps with a bonded-channel in a 16-node network
- Full backward interoperability with MoCA 1.1 devices
- Turbo-mode for two-node network with network throughput > 1 Gbps
- Using Orthogonal Frequency Division Multiple Access (OFDMA) for Reservation Requests (RRs) from each MoCA device to the NC
- Four new power states (‘Active’, ‘Idle’, ‘Standby’, ‘Sleep’) for energy savings were defined
- New multicast Parameterized QoS (PQoS) flows with reduced one-way average latency
- Enhanced link privacy using Advanced Encryption Standard (AES) in Cipher-Block Chaining (CBC) mode using 128-bit AES key length

Table 3 summarizes the MoCA 2.0 PHY and Medium Access Control (MAC) layer key parameters.

PARAMETER NAME	PARAMETER VALUE	NOTES
Bandwidth	100 MHz, 225 MHz (bonded channels)	
Modulation Type	OFDM	
Modulation Density	BPSK up to 1024-QAM	
Subcarrier Spacing	195.3125 kHz	
Cyclic Prefix	0.2 to 1.28 µs	In increments of 0.2 µs for data
FEC	QC-LDPC with code rate 39/46	LDPC = Low-Density Parity Code
Maximum PHY Rate (theoretical)	733 Mbps, 1466 Mbps (bonded channels)	
Maximum MAC Rate	430 Mbps, 860 Mbps (w/bonded channel)	
Medium Access Control (MAC)	TDD Scheduled MAC with Tx opportunities by NC	
QoS	Contention-free service with low-latency multicast flows	
Network Management	SNMP MIBs for MoCA 1.1	TR-069 support for MoCA 1.1
Maximum Network Size	16 adapters	
Power Save	'Active, 'Idle', 'Standby', and 'Sleep' modes	
Security	128-bit AES encryption in CBC mode Two sets of static and dynamic keys for data encryption	CBC = Cipher Block Chaining

Table 3 - Summary of MoCA 2.0 PHY and MAC Layer Parameters

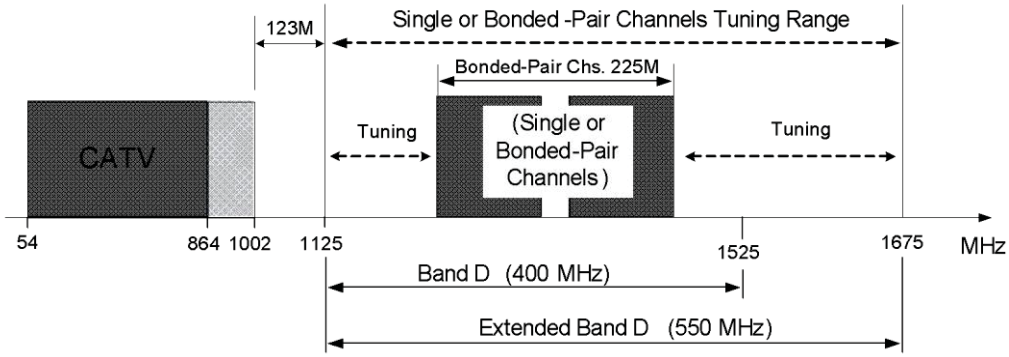


Figure 17- MoCA 2.0 Extended Band D Frequency Plan

MoCA 2.0 PHY layer operates in defined frequency bands from 400 MHz to 1675 MHz. Figure 17 shows the MoCA 2.0 Extended band D (ExD) frequency plan, which is used by most of the Cable operators in North America. Band D defined for MoCA 1.1 devices was extended from 1125 MHz to 1675 MHz, introducing two D sub-bands (D-low and D-high) so that two independent MoCA 2.0 networks can be supported. The MoCA 2.0 channels (100 MHz) are centered on a 25 MHz grid, and can be tuned in 25 MHz increments. Bonded channels (225 MHz) consist of 100 MHz primary and secondary channels centered on the 25 MHz grid with a 25 MHz gap between them. The ExD frequency plan supports mix-mode operation with MoCA 2.0 and MoCA 1.1 devices. Other frequency bands include Band E (400 MHz to 700 MHz) and band F (650 MHz to 875 MHz) used primarily by the satellite operators.

In some use cases, when a higher MAC throughput is required, MoCA 2.0 added a turbo mode support in a two-node network. In this network nodes may eliminate some MAC overhead in order to maximize the MAC throughput. The MAC throughput in a turbo mode is required to be > 500 Mbps using a 100 MHz channel, and > 1 Gbps using bonded-channels.

The MAC layer uses Time-Division-Duplexing (TDD) scheme where all the nodes on the network transmit on the same frequency, but at different time slots or transmit opportunities. All the transmit opportunities are coordinated by a single node called the Network Coordinator (NC). The NC is dynamically selected from all the nodes in the network based on which node has the best broadcast bitloading capability. The NC broadcasts to all the nodes a Media Access Plan (MAP) message approximately every 1ms, defining when each node can transmit in the upcoming time period called a MAP cycle. Thus, the NC ensures that there is no contention for the allocated transmit opportunities. During each MAP cycle, the MoCA nodes are given the opportunity to send RRs to the NC. The NC responds to all the RRs it receives in the MAP cycle by granting time slots in the next MAP cycle to as many transmissions it can. These transmission grants are sent in the next MAP message. Thus, the nodes 'know' when they should send and receive data during the upcoming MAP cycle. The MoCA 1.1 network throughput is reduced as the MoCA network expands from two nodes to more nodes due to increased overhead since the NC must schedule additional RRs, which reduces transmission time. This issue was addressed by MoCA 2.0 using OFDMA, allowing eight nodes simultaneously to send their RRs to the NC where each node is transmitting its RR on a different set of subcarriers. Not only does this reduce the overhead for the RRs, but also it reduces latency by allowing a MoCA 2.0 NC to grant RR opportunities to all the nodes every MAP cycle.[3]

MoCA defines two methods to protect video traffic from other type of traffic on the in-home coaxial network. In the first method, video is sent as prioritized traffic based on the VLAN tag. Thus, the MoCA device will provide preference to video streams with high MoCA priority compared with low-priority or untagged traffic. The second method is to send video streams using Parameterized Quality of Service (PQoS). A traffic flow with specific Traffic Specification (TSPEC) parameters is configured based on link metrics of the flow. Once the PQoS flow is admitted to the network, its bandwidth is guaranteed to be transported across the network. MoCA 2.0 defines additional TSPEC parameters for greater flow control such as maximum latency, classification rule, in-order packet delivery and retransmission.

Energy efficiency of consumer products, particularly Set-Top Boxes (STBs) and networking devices is an important requirement. U.S. Federal government and the European Commission have initiatives to regulate the maximum allowed energy consumption of STBs and networking devices.[4] To address this

[3] A. Monk, R. Lee, and Y. Hebron, "The Multimedia over Coax Alliance," Proceedings of the IEEE vol.101 (2013).
[4] European Commission, ICT Codes of Conduct – Please see

issue, MoCA 2.0 defined four power states as shown in Table 4, allowing the MoCA node under the control of its host processor to move in and out of low-power states in coordination with other MoCA devices in the network. In addition, the MoCA 2.0 specifies the rules for transitioning the MoCA device from active state to any other power states, and from the other power states back to the active state.

POWER MODE	POWER MODE NAME	DESCRIPTION
M0	Active	Normal operation of the MoCA interface; full power consumption.
M1	Idle	MoCA interface is unable to transmit data traffic, but can receive broadcast and unicast traffic; fast wake-up time.
M2	Standby	MoCA interface is unable to transmit data traffic, but can receive broadcast traffic; slower wake-up time.
M3	Sleep	MoCA interface is disconnected from the network.

Table 4 - MoCA 2.0 Power Mode Names and Description

MoCA 1.1 uses 56-bit Data Encryption Standard (DES) encryption for data traffic. The privacy of MoCA 2.0 was upgraded to 128-bit Advanced Encryption Standard (AES) encryption in Cipher Block Chaining mode. Two sets of static and dynamic keys are used for data encryption. In addition, each MoCA device has a programmable password, which is used for distinguishing between MoCA networks either in the same home or adjacent homes.

HomePlug AV and other powerline transmissions

Used for IP networking (IPVOD, CAS call-home for PPV/VOD purchase reporting, application data, and diagnostics).

Please refer to http://www.homeplug.org/ for more information.

Section III: Technologies (Functional) that enable the reception of MVPD or OTT service:

These are usage of devices technologies from above as applied to MVPD or OTT service reception.

Gateways and MVPD Provided Devices and Environments

Home Network Video and Internet Gateways (includes Residential Gateway)

Key components and features of the Residential Gateway (RG) are:

- xDSL Modem: terminates single-pair and/or bonded-pair copper connections. The modem detects the appropriate xDSL profile automatically and connects customers to the correct VDSL profile.
- Support for local network connectivity:
    - Wired: Ethernet, HPNA, MoCA

http://re.jrc.ec.europa.eu/energyefficiency/html/standby_initiative_main.htm

- Wireless: 2.4GHz 802.11n, 5GHz 802.11ac

- Supports integrated VoIP
- TR-069 Compliant, Integrated Firewall, NAT/PAT support, Diagnostics support
- Supports Ad Insertion (Also see DBS section above)
    - AT&T currently implements multiple levels of ad insertion into MediaRoom compliant streams. This includes National, VHO, and Zoned insertion. Zoned ad insertion takes place on the RG using a proprietary protocol and mechanism developed with RG vendors. Targeted ad insertion (currently in development) will take place using in-home MediaRoom DVR and STBs – again using proprietary protocols and mechanisms developed by the middleware vendor.
- Provides Battery backup for the VoIP service
- Provides broadband internet access
- May optionally support DVR capabilities
- Other key interfaces are:
    - DSL Modem, Gigabit Ethernet WAN, HPNA V3.1 Coax port, up to 4 Gigabit Ethernet LAN ports
    - 5GHz, 802.11 ac, 4x4 MIMO Wi-Fi, 2.4GHz 802.11n MIMO Wi-Fi
    - 2 VoIP lines
    - USB host support

Standalone STBs

AT&T is offering standalone wired and wireless STBs to U-verse customers. The U-verse standalone STBs are designed with a dedicated video System on Chip (SoC) with a secure core to support identification, authentication, and provisioning of services as well as Digital Right Management security system that is used for content security and protection. All of AT&T U-verse STBs are HD capable STBs and the U-verse content is encoded using the H.264/AC3/DD+ compression standards. Some of the key components of the standalone non-DVR U-verse STBs are:

- Dedicated DRAM
- Application Flash
- Boot ROM (or Secure Flash)
- 10/100 Ethernet Port bridged with HPNA – Internal Ethernet switch
- HPNA V3
- USB 2.0 port
- Composite, Component, S-Video, HDMI, Optical TOSLINK Audio outputs
- Infra-Red (IR) Remote Control
- Status LEDs

Digital Video Recorder

AT&T is offering a local Digital Video Recorder (DVR) STB with up to 1TB of HDD. Other features of the DVR STB hardware are similar to the standalone non-DVR STBs. In conjunction with the Mediaroom client software application, AT&T is using the DVR STB to offer Total Home DVR (THDVR) and Remote Pause Buffer services. The THDVR service enables customers to record and playback multiple HD channels (up to 6-record and 3 Playback) simultaneously. Customers can initiate recording sessions and playback of recorded content from any STBs within the home. In addition, the Mediaroom software along with the DVR STB, enables pausing of live TV as well as the use of trick modes on live streams from any STBs within the home. These features are based on proprietary implementations of THDVR and Remote Pause Buffer in the Mediaroom software that is licensed by AT&T. The DVR also supports the storage of ad assets and serving of these assets to other STBs within the home. See DBS section for information on DVR use in DBS systems.

Cloud or Network DVRs

MVPD's offer a Network/Multi-Room Digital Video Recording (MR-DVR) platform. Cablevision's system uses the existing STB within the home with no HDD. Other features of the MR-DVR STB are similar to the standalone DVR STBs without a pause buffer. This cloud service becomes a total Multi-Room Home DVR solution. This service enables customers to record and playback multiple HD channels (up to 15-recordings) simultaneously. Customers can initiate recording sessions and playback of recorded content from any STBs within the home. These features are based on proprietary implementations of MR-DVR based on VOD protocols. The MR-DVR system also supports the storage of ad assets and serving of these assets to other STBs within the home.

Mediaroom Applications Software

The Mediaroom application software is a proprietary IPTV application software licensed by AT&T for the U-verse service. The IPTV Mediaroom system was designed as an application platform to support the IPTV services and evolution of service features. The platform is now owned and maintained by Ericsson. The U-verse IPTV service is based on an all Internet Protocol (IP) delivery for Linear/Live and VOD. The service also encompasses a large number proprietary features and value-added services such as Instant Channel Change (ICC), Multiview, and a large number of interactive applications. The Microsoft Mediaroom DRM is used for content protection on AT&T U-verse STBs with an embedded secure SOC. U-verse is offered to third party devices such as smart phones (iOS, Android), tablets, PCs and laptops through AT&T U-verse applications. PlayReady DRM is used for content protection on these devices. Key implementation details of the AT&T U-verse IPTV features are confidential/proprietary.

Application on Retail Device

Apple iOS

Applications deployed to the Apple App Store for operation on iOS devices are written against an Apple-provided iOS SDK. These applications may incorporate code written in any of a number of languages, but Objective-C and HTML5 are historically the most common. Video applications in the iOS context are modal, though this may be changing somewhat in iOS 9. This means that content-provider library

discovery, search, and browsing are typically executed in the user-interface context of the application. Developer deployment of applications and application updates is generally managed via the Apple App Store for everyday users. Applications are submitted to Apple for review and distribution.

Google Android

Android device applications may be delivered to a device by a number of means ranging from side-loading (direct installation) to various application stores (e.g. Amazon appstore, Samsung Galaxy Apps, etc.), the Google Play store being the most popular. In the case of the Google Play store, applications are submitted to the store and made available at the discretion of the application developer. Google may remove application availability if an application is found to be malicious or otherwise harmful.

Video applications distributed on the Google Play store *may* be modal and isolated, as with iOS applications, but this is not the only mechanism for browsing integration. Instead, Android applications may expose their video programming via software interfaces that allow for system-integrated browsing, searching, discovery, and selection. Amazon's Fire TV provides similar functionality for 3rd party applications, allowing for integrated browsing, search, and discovery. Playback in both cases is handled by the 3rd party's application, but this integration between the 1st party browsing UI and 3rd party video playback UI does not require any service-specific user action. "Android TV" branded devices incorporate a local federated search mechanism whereby catalog search queries can optionally satisfied by included and downloaded applications. This mechanism allows applications to provide search "plug-ins" to give unified search results to users on these devices.

Smart TV

With a number of available Smart TV platforms (e.g. Android TV, WebOS, Tizen, Yahoo! Connected TV, Google TV, Google Cast), the approaches for application distribution and content discovery and playback are varied. Approaches to distribution and display range from generally open to curated to closed.

Generally open systems (e.g. Android TV) provide APIs and distribution mechanisms that allow for distribution control but remain largely unrestricted by their platform vendors, resorting to application restriction, for example, in cases of user harm.

More curated Smart TV platforms (e.g. LG's WebOS) provide APIs and distribution mechanisms but require platform vendor approval (typically after extensive testing and validation) before an application may be made available for use.

Further restriction is possible, leaving platform APIs and distribution mechanisms restricted by explicit agreement between platform and service vendors. At present, this group is not aware of any Smart TV platforms still using this approach to application distribution.

HTML5 with EME

HTML5 with EME encompasses a wide range of use cases for content discovery, search, navigation, and playback, as HTML5 with EME is merely a technology stack allowing for host-based provisioning

negotiation. Though HTML5 "applications" may be delivered in a number of ways, the most common approach is to receive the code and content in a browser context while interacting with a server.

PC-based "Native" applications

Personal computer-based streaming applications from individual service providers are more rare. Some, like Kodi and Boxee exist, but these are 3rd party aggregation applications often built without direct input from service providers. SlingTV supports a PC/Mac client, and PC/Mac clients exist for MVPDs and retail devices using SlingBox technology for streaming. As such, service support is inconsistent. We can look to music navigation applications (e.g. WinAmp, iTunes, Songbird, Amazon MP3) as a possible design example, but there are many distinct differences, including local library collection, high title count, and short title (track) duration. Instead, video services are more commonly deployed to computers via HTML with either EME or embedded plug-in viewing mechanisms (e.g. Flash, Silverlight).

Standalone Retail Devices

HDTV

What can be called an HDTV ranges in function from a dumb monitor to a display-integrated computer. HDTV devices generally incorporate external digital, analog, and tuner inputs, and HDTV endpoint devices may incorporate other interfaces such as USB, TOSLINK (for audio), CableCARD (on legacy HDTVs), Ethernet, WiFi, etc. Generally, HDTV devices may receive MVPD content via tuning unencrypted channels (e.g. ClearQAM, however not all cable providers have ClearQAM channels). "Smart TV" HDTV devices may also access video content over WiFi, Ethernet, or local storage connections.

DVR

Retail DVR devices vary greatly in functional characteristics and feature-sets, but a common feature among these devices is the inclusion of the ability to record programming programmatically, typically, but not necessarily, without the use of removable linear media such as videocassette or DVD+/-R. DVR systems leverage hard disk drive (HDD) and/or other local storage devices to record and retain video programs. Retail devices may be bound by regulation (e.g. Copy Control Information) with regards to this fundamental behavior. Additionally, DVR devices may include "trick play" functionality such as pause of live TV and may integrate other functionality (e.g. Netflix on TiVo devices). Furthermore, DVR functionality may be included as a functional feature in other devices (e.g. Microsoft Windows Media Center).

Portable media storage

Portable media storage devices (e.g. SD Cards, external Hard Disk Drives) may be used to store video content for later playback. These devices can be connected via a number of interfaces, the most common being USB. Content stored on these devices may be cryptographically "keyed" to be decodable on a single device or limited group of devices.

Section IV: Technologies that enable the reception of MVPD or OTT service:

This section provides information about specific technologies that enable the reception of MVPD or OTT service.

Google Fiber IPTV System Overview

Summary

This outlines the various components of the Google Fiber IPTV service. It's purpose is to explain how we may operate differently than other MVPDs and also to explain how it's service could be adapted to work with a market for 3rd party retail navigation devices. Overall, Google Fiber operates like most MVPDs do with regards to having installers, CSRs, headends, content ingestion/transcoding/distribution and in home STBs.

Linear TV Feeds

Linear TV channels are sent out over IPTV multicast (UDP multicast). The channels use H264 video encoding and either MPEG or Dolby Digital audio encoding. The transport layer is a single program MPEG2 Transport Stream. They carry multiple audio tracks when present. Closed captioning and AFD information is also retained in these streams. Retransmitted local broadcast channels are sent without encryption. All other channels are encrypted using Widevine with EMM/ECM data present in the stream. Households that do not subscribe to the TV service have the IPTV multicast signal blocked at the network level.

Video on Demand

Google Fiber has all types of VOD content; free, subscription based and transactional. VOD content is served over HTTP and encrypted using Widevine. The streaming format is specific to the Widevine VOD implementation that is used. We also provide VOD content served over the DASH protocol [40]; which is currently utilized by our mobile/tablet clients and will likely transition to this protocol for all VOD streaming in the near future. VOD streamed via DASH supports playback using standard EME.

Metadata

Metadata relating to the program guide information and VOD content is delivered via HTTP to the clients. This data also contains the mappings of logical TV channels to their actual multicast IP:port. It comes down as a compressed BLOB of data which is a delta of the information from the last retrieval. It is also possible to download the full set of information, which is what occurs for a newly provisioned STB. The data is in a proprietary format. Imagery associated with the metadata has URLs specified in the metadata so those images can be retrieved for presentation in the user interface.

Content Authorization

A secure HTTP RPC service is provided for clients to retrieve information relating to content authorization and subscribed channels. Connection to this service requires validation of security certificates in a bi-directional manner (i.e. SSL where both client & server certificates are validated). This service provides the information on what specific channel lineup the device should be using (so it can then request the proper metadata). It also provides a list of all the devices in the home that our whole home DVR storage box is allowed to communicate with. It also lists all of the channels that the user is authorized for viewing. The DRM components in the client also connect to this same service in order to obtain the data they need in order to enable decryption of the subscribed linear TV channels and

authorized/purchased VOD content and know the output protection rules associated with that content. (NOTE: These are not the actual encryption keys, but keys that in conjunction with the DRM secrets loaded into the device along with the ECM/EMM information in the MPEG stream allows it to generate the decryption keys for the content. Keys are rotated on a regular basis for the linear TV channels.)

Emergency Alert

EAS information is sent out over an IPTV multicast feed and contains all the information the device would need in order to properly respond to an EAS/EAN event.

Monitoring & Logging

Device logs are uploaded regularly to Google servers for analysis and processing. We use the TR-069 protocol for management, provisioning, remote configuration and other types of data collection.

Slingbox

The Slingbox is a TV placeshifting device that allows users to watch their live TV or DVR content anywhere via an IP connection. It is able to connect to virtually any MVPD's STB. Connections are only 1-1, meaning a single session per Slingbox.

Please refer to http://www.slingbox.com/ for more information.

Mediaroom

In order for a third party to implement the Mediaroom features, they need to license the Mediaroom platform. The following provides a high level overview of the two key features:

ICC: instant channel change is achieved by a combination of TCP and UDP IP traffic for a specific channel and detailed implementation of ICC is confidential.

RUDP: Resilient UDP is another technology used by Microsoft to provide reliability. This is also a proprietary Microsoft technology.

Section V: OTT Services

Some OTT services have different applications on different platforms. Table 5 describes the operation of each application for the discovery and reception of content on a sample set of OTT services. This table is not intended to be comprehensive or a survey of all current OTT services.

	Discovery	Reception	Content Type	Content source	Business model(s)	Ad support
Amazon	In-app and platform search and browse	Streaming and Download	Long Form TV and Film	3rd party (studio) and 1st party	Rent, Sale, and subscription	Content promo only
Netflix	In-app and platform search and browse	Streaming	Long Form TV and Film	3rd party (studio) and 1st party	Subscription	No

Hulu	In-app and platform search and browse	Streaming	Long Form TV and Film	3rd party (studio), regional exclusive, and 1st party	Ad-supported (always) and subscription	Yes
YouTube	In-app and platform search and browse	Streaming	Originally Short Form, now unlimited	Largely 3rd party sourced (user submission) with some 1st party content	Ad supported and (pending) subscription	Yes
SlingTV	In-app and platform search and browse	Streaming	Live Programming	Broadcaster/channel	Subscription with optional add-ons, VOD, and C3 (subscription inclusive)	In-band with live content

Table 5 - Sample OTT Service ca. Summer 2015

Section VI: Essential Customer Experiences

Include messaging and protocols that enable these experiences during analysis.

PURPOSE

Through a series of Use Cases, specify the content subscription service elements that are currently available and used by the market.

INTRODUCTION

These Use Cases serve to identify and describe the current service features that an end-subscriber (consumer) may gain access to when they have a subscription to a content service.

Examples of a content subscription service would be a subscription to a Multichannel Video Programming Distributor (MVPD) or an Over-The-Top (OTT) service. The dissemination of these services can be transmitted through a series of paths, such as cable, satellite or via an Internet connection or a combination thereof.

It is important to note that these subscriptions are governed by agreements made among several parties. Users traditionally enter into agreements with the content subscription service. Content subscription service providers typically enter into multiple agreements, including with content providers, advertisers, metadata providers, CAS and DRM vendors, OEM set-top box manufacturers, and others. Third party manufacturers currently enter into, and are bound by, specific licenses (such as DFAST) and/or specific business arrangements, and regulatory and legal requirements.

This group of agreements governs the content ecosystem that is currently accessed by the subscriber. The following Uses Cases take into account these agreements.

Outlining and categorizing virtually every service feature available aids in the identification of the salient differences amongst the categories and service offerings. Some of the devices reviewed by the DSTAC Working Group support only some use cases or only some features within a use case. The report

analyzes the features and use cases that are or should be supported. That analysis may assist in evaluating alternative systems and features that are or should be baseline requirements for service providers and device manufactures, as well as the evaluation of platforms or devices in the marketplace that are able to satisfy these Use Cases.

It should also be noted that these Uses Cases may change over time. The purpose of this document is to relay Use Cases based on current market availability.

END-USER Precondition:

In each of these use cases, the consumer already has a subscription with an MVPD or OTT provider.

USE CASE #1 - Tuning and Viewing a Linear Channel

USE CASE DESCRIPTION

This use case covers when a subscriber tunes to a new channel using channel up/down, direct channel entry, or from other navigation (the linear and on-demand navigation use case is covered below).

TRANSMISSION METHODS

While an MVPD device must only support the transmission methods for the MVPD's network, a retail device for this use case should be able to support methods for transmission of linear channels, including:

TRANSMISSION METHOD	ACTIVE EXAMPLE
Analog	There are a small amount of Cable operators in the country who still transmit some channels using analog transmission methods.
QAM broadcast	Quadrature Amplitude Modulation (QAM) is the standard for broadcast of digital video on cable networks today. In the United States, the QAM standard used is ANSI/SCTE 07, 2000: Digital Video Transmission Standard for Cable Television.
QPSK DVB-S	Quadra-phase Shift Keying (QPSK) is a modulation system used in DNBS broadcast systems. DVB-S is an advanced coding system defined by DVB.
QPSK DSS broadcast	See *International Telecommunications Union, Recommendation ITU-R BO.1516, 2001, "Digital multiprogramme television systems for use by satellite operating in the 11/12 GHz frequency range, System B"*

TRANSMISSION METHOD	ACTIVE EXAMPLE
DVB-S2 broadcast	DVB-S2 is an advanced coding system defined by DVB. See "Digital Video Broadcasting (DVB) User guidelines for the second generation system for Broadcasting, Interactive Services, News Gathering and other broadband satellite applications (DVB-S2), ETSI TR 102 376, V1.1.1, February 2005."
QPSK and 8-PSK Turbo broadcast	8-way-phase Shift keying 8-PSK
Multicast User Datagram Protocol (UDP)	See Google Fiber section for example.
Multicast Real-Time Protocol (RTP with custom adaptation layer) over UDP	See AT&T section above for usage example.
Unicast RTP (with custom adaptation layer) over UDP	The U-verse TV system uses unicast RTP based messages to deliver instant channel change video payload to the client. When booted, each STB receives a listing of video session assignments to a specific Distribution server (D-Server) from the D-Server cluster. The Payload is delivered vis Unicast RTP over UDP by the D-Server. The RTP adaptation fields contain information that identifies various real-time events such as Blackout markers and tables, Random Access Points (RAP) among others. In addition to this, the D-Server may add event specific markers to the RTP extension for a specific request. The unicast RTP delivery is also used for delivering error correction payloads for lost or corrupted packets as part of the resilient UDP (RUDP) mechanism.
QAM switched digital video (SDV)	Switched Digital Video (SDV) for QAM networks is a method of implementing IP multicast using broadcast QAM transport

TRANSMISSION METHOD	ACTIVE EXAMPLE
	rather than IP. This permits only those broadcast channels in a service group that are being watched to be transmitted to that service group. Those channels which are not being watched in a service group are not transmitted and thus save bandwidth enabling more channels to be carried in the same amount of bandwidth as a purely broadcast system. The two-way out-of-band channel used on the particular system provides the two-way communication path necessary for a set-top to request a particular SDV channel using a proprietary protocol.
NACK-Oriented Reliable Multicast (NORM) Transport Protocol	NORM is an IETF RFC for a protocol that can provide end-to-end reliable transport of video streams over generic IP multicast routing and forwarding services. CableLabs recently issued several specifications that use NORM for transport of Adaptive Bit-Rate video streams over IP multicast. The relevant specifications are: ● IP Multicast Server – Client Interface Specification, OC-SP-MS-EMCI, Cable Television Laboratories, Inc. ● IP Multicast Controller-Server Interface Specification, OC-SP-MC-MSI, Cable Television Laboratories, Inc. ● IP Multicast Controller-Client Interface Specification, OC-SP-MC-EMCI, Cable Television Laboratories, Inc. IETF RFC 5740, NACK-Oriented Reliable Multicast (NORM) Transport Protocol, November 2009.

As some MVPDs transition to converged IP networks, new transmission methods will be introduced and some transmission methods will be deprecated. Examples of IP streaming include HLS [38] and DASH [40].

CODEC SUPPORT

While an MVPD device must only support the codecs used by the MVPD's network, a retail device for this use case should support audio and video codecs, including:

- MPEG-2 [6] (Note that DBS systems will typically use GOP structures lasting multiple seconds.)
- MPEG-4 AVC/H.264
- HEVC/H.265
- MPEG-1 Audio
- Dolby AC3
- Dolby Digital Plus
- AAC
- AAC Plus

The following table lists examples of codecs and how they are currently being used by the listed entities.

MVPD	Transport	Control Channel	Video Codec
Cable	• QAM/MPEG-2 TS • QAM/MPEG-2 TS • QAM/MPEG-2 TS • QAM/MPEG-2 TS • QAM/MPEG-2 TS • QAM/MPEG-2 TS	• SCTE-55-1 • SCTE-55-1/DOCSIS • DOCSIS • SCTE-55-2/DOCSIS • In-Band • Generic IP	• MPEG-2/AVC • MPEG-2/AVC • MPEG-2/AVC • MPEG-2/AVC • MPEG-2/AVC • MPEG-2/AVC
Satellite	• QPSK/DSS TS, DVB-S2/MPEG-2 TS • (QPSK, DVB-S, 8-PSK Turbo)/MPEG-2 TS	• In-Band • In-Band	• MPEG-2/AVC • MPEG-2/AVC
Off-Air	• 8-VSB/MPEG-2 TS	N/A	
Telco	• Multicast/Unicast-IP/VDSL/FTTP • QAM/MPEG-2 TS & IP/BPON or IP/GPON	• IP/VDSL/FTTP • SCTE-55-1/SCTE-55-2	• AVC • MPEG-2/AVC
Google Fiber TV	• IP/GPON/MPEG-2 TS	• IP/GPON	• AVC

Table 6 - Transport, Control, And Codec Support

NOTE: A earlier version of this table was cited within the DSTAC Working Group 2 report **Error! Reference source not found.** (as "Table 1 Currently Deployed CAS Systems") and was described as a summary of known, deployed CAS systems, each of which has its own unique licensing and trust infrastructure, along with the associated core ciphers, transports, control channels, and video codecs in use.

As new video and audio codecs are introduced, MVPDs will take advantage of them. Over time some codecs will be deprecated. In instances where a separate decoder is used these aforementioned codecs may not be called upon for use. For example, a gateway device might not have an HDMI output, and

therefore have no decoders on board. The device with the decoder would be the end point client device, such as a tablet or RUI client.

IMAGE QUALITY

While an MVPD device must only support the picture resolutions and formats used on the MVPD's network, a retail device for this use case should be capable of supporting common picture resolutions and formats, including:

- SD 480i/480p
- HD 720p (30 and 60 fps)
- HD 1080i
- HD 1080p (24 and 30 fps)
- 4K and UltraHD (High Dynamic Range (HDR), Wide Color Gamut, deep pixel depth)
- 3D frame compatible (Side-by-side, Top-and-Bottom, Interlace)

As new picture resolutions and formats are introduced, MVPDs will take advantage of them. Over time some resolutions and formats will be deprecated.

Because content may be decoded to various resolutions and refresh rates, devices displaying content to different target resolutions and rates should be capable of spatially and temporally resampling supplied content to maintain spatial and temporal consistency. Example algorithms include, but are not limited to, nearest-neighbor, bilinear, Lanczos.

Normative References:

- ARIB STD-B56, "UHDTV System Parameters for Programme Production"

STREAM MANAGEMENT (Resource Allocation)

Stream management is the allocation of stream resources within a defined network. Where necessary, a device for this use case must support the concurrent stream management required to limit the number of concurrent streams that a subscriber can receive and/or view. Stream management is also used to manage the number of simultaneous ingress and egress streams for THDVR.

The device shall limit streams to be consistent with the number of authorized access points. Note that stream management is not limited to solely HD and SD streams.

Stream management is necessary when addressing access network bandwidth limitations, tuner limitations (in particular in the case of satellite) or fraud prevention (credential or password sharing).

SYSTEM	ACTIVE EXAMPLE
AT&T U-Verse	Stream management used by Mediaroom is a proprietary implementation that manages the number concurrent WAN streams (coming to the home) and DVR record and playback streams. This feature is part of the Mediaroom application software running on the STBs.
DBS	DBS receivers typically have limited numbers of tuners that are distributed among DVR recordings, attached displays, and network displays.

SYSTEM	ACTIVE EXAMPLE
	Management of tuner resources is a task for the main server in a DBS installation.
CableCARD	CableCARD supports 6 concurrent programs with 120Mbit maximum bandwidth.

Table 7 - Examples of Stream Management

SWITCHED DIGITAL VIDEO

Switched Digital Video (SDV) allows an MVPD to make efficient use of bandwidth by only broadcasting those channels that are currently being watched within a given area, e.g., a node, or neighborhood. This allows the MVDP to use the reclaimed bandwidth for other services, including higher data speeds. The network looks for tell-tale signs of viewer inactivity, asks the viewer if he or she is still watching, and recovers the channel if there is no response. The exact SDV techniques vary by vendor, but they rely upon SDV client software in the customer device or a tuning adapter as well as two way communication. For SDV to work within retail devices without the requirement of an external MVPD-specific tuning adapter, all current implementations would need to be ported and a predictable software client would need to be present in the retail device. These solutions would need to be tested for operability and for functional tuning performance across MVPDs, and room would need to be left for the implementations to continue to evolve and improve. If there is no client to communicate viewing status upstream, there is no recovery of bandwidth, and SDV would fail in its essential purpose of opening bandwidth for more channels, more high-definition, faster broadband and more advanced services. See below for high level overview of SDV. External tuning adapters are used by some UDCPs to receive SDV.

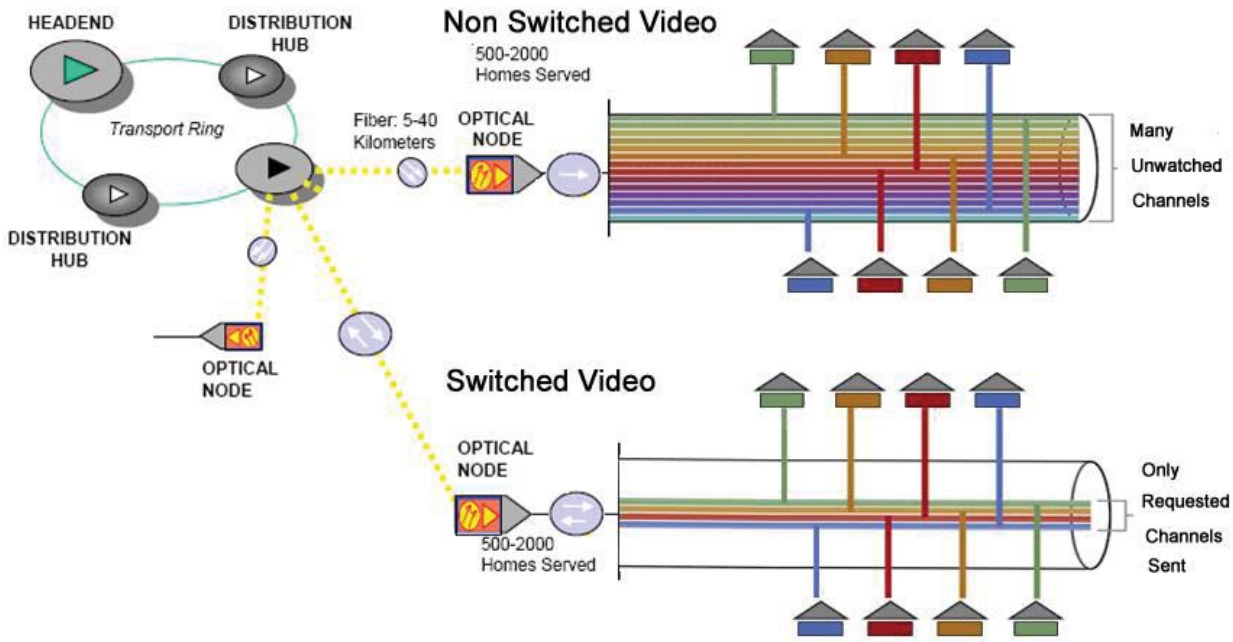


Figure 18- Switched and Non Switched Video

Some of the key elements of SDV are:

- Dynamic channel mapping information identifying the current channels being transmitted into a service group and their tuning information.
- Tuning requirements (methods).
- Keep-alive messages, indicating that a channel is still being watched.
- Time-outs, indicating that a channel may potentially no longer being viewed based on the lack of viewer activity via the remote control.
- Customer notifications (e.g., tear-down of channel), to insure that the viewer is in fact no longer watching the channel, before actually taking down the channel.

APPLICATIONS

Applications provide additional information or access to additional services, as selected by or subscribed to, by the User. A device with the ability to support integrated or program synchronous applications, should ensure that integrated applications or applications associated with the tuned channel, are presented and accessible to the User. Currently, some technologies used are Widgets, Enhanced TV (EBIF) [37], and MediaRoom. Other proprietary applications, such as those related to OTT services, may also be supported by the device.

Examples of integrated or program synchronous applications include:

- Headlines ticker
- Instant local weather
- Sports scores and statistics
- Shop by remote
- Bookmarking ads
- Social networks (Twitter, IM, SMS, etc.)
- Mosaic channels
- Telescoping
- Auto-tune HD
- “Mix” channels (mosaic of multiple channels / camera angles)
- Set timers (e.g. for future sport events or tune to current events)
- Communication service compatibility
    - Voicemail, CallerID requires integration with telephone networks
    - May be used for home automation and home security networks

ADVERTISING

Advertising messaging, when part of a service, should not be deliberately filtered out. The following advertising models must be supported:

- Local insertion of broadcast advertising into linear television
- Local insertion of zoned or targeted advertising into linear television
    i) Must receive if delivered from network
    ii) Must securely store & delete in device and insert if managed by the device
- Interactive Request For Information (RFI)
- Telescoping to on-demand advertising
- Must honor and be compliant with advertising rules, such as:
    i) Rules about ads in conjunction with a network’s video
    ii) Rules preventing interference, substitution or removal of ads

iii) Limitations on web links when programming is directed to children
iv) Rules about the inclusion of advertisements, promotions, sponsorships, and/or overlays that are displayed, in or around, a network's video window (linear & VOD) while the guide experience is engaged.
v) Support for availability windows (e.g., C3 or Post-C3 ad loads)

- Ad measurement and reporting
  i) Report back the display of an ad for frequency limits or analytics of reach of the ad campaign
- Protection of ad boundaries, especially as it relates to substitute programming or downstream devices
- Ad asset storage and lifecycle management
- Integration with Ad Decision Management (ADM) and Ad Decision Systems (ADS)
- Honor C+3, C+7, etc. ad insertion rules for DVR content playback

This use case also requires support for an audit trail to validate that the advertising has been presented as relayed.

DEVICE REQUIREMENTS

1) A device must ensure that blackouts are supported.
   a. Content delivered to the device (e.g., from satellite or cable distribution hub or IPTV super hub office) must be blacked out if not authorized (e.g., in-home vs. out-of-home, in-market vs. out-of-market, in-region vs. out-of-region, domestic vs. international).
   b. Customer notifications, including messaging, signaling & placement (e.g., notifying customers of blackout restrictions or alternate programming requirements).
2) A device must support parental control.
   a. Content delivered to the device must not be tuned or must not be presented if restricted by Parental Control (PIN setting and resetting both via device and through customer support, PIN enabling and disabling, PIN entry).
   b. Adult title blocks.
   c. Requirements: §§ 624(d)(2) and 640, 47 U.S.C. §§ 544(d)(2) and 560
   d. Supporting standards: CEA-608, CEA-708, CEA-766.
3) A device should support Alternative Content.
   a. The device must receive and insert appropriate content as alternate to regional blackouts (sports, network non-duplication, syndicated exclusivity) or other programming rights restrictions (e.g., in-home vs. out-of-home).
   b. Customer notifications, including messaging, signaling & placement.
   c. Advertising substitutions to accommodate content and channel ratings.
4) The device must support messaging and redirection for unauthorized channels.
5) The device must enforce copy control, image constraint, and selectable outputs control as indicated by CCI or on-demand applications.
6) The device must enforce copy count limitations.
7) The device must enforce pass-through/regeneration of copy control information on outputs (e.g., CGMS-a, APS).
8) The device must enforce/allow transit, delay/latency and round-trip time restrictions beyond those defined by standards such as DTCP or HDCP.

9) The device must not deliberately filter out watermarks (video, audio, other). Watermarks, in this case, are forensic markers embedded into a piece of content to permit after-the-fact detection of the source of security breaches.
10) The device must enforce geo-filtering and geo-fencing requirements & restrictions beyond blackouts (e.g., alternate programming).
    a. E.g., restrictions/requirement for what can be displayed in common areas, commercial/university properties
11) The device should support and must tolerate the presence of Active Format Descriptor (AFD) signaling (e.g., letterbox, center-cut an HD signal to fit SD presentation).
    a. Normative references: CEA-805, ATSC (A/65, A/81), SMPTE AFD.
12) The device must support transcoding or down-res'ing restrictions or requirements (e.g., minimum encoding bitrates/quality).
13) The device should support the feature of HD channel preferred.
    a. When the subscriber tunes to a simulcast SD channel the device suggests tuning to the HD version, or does so automatically if configured accordingly.

AUDIENCE MEASUREMENT

Audience measurement is the ability to report back viewing metrics based on anonymized census-level audience data derived from set-tops. This is a non-intrusive service. Current audience measurement techniques enable MVPDs to measure audiences for channels and when viewers tune in and tune out. This helps to determine which programs are most popular, how many people watch a program to its conclusion, what viewership to report to advertisers, which programs and channels to carry, how to optimize programming to meet changing viewer demand, and how to sell advertising that underwrites the programming and networks provider to consumers. Examples include: Audience measurement of long tail and small market programming; Audience measurement to allow ad buyers to buy advertising in specific dayparts and networks; DBS delivery of targeted ads based on household characteristics; Consumer-packaged-goods companies measuring ROI by correlating campaigns with lift in sales.

PLAYBACK

This use case requires the activation of trick play capability of live TV, e.g. pause, fast forward, and rewind, each at multiple speeds and may be enacted through the following methods:

- Time shift buffer
- Using local DVR
- Using network DVR

Pause and Resume are currently available and traditional features. The device and system should support pausing content on one device and resuming from another device.

INSTANT CHANNEL CHANGE

Some MVPD devices support Instant Channel Change (ICC), a feature that minimizes or eliminates channel change latency, depending on the MVPD's network. A retail device for this use case should support and include a variety of different methods of implementing ICC, including:

- IPTV – multicast and unicast RTP/UDP/IP
- QAM SDV
- Broadband tuners and demodulators

- Opportunistic device caching
- Pre-decoding of adjacent channels, with associated stream count limitations enforced.

REGULATORY REQUIREMENTS

There are a number of regulatory requirements for this use case. A device should support all service provider and device regulatory requirements, as obligated by law. Examples of regulations include:

- Safety and interference requirements.
- Emergency Information
  - Emergency Alert System (EAS) local and regional. Receives EAS on all channels. Supports force tune and text crawls with audio replacement.
  - Emergency Information: When emergency information is conveyed visually during non-newscasts (such as in on-screen crawl), the secondary audio stream must be used to convey such emergency information aurally, preempting any other use of SAP, such as DVS or foreign-language.
- Accessibility Access (e.g., top-level vs. lower-level; ease of access)
- Advanced Communications Services (ACS), such as two way electronic messaging services (e.g., real-time text and video chat applications), must be accessible to and usable by persons who are blind or have limited vision
  - On July 1, 2016, the waiver of the ACS requirement is set to expire. The waiver includes IP-TVs, IP-Digital Video Players (DVPs), and Set-Top-Boxes leased by cable operators.
- Nielsen
  - Audio watermark pass-through
  - ID3 tag pass-through and/or regeneration
- Commercial Advertising Loudness Mitigation (CALM) Act
- Pass-through of VBI (analog) (e.g., V-Chip, CC, VITC, etc.) and regeneration of digital counterpart.

Normative References:

- Accessibility: 47 C.F.R. Parts 14, 79; SMPTE ST 2052-1-2010, Timed Text Format (SMPTE-TT)
- CALM: 47 CFR §76.607; ATSC Recommended Practice (RP) A/85
- EAS: 47 C.F.R. Part 11
- Nielsen: 47 C.F.R. §§76.62; Carriage of Digital Broadcast Signals, 16 FCC Rcd 2598 ¶ 61 (2001).
- Privacy: 47 U.S.C. §§ 338(i), 551
- Pass-through & V-Chip: 47 U.S.C. § 534(b)(3); 47 C.F.R. §§76.62; 76.606; ATSC A/65 PSIP standard; Carriage of Digital Broadcast Signals, 16 FCC Rcd 2598 ¶ 61 (2001); Second Periodic Review of the Commission's Rules and Policies Affecting the Conversion to Digital Television, 19 FCC Rcd 18279, ¶¶ 154-159 (2004).
- Parental control: §§ 624(d)(2) and 640, 47 U.S.C. §§ 544(d)(2) and 560

USE CASE #2 - Viewing On-Demand Content

USE CASE DESCRIPTION

This use case incorporates the features laid out within the Linear Content Use Case.

This use case also covers the multiple forms of on-demand content consumption, examples include:

- Transactional VoD (rental transaction, including purchase screen)
- Subscription VoD (premium subscription content, authorization only)
- Free VoD (non-premium content, no authorization or purchase screen)
- Electronic Sell Through (EST, purchase screen on first viewing only, authorization only on subsequent viewing)
- Start Over™ (similar to subscription VoD, but contextual)
- Look Back™ (similar to subscription VoD)
- Purchase PIN (PIN setting and resetting both on TV and through customer support, PIN enabling and disabling, PIN entry)
- Device meets trick play requirements, e.g. disables FF with OD content (typically during advertisements), per content provider condition, disable skip (e.g., 30-second skip) for full assets or intra-asset.
- 3rd party devices may purchase and display VOD from MVPD and OTT services via 2-way agreements.
- 3rd party devices may support a purchase of MVPD provided content.

In satellite systems, each of these can furthermore be implemented via a priori staging of content on local DVR storage. Devices interacting with DBS systems must accept catalog information from the attached DBS gateway – depending on download history and broadband connectivity, any particular DBS gateway will have unique sets of VOD content available. The variations in content and viewing window will include variations of resolution (1080p/3-D/UHD/HD (1080i & 720p)/SD, etc.) and pricing.

USE CASE #3 - Tuning and Viewing Pay Per View (PPV) events

USE CASE DESCRIPTION

This use case incorporates the features laid out within the Linear Content Use Case.

This use case covers the purchase and viewing of PPV events including the following PPV features:

- Free preview window – period of time subscriber can view PPV event without paying.
- Purchase window – period of time subscriber can purchase the PPV event.
- Cancellation window – period of time during which subscriber can cancel the purchase of the PPV event
- Secure purchase credits and purchase limits – In general, PPV event purchases are done on a store and forward basis, purchases are stored securely, set-tops are provisioned with limits on the number or amount of purchases that can be made before the purchases are collected
- User interface required to present time remaining in preview, purchase, and cancellation windows, as well as the transaction and when the purchase limit is exceeded, including messaging capabilities (e.g., call-in numbers, contact information)
- Purchase PIN (PIN setting and resetting both on TV and through customer support, PIN enabling and disabling, PIN entry)
- Auditing and reporting
- Devices interacting with DBS systems must accept guide data from the attached DBS gateway – accurate guide data is available for in-home use. The variations in content will include variations of resolution (1080p/3-D/UHD/HD (1080i & 720p)/SD, etc.) and pricing.
- Limited time recording of PPV events on 3rd party devices may be supported.
- 3rd party devices must support a purchase UI controlled by the MVPD system.

USE CASE #4 - Navigation

USE CASE DESCRIPTION

This use case covers the broad range of methods for navigating linear and on-demand content. Regardless of the method, the navigation must respect the content provider's license agreements about channel placement and neighborhoods. There is a significant effort that goes into the navigation to optimize consumer satisfaction and make it easy to use / enjoy features of the service.

There are many different methods of navigating linear and on-demand content that should be considered, some examples include:

- Provide a familiar or similar interface across the multiple devices consumers use to access the service
- Grid guide
- Cloud based guide variants / RUI
- Talking guide
- Emergency Information settings & accessibility
- Closed Captioning settings & accessibility
- Channel presentation in required neighborhoods (e.g., news channels) and channel assignments (e.g., broadcaster carriage on channel)
- Favorite channels, recent tuning history, bookmarks, etc.
- Recent tuning history across devices
- Mosaics & associated navigation
- Cover art
- Channel logos
- Thumbnails
- Search – including both locally-based and network-based
- Network-branded points of entry, e.g. content provider requires that their on-demand content be accessible through a network-branded folder labeled "Disney" or "HBO" rather than just being commingled with other on-demand content
- Multiple guide view…genre, by network
- Devices interacting with DBS systems must accept guide data from the attached DBS gateway – accurate guide data is available for in-home use. Variations between particular homes will include blackout and local channel availability, and will require a generated guide to accurately reflect conditions in any particular subscriber's home.
- Both HD and SD versions of channels may be available with otherwise identical service and event information. Standardized table structures may not distinguish between 3-D, UHD, HD and SD versions.
- Recommendations from user profile across devices
- Recommendations from what's trending or popular in neighborhood
- Trick play – fast forward and/or rewind, at multiple speeds, skip chaptering, etc.
- Navigating and Billing for VOD including:
    - Verification of purchase
    - Offer of multiple options (e.g., rent or EST)
    - Integration with billing system/account management
    - Record customer purchases
- Search, including:

    - Voice control via remote
    - Voice control smart phone, tablet or similar device
- Whole Home capabilities:
    - Ability to advertise services to the home network
    - Ability to discover services on the home network

Multiple features above may be combined in the navigation functions.

USE CASE #5 - Recording Linear Content

USE CASE DESCRIPTION

This use case includes all of the features of the Linear Content Use Case and also covers the recording of linear content via Digital Video Recording (DVR) capabilities. If recording rights are available for a particular channel or event, then also see linear tuning use case for additional features.

There are a number of implementations that should be considered:

- Record on local hard disk drive
- Record on whole home DVR and supporting home network protocols
- Record on Remote Pause Buffer (Pausing Live TV from any STBs within the house)
- Record on Network or Remote Storage DVR (similar to subscription VoD, but on a per subscriber basis, with associated database and navigation)
- Time-shift-buffering and limitations (e.g., restricted to 30 minutes)
- Record timers based on:
    - Content type: first time airing, reruns
- Content removal incited by the timed recording.
    - Content can be expunged based on settings related to number of recordings to keep, priority, etc.
- Record on mobile device, side car recording
- Move recorded content onto an authorized device(s)
    - A “move” removes the content from the source device. No copies are to be made in a “move” scenario.

To support accessibility requirements and choices made during playback, 3rd party devices must preserve all audio streams and associated metadata at the time of initial recording.

Recording rights may differ on a channel and/or event basis.

Recording rights may change over time and should be verified at the time of recording.

USE CASE #6 - Remote Management by Consumer

USE CASE DESCRIPTION

This use case covers management functions available to the subscriber remotely or on a network-connected mobile device.

RELATED REQUIREMENTS

Management of Tuning

Management of the service by the subscriber remotely, including by the primary display and by a network-connected mobile or second screen device:

- DVR scheduling
- Content search
- Remote control
- Parental controls, including device restrictions (e.g., by channel, rating, time-of-day, etc.)
- Management of some DBS gateways may require security certificates available from the MVPD.

Management of Account

Management of the account by the subscriber remotely, including by the primary display and by a network-connected mobile or second screen device:

- Account management, pay your bill via integration with billing system
- Subscription management – ability to upgrade or downgrade service packages on-screen with remote, requires access to service catalog and integration with the billing system
- Self-help customer service support items (e.g. schedule a service call or appointment)
- Subscriber Account Management may be supported on standard HTML5 web browsers that are connected to an MVPD's internet site.
- Account and password information should not be cached by an unsecure device or in unsecured/unencrypted storage.

USE CASE #7 - Set-Top Box set-up

USE CASE DESCRIPTION

This use case covers how a subscriber can set-up a number of preferences for the operation of their set-top box, including:

- Menu Preferences, such as changing the background darkness level and auto-tuning to HD channels, overscan of image, on-screen overlays and their positioning.
- Device Settings
    - Closed captioning
    - Audio settings
    - Light brightness of your set-top box
    - Inactivity standby options
    - Nightly reset time
    - EPG preferences (size, favorite channel list)
    - Remote control setup for 3rd party devices (TV, A/V receiver)
    - Audio output format and volume leveling settings
    - Control of HDMI-CEC for 3rd party devices (TV, AV Receiver)
    - Output video resolution to TV:
        - SD 480i
        - ED 480p
        - HD 720p

    - HD 1080i
    - HD 1080p
    - UHD 2160p
- Parental Controls, see above
- PIN Controls, see above
- Accessibility (e.g., Closed Captioning, audio track selection, etc. – see above)
- Many settings and options will only be available through the MVPD device UI.

Management of Device

Management of the device settings by the subscriber, including by the primary display and by a network-connected mobile or second screen device:

- Captioning
- Language selection
- Energy management
- Remote management and other tasks may require access to the video output or UI pages generated by an MVPD device.

USE CASE #8 - Customer Support and Remote Management by Service Provider

USE CASE DESCRIPTION

This use case covers customer support and remote management features provided by the MVPD.

- Remote diagnostics
- On-screen diagnostics
- Ability to disable a device and display a notification (e.g. Call your service provider)
- Backup of set-top box configuration in the network (e.g. preserves DVR scheduling, configuration preferences, etc.)
- Unified remote control experience
- Reporting back on statistics like signal level, device temperature and crash reports
- Software updates
- Some MVPD devices may save device and user settings in associated remote control devices.
- CSR support will require the subscriber to access the MVPD's device UI and may require access to raw video output of the MVPD device.

USE CASE #9 - Installation and Provisioning

USE CASE DESCRIPTION

This use case should describe the installation and provisioning of the service and customer premise equipment necessary to receive the service. This use case should cover the range of installation from self-install to professional install, and should include home networking setup of multiple display devices (retail and MVPD/OTT) in the home.

This use case includes functionality to verify the quality of an installation (e.g. correct orientation of a satellite dish) prior to allowing authorization of services.

- Ensure pre-requisites for service have been met by customer – i.e. network access setup and configuration, Wireless network, home wiring, etc.
- If Ethernet over Coax technologies (i.e. HPNA or MoCA) are used, coaxial home wiring should be tested before installing STBs to ensure proper network connectivity and throughput
- When wireless home networking is used, installers should verify rate, reach, Wi-Fi interference to ensure high quality of service over Wi-Fi
- Secure Register with unique Consumer Device ID with backend systems to receive service authentication and access data
- Ensure that customers are correctly provisioned for the services/packages they sign up for
- During installation verify the following:
    - Service is up and running
    - Remote control functions properly
    - All services features (i.e. ICC, THDVR, etc…) and interactive applications are operational
- Some in-home network technologies will not interoperate with more than one MVPD present. Parallel wiring may be required.

DBS-RELATED REQUIREMENTS

DBS systems need to be able to:

- identify the customer's satellite matrix (which satellites are visible, and how to connect and tune to them through a multiswitch),
- connect to "slim" clients within the house,
- prompt for STB authorization requests (e.g.,. call for authorization),
- Configure STB remote to control TVs, A/V Receivers, DVD/Blu-ray players that may be connected to the system, universal remote setup, and configuration of IR-Blasters for control of VCRs.
- Professional installation of service will require access to the video output (HDMI, Component, composite) of provided gateway device.
- MVPD provided devices will require access to DBS broadcast to download current device software.

USE CASE #10 - Device Operation Requirements

USE CASE DESCRIPTION

This use case covers additional features that normally run in the background, and are generally part of maintenance, security, and efficiency interests. Such interests place requirements on the device, for example:

Software Updates

Software updates for retail devices are typically the responsibility of the device manufacturer, while software updates for MVPD provided devices are typically the responsibility of the MVPD. There are some instances, for example DOCSIS cable modems purchased at retail, in which the cable operator may assume responsibility for software updates to insure that network interoperability is maintained. Methods by which software updates are disseminated and secured for retail devices is also typically determined by the retail device manufacturer. Frequently, software updates for retail devices are disseminated over the Internet, which assures two-way communication and permits validation of the

receipt and successful, secure installation of the software update on the retail device. Methods by which software updates are disseminated and secured by MVPDs are specific to the MVPD, as well as performed over the MVPD's network. CableLabs specifies a secure software download mechanism as part of the DOCSIS and PacketCable (VoIP) specifications. Secure software download is tested as part of the certification of these devices.

Privacy and security

- Device secured against unauthorized access
- System requires court process for access by government
- Device must have required registered certificates for encrypted communications with backend systems.
- Device must comport to FCC and FTC rules on privacy.
- May need to access raw video output during countermeasure checks.

Energy Efficiency requirements (Voluntary Agreement for set-top boxes)

Including configurability of sleep timers, inactivity & turn-off notifications

Meet consumers' expectations of how well hardware and software should work together (i.e. performance requirements)

USE CASE #11 – User Authentication

USE CASE DESCRIPTION

This use case covers the minimum requirements a device must comport to in order to authorize transmission of content to an approved device.

In order for a device to receive specified content, the User and Device must abide by the following:

- Per the Precondition, the User has a subscription to a content service.
- The content service subscription authorizes connection to the content being accessed (e.g. conditional access).
- The device must abide by the rules invoked by the content usage and security settings. Examples include:
    - Permissions
        - Subscription will conform to region settings (neighborhoods, blackouts) and service settings (entitlements).
        - Device Authorization Access
        - Content or application enforces applicable usage restrictions
        - Rights Management
    - Devices are required to track current version of DRM and security updates.
        - Currently these updates are managed by the device and/or service provider network.

In the event the conditional access permissions do not align, then the User should see a notification message about this incompatibility and content will not be sent to the device.

USE CASE #12 – Renewability (DELETED DURING DELIBERATIONS)

USE CASE #13 - Cloud VOD Delivery

Pre-Condition: Subscriber has access to the same or similar VOD content that is available through the primary Home Gateway or STB that the MVPD provides to the home subscriber.

USE CASE DESCRIPTION

This Use Case reviews the elements related to delivering content from a remote access, or cloud source to a supported device. This is described in WG2 Report Part VI [45].

To support this use case a device should provide one or more of the following:

1. An App platform that provides support for multiple App developers including video distributors, examples include: iOS, Android, Android TV, Tizen, WebOS, Yahoo Widgets, Xbox, and PlayStation. The robustness of the App platform may affect what content is available to devices that are supported by the the App platform.
2. An HTML5 based platform that supports Media Source Extensions (MSE) [57] and Encrypted Media Extensions (EME) [58] with one or more Content Decryption Modules (CDM). As with the App platform, the robustness of the implementation may affect what content is available to devices that support HTML5 MSE/EME.
3. A DLNA VidiPath compliant client that can connect to an MVPD VidiPath server.

SERVICE DESCRIPTION

A Cloud VOD library typically also includes expanded VOD, such as look back content or episodic content from previous weeks of a programmatic series. There may be different servers handling the home VOD compared to the Cloud VOD media assets, thus not all content in the Cloud is offered at home and vice versa.

Most implementations of Cloud VOD from MVPDs are growing to be a superset of the home use case for VOD. Divisions of titles tend to be categorized in areas such as:

- Free
- Genre-based
- Network specific
- Premium Subscription
- Event-driven titles.

As Pay TV operators deploy HTML5 based UI's, the MVPD subscriber can leverage a consistent UI across the TV, mobile device, or PC. Content is typically accessed over the Internet using a Browser or Web application. Platform dependent applications for iOS or Android are also being developed to provide this TV Everywhere experience.

See also USE CASE #2 - Viewing On-Demand Content for IP VOD, which is already cloud based.

USE CASE #14 - Cloud Live Streaming

Pre-Condition: Subscriber has access to the same Live or Linear broadcast TV content that is available to the primary Home Gateway or STB that the MVPD provides to the home subscriber.

USE CASE DESCRIPTION

This Use Case reviews the elements related to streaming the delivered content from a remote access, or cloud source to a supported device.

To support this use case a device should provide one or more of the following:

1. An App platform that provides support for multiple App developers including video distributors, examples include: iOS, Android, Android TV, Tizen, WebOS, Yahoo Widgets, Xbox, and PlayStation. The robustness of the App platform may affect what content is available to devices that are supported by the the App platform.
2. An HTML5 based platform that supports Media Source Extensions (MSE) [57] and Encrypted Media Extensions (EME) [58] with one or more Content Decryption Modules (CDM). As with the App platform, the robustness of the implementation may affect what content is available to devices that support HTML5 MSE/EME.
3. A DLNA VidiPath compliant client that can connect to an MVPD VidiPath server.

Examples include:

- In the cases when a unidirectional DBS receiver is operating with access to the internet, cloud VOD content available from the DBS MVPD is integrated into features such as navigation and search on the DBS receivers to expand the scale and scope of the service offered to a DBS customer. Both DBS MVPDs offer limited cloud-based live streaming content as alternative OTT services using alternative navigation devices. In contrast to cloud VOD, this streaming content generally duplicates what is offered through the DBS broadcast and is not also received by DBS receivers.

SERVICE DESCRIPTION

Live or linear content is delivered at the time that the originally schedule content is delivered to the subscriber's home video gateway or STB. Access to these TV video streams tends to be sought from mobile devices for the purpose of providing a TV Everywhere experience.

MVPDs offer applications that directly stream content from the Cloud using broadband access for home devices such as gaming consoles, Smart TVs, and Tablets. The home user can avoid having to connect to a STB with a wired HDMI cable. As MVPDs move to upgrade their network to a full IP distribution architecture, these directly attached networked devices can receive a complete lineup of linear and live TV content directly, without having to be tethered to a Gateway or STB.

USE CASE #15 – Cloud DVR Recording and Streaming

Pre-Condition: Subscriber has access to recorded content that is available from a Remote Storage DVR service offered by the Pay TV provider, or access to a copy of the DVR content located on a home DVR or Gateway device that is remotely stored in the Cloud.

USE CASE DESCRIPTION

This Use Case reviews the elements related to recording the delivered (via streaming) content from a remote access, or cloud, source to a supported device.

To support this use case a device should provide one or more of the following:

1. An App platform that provides support for multiple App developers including video distributors, examples include: iOS, Android, Android TV, Tizen, WebOS, Yahoo Widgets, Xbox, and PlayStation. The robustness of the App platform may affect what content is available to devices that are supported by the the App platform.
2. An HTML5 based platform that supports Media Source Extensions (MSE) [57] and Encrypted Media Extensions (EME) [58] with one or more Content Decryption Modules (CDM). As with the App platform, the robustness of the implementation may affect what content is available to devices that support HTML5 MSE/EME.
3. A DLNA VidiPath compliant client that can connect to an MVPD VidiPath server.

SERVICE DESCRIPTION

Live or Linear broadcast TV content can typically be recorded simultaneously on both a local DVR and on a remote server for access by a mobile device outside of the home. Control of the scheduling for recordings can be done though a Web browser application running on a networked enabled device with Internet access or using a Pay TV developed application, such as those downloaded for Android or iOS devices. Remote control of the home DVR or remote control of the Cloud DVR is available through these device MVPD applications. APIs may be provided by the MVPD for a retail device to use a third party guide to control DVR content recording.

USE CASE #16 - Cloud Content Downloading for Mobile Devices

Pre-Condition: Use Case #15 has been met

USE CASE DESCRIPTION

This Use Case reviews the elements related to managing download content that has been delivered from a remote access, or cloud, source to a supported device.

To support this use case a device must:

- Be an authorized device
- Maintain (i.e. no deliberately remove) content protection technologies that are inherent to the downloaded content, such as Digital Rights Management or watermarks).
- If the downloaded content is marked with an expiration date, then the device must make every reasonable effort to forbid playback of content once the expiration date has been reached.
- If the authorized device has a domain restriction imposed upon it, then the device must abide by that requirement.
    - Such a requirement is used to ensure that the device is tied to the subscriber's home network; protecting entitlements.
- Provide one or more of the following:

    1. An App platform that provides support for multiple App developers including video distributors, examples include: iOS, Android, Android TV, Tizen, WebOS, Yahoo Widgets,

Xbox, and PlayStation. The robustness of the App platform may affect what content is available to devices that are supported by the the App platform.

2. An HTML5 based platform that supports Media Source Extensions (MSE) [57] and Encrypted Media Extensions (EME) [58] with one or more Content Decryption Modules (CDM). As with the App platform, the robustness of the implementation may affect what content is available to devices that support HTML5 MSE/EME.
3. A DLNA VidiPath compliant client that can connect to an MVPD VidiPath server.

The availability of download varies among content subscription services; rights are often content or programmer specific. Typically, the expiration date indicates how long the downloaded program is available for playback.

Examples include:

In the case of a DBS service to a customer with no cloud access, it may be possible for the in-home DBS system to act as a proxy for internet cloud-based content. This capability does not currently exist in any fielded DBS STBs.

SERVICE DESCRIPTION

When available, a User has the ability to copy or move content from the Cloud for temporary storage and manage content playback on a mobile device. Examples of this content may be VOD content or copies of Live/Linear content stored in a Cloud DVR service. One reason that content is available for download is to allow for offline viewing of subscription content. A device is considered “offline” when it does not connect to a broadband network, wireless LTE service area or Wi-Fi access point.

Each service varies in how the downloaded content is managed. Examples of management methods are:

- Some require the device connect to a network after a certain number of days, in order to renew rights and confirm expiration dates, other services do not require such check ins.
- When required, such as through rights limitations, one title is allowed to be checked out or downloaded at a time per subscriber.

Part II: Systems that Enable Competitive Availability of Devices

Identify systems comprising minimum standards, protocols, and information other than security elements to enable competitive availability of devices that receive MVPD services.

Section I: SAT-IP

Description

SAT-IP is a remote tuner control protocol that provides a standardized way for IP clients to access live media broadcasts from satellite reception servers on IP networks. It separates distribution-specific elements such as tuners, dish LNBs, etc into a single device that then provides video services to over IP to client devices on the home network using common protocols. The client devices and protocols are agnostic to the physical layer differences between satellite service providers. Satellite services can be forwarded over all types of IP wired or wireless technologies to a range of IP client devices.

The protocol envisions a number of different possibilities for the server where it could be built-in to different devices such as consumer or commercial versions of LNBs, IP Multiswitches, or set-top boxes.

Protocols

The SAT-IP home network protocols are based on IP, RSTP, UPnP and HTTP. It was made to be integrated into DLNA as an option.

SAT>IP servers identify themselves on the IP network using standard UPnP mechanisms (SSDP). Stream Control in SAT>IP is done via RTSP or HTTP. SAT>IP clients request access to satellites, transponders and MPEG PID streams as needed. RTSP queries are used for requesting RTP unicast or multicast streams. HTTP queries are used for requesting HTTP streams.

In summary, the client can provide low level tuning functions with the reception servers using this protocol to translate to whatever specific technologies are used by the service provider.

Security

The solution current assumes either “Free-to-Air” unscrambled or a pass-through scenario that assumes that any CA or DRM descrambling will be done by the client. Because the protocols can be used under DLNA, DTCP-IP encryption could be applied to scrambled services. As a specification for use in Europe, there is an assumption that DVB Common Interface + (CI+) would be used.

Information

The following links provide useful information:

http://www.satip.info/

http://en.wikipedia.org/wiki/Sat-IP

Section II: CableCARD

Description

The CableLabs CableCARD specification defines a two-way interface that is licensed to decrypt and view one-way linear digital cable television in the United States. CableCARD only functions on Hybrid Fiber-Coax (HFC) based networks and does not function on DBS or IPTV systems. CableCARD uses a physical PCMCIA PC Card type II form factor device for all conditional access and provides copy protection of content across the PCMCIA interface. A CableCARD is able to decrypt up to six simultaneous programs from a service provider. A CableCARD set top box is comprised of the set top box, purchased at retail or rented from operator, as well as the CableCARD itself which must be provided by an operator, generally for a monthly fee.

At the core a set top box obtains a channel lineup from the CableCARD and then may request entitlement to decrypt and display a particular program in the lineup. The CableCARD emits Copyright Control Information (CCI) which the set top box Host is required to abide by, in cases such as recording. Premium content requires a one-to-one pairing of CableCARD to Host to protect against unauthorized viewing. Host binding requires an end user to contact their service provider with unique information from both the Host device and the CableCARD, thus ensuring that all Hosts are licensed and certified devices.

CableCARDS provide a few other mechanisms besides merely decrypting signals. The CableCARD terminates and decodes the forward out-of-band channel which carries service information data such as channel lineups (virtual channel map and source names), EMMs, software downloads, EAS messages, and other control data, and proprietary service data. SCTE 65 defines six profiles for Service Information tables for delivery via an out-of-band channel on cable, but if UDCPs wish to use guide data, then based on the 2002 MOU and FCC Rule 15.123(b) retail UDCPs must obtain guide data through third-parties other than the cable system.

The CableCARD provides an application information interface, which can be used to obtain information about the CableCARD itself, including Host binding status, card manufacturer, card modes, packets/tables received, et cetera. CableCARDs also provide a Man Machine Interface (MMI) that provides a way to present messages on the display using HTML pages with URL's that are passed back to the CableCARD to request further data from the MMI. The CableCARD specification defines a baseline HTML profile that constrains the functionality required of the Host for the MMI. The Baseline HTML Profile only supports formatted text messages, in the form of HTML pages, with one hyperlink. In practice the MMI is only used for the Card/Host binding and diagnostic purposes.

Originally, CableCARD devices were either an integrated digital television with a CableCARD slot or a set top box with video outputs only. A subsequent OpenCable Unidirectional Receiver (OCUR) specification was developed to enable an interface to Microsoft Windows Media Center PCs. CableLabs eventually offered additional secure IP output options and current CableCARD devices utilize them to distribute video throughout the house. The OCUR Digital Receiver Interface is discussed in another section of this

document. The CableCARD ecosystem provides set top box implementors the ability to add features consistent with the DFAST license, such as enforcement of content protection.

Standards

Standards in use by CableCARD include:

- SCTE 28 – Host POD interface describes low level CableCARD interaction, like the Man Machine Interface (MMI), entitlement requests, application information, and other conditional access related operations.
- SCTE 41 – Copy protection standards, includes key and certificate exchanges, device authorization, content protection, Host binding, and algorithms in use.
- SCTE 65 – service information delivered out of band. Profiles 1-3 include virtual channel maps, source names, and parental control. Profiles 4-6 are event information tables relating to guide data.
- EIA-608/EIA-708/SCTE 21 – Embedded user data, such as CGMS-A content rights descriptor and captions.
- Joint Test Suite.

Information

http://www.cablelabs.com

http://en.wikipedia.org/wiki/CableCARD

OpenCable CableCARD Interface 2.0 Specification, OC-SP-CCIF2.0, http://www.cablelabs.com/wp-content/uploads/specdocs/OC-SP-CCIF2.0-I27-150330.pdf, Cable Television Laboratories, Inc.

OpenCable CableCARD Copy Protection 2.0 Specification, OC-SP-CCCP2.0, http://www.cablelabs.com/wp-content/uploads/specdocs/OC-SP-CCCP2.0-I13-130418.pdf, Cable Television Laboratories, Inc.

OpenCable Security Specification, OC-SP-SEC, http://www.cablelabs.com/wp-content/uploads/specdocs/OC-SP-SEC-I08-110512.pdf, Cable Television Laboratories, Inc.

Uni-Directional Cable Product Supporting M-Card: Multiple Profiles, Conformance Checklist: PICS, M-UDCP-PICS-I04-080225, http://www.cablelabs.com/wp-content/uploads/specdocs/DVC-RQ-M-UDCP-PICS-I04-080225.pdf, Cable Television Laboratories, Inc.

Applicable Devices

- Most MVPD supplied cable boxes, excluding DTA's. (Requirement expires December 4, 2015).
- TiVO's
- Hauppauge/SiliconDust/Ceton network CableCARD tuners (OCURs)
- Ceton internal CableCARD PCI card

Section III: DRI and OpenCable interfaces (and specifications)

Description

An OpenCable Unidirectional Receiver (OCUR) is designed to be interoperable across all CableCARD cable systems in the United States. The OCUR does not interoperate with DBS or IPTV MVPD systems. The OCUR is designed specifically to work with a Windows-based PC with PlayReady DRM. The PC may separately support OTT interactive applications, real time services, and other on demand services. OCUR devices are unidirectional CableCARD devices, but an OCUR is defined as having IP outputs only with DRM protection; physical video outputs are not allowed in this device model. The OCUR may optionally have a USB interface host interface for connection of a Tuning Resolver. OCUR IP outputs are specified by the Digital Receiver Interface (DRI). Various approved DRM systems are permitted to protect premium content across the network; Microsoft PlayReady is the only currently approved full DRM for the OCUR, while DTCP-IP is approved for link level security.

All client-server interaction leverages open standards and protocols, and adds additional DRI-specified requirements, including a unique content protection layer ("DRI Security") that must be supported in all DRMs. Signal source and other CableCARD details are mostly hidden from the receiving client, who only receives protected content streams and various ancillary information externally.

Protocols

OCUR devices advertise themselves on the network using UPNP SSDP announcements. OCUR devices offer two interfaces to obtain content using UPnP and DLNA protocols. An OCUR device supports the DRI Tuner UPnP protocol, and optionally the DLNA Digital Media Server (DMS) function.

A Tuner object is available for each physical tuner the OCUR has. This DRI Tuner exports a variety of operations and queries which closely resembles interacting with a physical tuner, this inferface allows direct manipulation in cases of clear QAM. The interface also offers high level operations a user might expect such as tuning to a linear digital cable channel. All data through this interface is transmitted via UDP unicast streams using RTP.

An OCUR might also export a DLNA digital media server (DMS) content directory service (CDS). This CDS allows for HTTP requests of streams and completely abstracts all details away from the tuner. The CDS approach allows clients without an approved DRM access only to programs with Copy Control Information (CCI) identifying them as Copy Freely, expanding the number of supported clients that can access Copy Freely content to any device that supports DLNA.

Security

OCUR devices use IP for all outputs. OCUR devices can use either PlayReady or DTCP-IP for RTP transmissions when using the DRI Tuner UPnP object model. OCUR devices encrypt all content that is not Copy Freely, so the client is responsible for decrypting secure content. Programs accessed over DLNA, which are not marked Copy Freely, can be secured using DTCP-IP or PlayReady. Any device which

is licensed to use Windows/PlayReady or is DLNA/DTCP compliant can interact and get content from an OCUR device.

Devices that receive content from an OCUR device using Microsoft PlayReady must also conform to OCUR license requirements managed by Microsoft for population of an Association Database of paired CableCARD-OCURs, QoS, carriage of System Renewability Messages (SRM), Breach Management, Revocation and Renewability, and indemnity. These supplement the license requirements for the OCUR device itself.

Information

http://www.opencable.com

http://en.wikipedia.org/wiki/OpenCable

OpenCable CableCARD Interface 2.0 Specification, OC-SP-CCIF2.0, http://www.cablelabs.com/wp-content/uploads/specdocs/OC-SP-CCIF2.0-I27-150330.pdf, Cable Television Laboratories, Inc.

OpenCable CableCARD Copy Protection 2.0 Specification, OC-SP-CCCP2.0, http://www.cablelabs.com/wp-content/uploads/specdocs/OC-SP-CCCP2.0-I13-130418.pdf, Cable Television Laboratories, Inc.

OpenCable Unidirectional Receiver, OC-SP-OCCUR, http://www.cablelabs.com/wp-content/uploads/specdocs/OC-SP-OCUR-I11-130607.pdf, , Cable Television Laboratories, Inc.

OpenCable Digital Receiver Interface Protocol, OC-SP-DRI, http://www.cablelabs.com/wp-content/uploads/specdocs/OC-SP-DRI-I04-100910.pdf, Cable Television Laboratories, Inc.

OpenCable Security Specification, OC-SP-SEC, http://www.cablelabs.com/wp-content/uploads/specdocs/OC-SP-SEC-I08-110512.pdf, Cable Television Laboratories, Inc.

Applicable Devices

- Hauppauge WinTV network CableCARD tuners
- SiliconDust HDHomeRun network CableCARD tuners
- Ceton Windows Media Center Extenders

Section IV: Android/iOS Store Device Architectures from DEVELOPER Point of View

Collectively, the app model is the means for bridging the differences between varied and rapidly changing services and varied and rapidly changing consumer electronics platforms. These application approaches abstract the diversity and complexity of service providers' access network technologies and customer-owned IP devices and accommodate rapid change and innovation by both service providers and consumer electronics manufacturers. These application approaches may also make use of a combination of software-downloadable security and a hardware root of trust. This diversity and flexibility enables the broadest coverage of retail devices, optimizes the consumer experience on the

latest devices and technologies, and takes advantage of a wide range of market-tested security measures including downloadable DRMs.

Table 8 shows how the major MVPDs currently support retail devices using this three-pronged approach. All of the major MVPDs support an iOS and Android App to access their service on smart phones and tablets. All of the major MVPDs support their service on Microsoft Windows and Apple Mac OS X either through an application or a Web app (using a plug-in model for content protection today and transitioning to an HTML5 EME Web App in the future). Some of the major MVPDs support Smart TVs (LG, Samsung, Sony, Toshiba), game consoles (PlayStation 3 & 4, Xbox 360 & One), and media adaptors (Roku). VidiPath Certification was launched in September 2014. Many of the major MVPDs either support DLNA VidiPath today or plan to in the near future. DLNA RVU, developed and maintained by the RVU Alliance, is supported by DirecTV. Certified VidiPath client devices are expected in the market later in 2015. Table 8 lists some of the currently supported devices, which continue to grow.

Standards

By definition native apps are written specifically for a particular platform, e.g. iOS, Android, Tizen, Xbox, Playstation, etc. While these platforms and devices make use of many different standards, summarized below, the specific user interfaces, device features and platform APIs enable differentiation and competition among them. This competitive marketplace for devices and platforms has resulted in an explosion of smart phones, tablets and more recently smart watches, with a large array of features and capabilities. Smart TVs are also offering application platforms that enable access to new service offerings, including applications such as Netflix, YouTube, and Amazon Prime Video, as well as some MVPD apps.

In general, these platforms offer some form of app marketplace (e.g. Apple's App Store or Google's Google Play App Store), where MVPD app developers can offer their apps and consumers can download them to their devices.

In order to support their App marketplace these platforms have developed various security capabilities to insure that the content and applications are protected appropriately.

MVPDs have focused their app development efforts thus far on those devices and platforms that enjoy the greatest consumer use and marketplace success. Table 8 ranks particular devices/platforms by the number of units sold in the United States. As can be seen by this table, MVPDs broadly support device/platform specific apps on the most popular devices/platforms. MVPDs are also devising other ways to expand the range of devices and platforms that can support MVPD apps, such as via an HTML5 web browser, VidiPath, or RVU. Some observations that can be drawn from these and other marketplace facts:

- The total number of retail devices in the US that can be served by an MVPD app is over: **450 million devices**
- The percentage of these retail devices that can be served by one or more MVPD apps is: **96%**
- The percentage of these retail devices that can be served by an app from all of the top 10 MVPDs is: **67%**
- The average number of MVPD set-tops per subscriber is **2.4**
- The average number of these retail devices per US household is **4,** well exceeding the **2.4** MVPD set-tops per subscriber

Other devices can be supported by either an HTML5 web browser, VidiPath, or RVU.

Retail Device	United States Units	MVPD Apps
Android phones[5]	92,036,000	All top 10 MVPDs[6]
PCs & Macs w/Broadband[7]	85,358,000	All top 10 MVPDs
iOS phones[5]	71,449,000	All top 10 MVPDs
Xbox 360[8]	48,460,000	5 of the top 10 MVPDs
Android Tablets[9]	43,260,000	All top ten MVPDs
PlayStation 3[8]	29,160,000	2 of the top 10 MVPDs
iOS Tablets[9]	23,730,000	All top 10 MVPDs
Samsung TV[10]	14,740,800	4 of the top 10 MVPDs
Vizio TV[10]	12,151,200	0
Apple TV[11]	8,800,000	N/A
Sony TV[10]	8,764,800	1 of the top 10 MVPDs
PlayStation 4[8]	8,650,000	2 of the top 10 MVPDs
Xbox One[8]	7,790,000	2 of the top 10 MVPDs
LG TV[10]	6,500,000	2 of the top 10 MVPDs
Roku[11]	5,000,000	1 of the top 10 MVPDs
Chromecast[11]	4,000,000	1 of the top 10 MVPDs
Total Number of Retail Devices	469,849,800	

Table 8- US Retail Device Numbers

Protocols

Some of the common standards that these platforms support include:

- IETF Internet Protocol Standards
- IEEE 802.11xx Standards

[5] comScore Reports January 2015 U.S. Smartphone Subscriber Market Share, March 4, 2015 - http://www.comscore.com/Insights/Market-Rankings/comScore-Reports-January-2015-US-Smartphone-Subscriber-Market-Share

[6] Top 10 MVPDs – AT&T, Bright House, Cablevision, Charter, Comcast, Cox, DirecTV, DISH, Time Warner Cable, Verizon

[7] Computer and Internet Use in the United States: 2013 *American Community Survey Reports,* U.S. Department of Commerce Economics and Statistics Administration U.S. CENSUS BUREAU, November 2014 - http://www.census.gov/history/pdf/2013computeruse.pdf

[8] Platform Totals, VGChartz Limited, http://www.vgchartz.com/analysis/platform_totals/ (accessed: 6/18/15)

[9] THE STATE OF THE TABLET MARKET - http://tabtimes.com/resources/the-state-of-the-tablet-market/ (accessed: 6/18/15)

[10] Majority of US Internet Users to Use a Connected TV by 2015, eMarketer, June 13, 2014 - http://www.emarketer.com/Article/Majority-of-US-Internet-Users-Use-Connected-TV-by-2015/1010908 and Samsung, Vizio Control US smart TV market, Broadband TV News, MARCH 10, 2014 - http://www.broadbandtvnews.com/2014/03/10/samsung-vizio-control-us-smart-tv-market/

[11] Streaming devices sales in the United States in 2014 (in million units), Statista Inc. - http://www.statista.com/statistics/296641/streaming-devices-sales-united-states/ (accessed: 6/18/15)

- 3GPP LTE Standards
- UPnP and DLNA Guidelines [60]
- W3C Standards
- MPEG video and audio standards

Information

MVPDs and OTT providers have developed apps for the following devices and platforms, among others:

- Apple iOS
- Google Android
- Samsung Smart TV and Tizen
- LG WebOS
- Microsoft Xbox
- Sony PlayStation
- Roku
- Slingbox Client

The following sections discuss these platforms.

Apple iOS

Apple supports an app ecosystem for its mobile devices, smart phones, tablets, and smart watches based on its iOS platform.

Apple has an extensive developer program for Apple devices that is accessible under license (https://developer.apple.com/programs/). Apps can be submitted to the Apple iTunes Store for distribution to iOS devices.

The iTunes Store, originally the iTunes Music Store, is a software-based online digital media store operated by Apple Inc. It opened on April 28, 2003, and has been the largest music vendor in the United States since April 2008, and the largest music vendor in the world since February 2010.

iOS (originally iPhone OS) is a mobile operating system created and developed by Apple Inc. and distributed exclusively for Apple hardware. It is the operating system that presently powers many of the company's mobile devices, including the iPhone, iPad, and iPod touch.

iOS was originally unveiled in 2007 for the iPhone and has been extended to support other Apple devices such as the iPod touch (September 2007), iPad (January 2010), iPad mini (November 2012) and second-generation Apple TV onward (September 2010).

The iTunes Store is accessible using a web browser, or using native applications on an iOS device. In order to complete a purchase, one is required to register an account with Apple. This is a secure process that every iOS customer needs to perform in order to be able to browse, download, install, and use any of applications published through the iTunes Store. In order to create an Apple ID, one would need to

access the App Store and follow the steps that include entering contact information, email address, and billing information.

Once a user account is created, the customer can browse all available applications, video, and music, and make purchases. Applications are instantly available on the device.

The iOS platform allows applications to use HDMI and Airplay outputs to stream video and audio. Content licenses may have different rules on allowing streaming over HDMI and/or Airplay. Given these requirements, MVPDs are left to decide on allowing or denying access to high definition devices over HDMI and/or Airplay. Requirements to manage HDMI and/or Airplay connections may be enforced by the chosen DRM system.

The iOS platform provides the means of utilizing the underlying hardware security. All iOS devices have a dedicated AES-256 crypto engine built into the DMA path between the flash storage and main system memory, making file decryption very efficient. Application developers are free to use this mechanism or implement their own. A summary of iOS provided hardware security is available at: https://www.apple.com/business/docs/iOS_Security_Guide.pdf

Google Android

Google supports an App ecosystem for mobile devices, smart phones, tablets, and smart watches with its Android platform. Google supports an App ecosystem for smart TVs with its Android TV platform. Google also has an extensive developer program for Android Apps that is available under license to Google (http://developer.android.com/index.html).

Google Play is the app store for the Google Android App ecosystem. Android is the operating system created and developed by Google and, unlike Apple's iOS, is available via open source for any device manufacturer who chooses to licenseit. It is the operating system that powers many smart phones, tablets, and media players. Use of the Android OS does not mandate distribution of Android Apps through the Google Play Store. For example, Amazon has its own Amazon Fire Apps store for Android apps that run on Amazon tablets and Fire TV media players.

The Google Play Store and Amazon Fire App Store are both accessible using a web browser, or using native applications on an Android or Amazon device. In order to complete a purchase, one is required to register an account with Google Play or Amazon.

Once a user account is created, the customer can browse all available applications, video, and music, and make purchases. Applications are downloaded and made available on the device.

There are two integrated application development environments (IDEs) available for Android; Eclipse and Android Studio with Java as the development language.

Google also provides a set of developer guidelines to assist in the development of Android apps, as well as a set of design guidelines that help developers to make apps that not only work well but also look good.

The Android platform provides a secure boot process, as well as providing for signed application code, although sometimes this can be device manufacturer dependent. Android provides application sandbox support. However, Android does not provide a native secure media player, so an app developer must implement a secure media player to meet its content license and regulatory requirements. Miracast and/or HDCP protected output is often provided, but depends on the device manufacturer.

The Android App ecosystem is not as stringently managed as the Apple iOS app ecosystem. Android apps are not strictly approved by Google and are self-signed only. Apps can be delivered from the Google Play Store over Google protocols, or the Amazon Fire Store, or they can be side-loaded directly onto the device.

The Android platform does not provide access to unique keys or certificated identities through Android. However, access to the device MAC address is permitted.

Samsung Smart TV & Tizen

Samsung supports an App ecosystem for its smart TVs either with its Smart TV platform or more recently its Tizen platform initially released in March of 2015 (http://www.samsungdforum.com/). During 2015, Samsung Smart TV will fully migrate to the Tizen based ecosystem. The new Tizen platform will provide for Samsung Smart TV App developers a better performing and easier app development environment.The Smart TV platform supports Web applications, while Tizen supports Web applications, native applications and hybrid applications, but Samsung Tizen TV only provides a Web application environment for developers. App developers in Tizen develop applications based on Web technology (HTML5, CSS3, JavaScript). Tizen also supports Samsung's mobile devices, tablets, smart phones, and smart watches.

Samsung Smart TV is a web-based application that runs on an application engine installed on Samsung's digital TVs that are connected to the Internet. Smart TV applications are special web pages implemented in a web browser and displayed on a TV screen. Users can download *Smart TV Applications* from Samsung Apps and install them on their TVs, or even develop their own applications.

Consumers can view an application on the TV screen similar to how they view web pages in a web browser on a computer. However, the experience is adjusted to screen resolution, hardware specifications, using the TV remote control for user interaction, and typically only executing one application at a time.

The Smart TV platform supports HTML5, DOM3, CSS3, JSC, and a variety of DRMs including: PlayReady, Widevine, Secure Media and Verimatrix. For transport the Smart TV platform supports DASH [40], HLS [38], Smooth Streaming, as well as Live Streaming. The Smart TV Platform is based on two engines: Gecko, for platforms from years 2011 and 2010 and WebKit [74] for more recent years. It supports three resolutions:

- 960 x 540 pixels
- 1280 x 720 pixels

- 1920 x 1080 pixels

The Tizen platform supports HTML5, DOM3, CSS3, JSC, and a variety of DRMs including: PlayReady, Widevine, Verimatrix, SecureMedia, SDRM, and SCSA. For transport the Smart TV platform supports DASH, HLS, Smooth Streaming. Applications are signed with the developer certificate.

In order to distribute applications on Samsung TVs and make them available through the Samsung Smart Hub Apps TV store, it is necessary to register the application and it must go through a certification process provided by Samsung or its Affiliate at the Application Seller Office before being launched on the Samsung Apps TV store. To request certification, it is necessary to prepare the Tizen widget package and metadata and submit it in the Samsung Apps TV Seller Office. To aid development Samsung provides both a development guide and a UX guide.

LG WebOS

LG supports an app ecosystem for its smart TVs with its WebOS platform. Applications are packaged in IPK format and registered in the LG SmartWorld Seller Lounge. The LG application quality assurance team evaluates the performance, function, and UIs of submitted apps to verify the suitability for publishing on LG Content Store (LG STORE). Valid apps are published on LG Content Store (LG STORE).

Every app submitted to LG Smart World will go through a Quality Assurance (QA) process before sale is permitted. Those Apps that do not meet the QA criteria can be rejected for sale.

The QA criteria applies to every app submitted but certain Apps such as game, video, education, etc, can be subjected to additional criteria by category.

Apps that cause TV errors, illegally collect user information, contains malignant codes, and/or contains viruses will be removed from the store, and the Seller can be held responsible.

Microsoft Xbox

Microsoft supports an app ecosystem for its Xbox game consoles, both Xbox 360 and Xbox One.

Roku

Roku supports an app ecosystem for its streaming video players, including its Roku 1, 2, 3, and Roku Streaming Sticks. There is no fee for joining the Roku Developer Program or for publishing a Roku app. Roku Channels are written in a Roku-specific language called BrightScript. BrightScript is a scripting language similar to VisualBasic and is quickly learned by experienced programmers. Communication with services and servers is done over HTTP using standard XML-based technologies like (M)RSS, RESTful APIs and JSON. For video, Roku recommends H.264 video with AAC-LC audio wrapped in a MP4 container. Roku also supports the VC-1 video codec, and the WMA and MP3 audio codecs. Roku supports the HTTP Live Streaming protocol (HLS) [38], which is quickly becoming the standard across home entertainment and mobile devices. This technology provides adaptive streaming of either live or on-demand content. Roku supports PlayReady for Smooth Streaming and AES-128 bit encryption for HLS. Roku reviews and approves all apps prior to publishing them to the Roku Channel Store to ensure

that they are of high quality and function properly. Roku attempts to make this process as streamlined as possible. The specific restrictions and terms for publishing content to the Roku Channel Store are found in the Roku Developer Agreement. In a presentation to Working Group 4, Time Warner Cable commented that the Roku developer support team was skeptical about developing a grid based EPG app on Roku devices that would have acceptable performance. Based on Time Warner Cable's extensive experience in developing grid based EPG applications, they were able to provide an EPG app on Roku devices that performed very well. This Roku app was demonstrated at the June 2, 2015 Working Group 4 meeting. {Link to video}

Applicable Devices

As outlined above Apps can be developed for almost every class of retail device, including:

- Smart or connected TVs
- Game Consoles
- Retail set-top boxes or HDMI sticks
- Personal computers (both Windows and Mac)
- Tablets
- Smart phones

Section V: VidiPath

The Digital Living Network Alliance (DLNA) is a technology standards organization with participants from consumer electronics manufacturers, software developers, content providers, and MVPDs that builds industry consensus to advance the interoperability of video products in consumers' connected homes. DLNA was founded in 2003 and currently has a membership of more than 200 companies. DLNA's multi-industry collaboration implements a set of guidelines utilized by service providers, electronics manufacturers, and software developers to provide consistent performance in a connected home environment.

"VidiPath" enables MVPDs to deliver their service to retail devices by using an HTML5 app with extensions developed in the W3C standards body. VidiPath was developed in DLNA by major retail device manufacturers (including Samsung, Panasonic and Sony); major chip manufacturers (Intel and Broadcom) and major MVPDs (including Comcast, TWC, AT&T and DISH). The retail device can operate as a retail "mall" in which many different video providers can operate as retail stores presenting their own brands and experiences. The subscriber clicks on the app and receives the full service offered by the MVPD. VidiPath Certified devices, include mobile devices, PCs, set top boxes, AV receivers, game consoles, TVs. DLNA has also created a robust certification program which tests and verifies the interoperability of products built to its standards, ensuring consumers that devices branded with the DLNA Certified and VidiPath Certified marks will successfully connect and exchange content. VidiPath service operator services can be forwarded to all types of devices attached to the home network over wired or wireless technologies.

With DLNA VidiPath certification and a “C2” flag in the DTCP certificate for LAN services or commonName field with value "DTLA CVP-2 SP CA" in the X.509 certificate for cloud services, service providers are guaranteed pixel accurate rendition of their user interface on devices and with a good level of quality of service. VidiPath does not allow a competitive navigation device to employ its own user interface to access MVPD content. There is no standard protocol for discovering the list of premium channels, tuning to them, or recordings outside of the MVPD’s remote user interface. The MVPD’s user interface is the only method for accessing content.

DLNA VidiPath enables both a home server model, or as MVPDs move more to the cloud, a cloud to ground model. VidiPath does not facilitate retail device manufacturers the ability to access to video content directly outside of the RUI.

This section presents an overview of the VidiPath specifications that include features such as HTML5 Remote User Interface (RUI), Authentication, Diagnostics, Low Power, MPEG-DASH, and DTCP-IP [60]. Benefits offered by VidiPath to consumers, OEM manufacturers and service providers are also discussed. To support market adoption and implementation of VidiPath, CableLabs has developed an open source implementation of VidiPath Server and Client reference devices [56]. The main objectives for the VidiPath open source implementation efforts are: provide reference devices to DLNA to help launch VidiPath certification program; provide reference devices to the industry for testing and development of VidiPath products; and foster VidiPath adoption and speed time to market. The Server and Client reference devices serve as reference platforms for retail device manufacturers and MVPDs and other MVPDs to test their VidiPath implementations.

Summary

To enable secure distribution of premium content from an in-home video gateway to retail devices, major MVPDs in the U.S., CableLabs, retail device manufacturers and other service providers all over the world, led an effort to define VidiPath specifications within Digital Living Network Alliance (DLNA) [59].

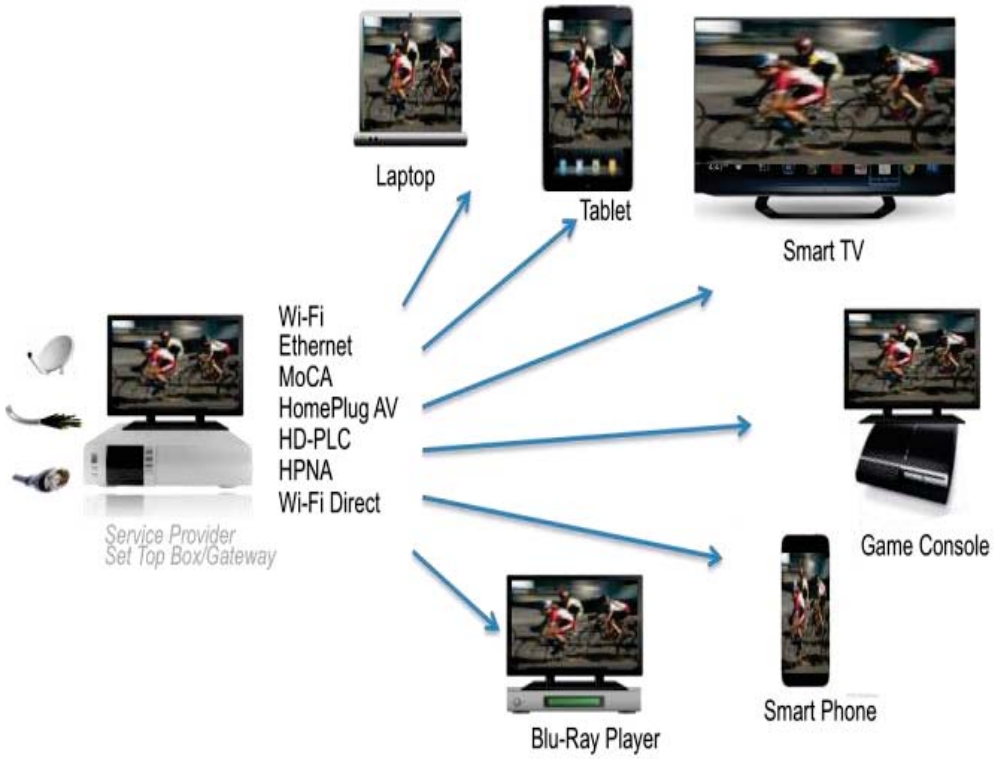


Figure 19 - DLNA VidiPath Overview

Using VidiPath specifications, MVPDs can stream various content from a video gateway to retail devices, such as TVs, game consoles, tablets, mobile phones, and laptops, with a consistent MVPD user interface across different devices without the need of a dedicated MVPD supplied STB per device.

The DLNA VidiPath Specifications define the following set of features for VidiPath Server and Client [60]:

- HTML5 Remote User Interface (RUI)
- MPEG-2 and AVC media formats
- DTCP-IP Link Protection
- Diagnostics
- Low Power
- Authentication
- 3D Media formats; conditionally mandatory
- HTTP Adaptive Delivery; mandatory for Client, optional for Server

- Priority-based QoS
- Digital Media Server (DMS); mandatory for Server only
    - No Content Directory Store (CDS) for linear content, VoD, or PPV is provided
- Digital Media Player & Digital Media Renderer; mandatory for Client only

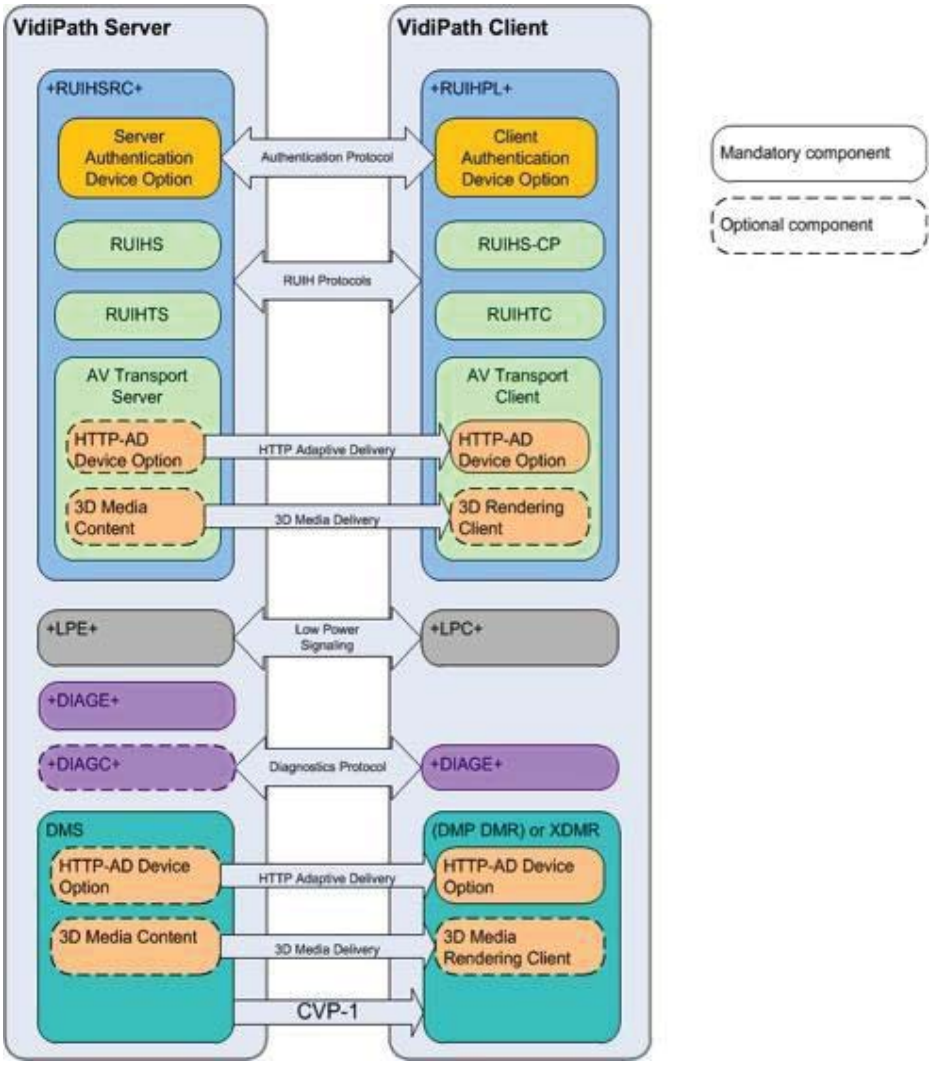


Figure 20 - DLNA VidiPath Architecture

HTML5 Remote User Interface (RUI)

In order to support a consistent MVPD user interface to different form factors of retail devices (e.g., TVs, tablets, mobile phones, and, game consoles) and requirements identified in the Application Framework subsection, DLNA VidiPath specifications specify support for an HTML5-based Remote User Interface. DLNA HTML5 Remote RUI specification defines a profile of W3C's

HTML5 specification [39] and other related specifications such as Cascading Style Sheets (CSS), Web Sockets, XMLHTTPRequest (Ajax), and FullScreen.

HTML5 is a widely adopted industry standard supported by a broad range of browsers on a wide variety of devices. Thus, it enables MVPDs to develop their guide once and offer it on a wide range of platforms resulting in reduced development costs and faster time to market for new services/applications. It also enables MVPDs to offer their guides directly from the cloud, thereby enabling them to rapidly evolve their services and applications to consumers.

An MVPD video gateway advertises that the Uniform Resource Locator (URL) of the MVPD HTML5 guide and VidiPath devices discover the URL using the UPnP RUI Discovery mechanism [63]. Cable operator's HTML5 guide can be served either from the in-home video gateway or from the cloud. Using the <video> tag defined in the HTML5 specification, MVPDs are able to display video within their guide user interface pages. DLNA HTML5 RUI Specification defines DLNA specific extensions to support playback of video content using <video> tag over an IP link protected by Digital Transmission Copy Protection (DTCP). In addition, the DLNA HTML5 RUI specification defines extensions to HTML5 <video> tag to support time-based seek and playspeed trick modes so that a consumer is able to pause, rewind and forward the video from the HTML5 guide page.

CableLabs developed a specification [64] that defines a standardized mechanism for exposing information about MVPD regulatory and contractual services, such as closed captions, content advisories, SAP, DVS, and ad insertion carried in the MPEG-2 TS video stream as HTML5 audio, video and text tracks, so that MVPD HTML5 Web applications can provide these services to consumers. DLNA HTML5 RUI requires implementation of this specification, so that MVPDs can fulfill their regulatory and contractual obligations while offering the full MVPD service to VidiPath devices. DLNA HTML5 RUI Specification also requires support for W3C's Server Sent Events (SSE) specification [65]. Using SSE, MVPDs are able to provide EAS messages to MVPD HTML5 RUI applications running on VidiPath devices. Figure 21 shows various HTML5 RUI entities and their functions.

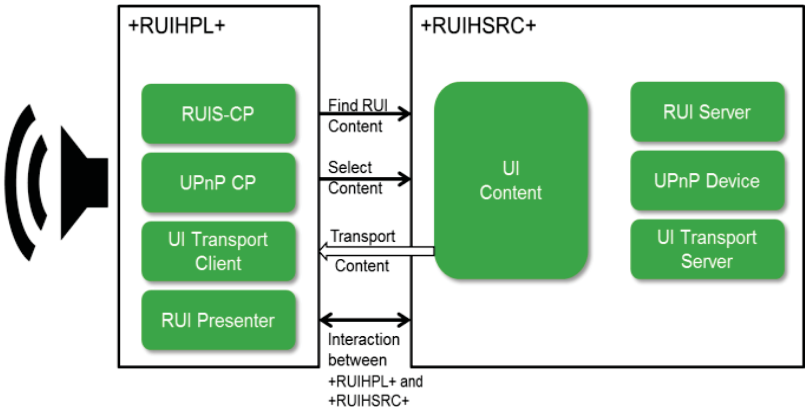


Figure 21 - VidiPath HTML5 RUI Usage Model

HTML5 RUI (RUI-H) Source capability (+RUIHSRC+) has the role of exposing and sourcing RUI-H content and includes RUI-H Server (RUIHS), RUI-H Transport Server, and an optional DLNA Media Transport Server (for serving media content):

- RUIHS provides UPnP RUI Server device functionality, which enables VidiPath Servers to offer one or more remote UIs based on HTML5, and to handle UPnP RUI Server service actions.
- RUI-H Transport Server and RUI-H Transport Client are the device functions for transport of the RUI-H content between a client and server.
- RUI-H Pull Controller (+RUIHPL+) has the role of finding and loading RUI-H content that is exposed by a +RUIHSRC+ capability, rendering the UI content, and interacting with it. RUI-H Pull Controller includes RUI-H Server Control Point (RUIHS-CP), RUI-H Transport Client, RUI-H User Agent and an optional DLNA Media Transport Client.
- RUIHS-CP is a controller for browsing and selecting an HTML5 remote UI offered by a RUI-H Server.
- RUI-H User Agent functionality on a RUI-H Client is responsible for retrieving, decoding, presenting and interacting with the RUI-H content received from the RUI-H Server.

MPEG-2/AVC Media Formats

In order to support the full set of MVPD service features, retail devices need to support an appropriate set of audio and video codecs with specific resolution, bit rate, and frame rate. MVPD video content predominantly uses MPEG-2 video encapsulated in MPEG-2 TS, and H.264/AVC in MPEG-2 TS to a lesser degree. In addition, support for adaptive bit rate streaming needs to be considered as MVPDs may have a need to stream video over Wi-Fi networks to portable devices. Support for MVPD contractual and regulatory services (e.g., closed captions, parental control, EAS, SAP, and ad insertion) needs to be supported by this application framework. Information about these services for video content is carried in-band as elementary streams of the MPEG-2 transport streams (TS). So, the application framework needs to support mapping of these elementary streams to the application layer. In order to enable rapid application development cycle, the application framework needs to support a “write once and run anywhere” model.

In order to ensure baseline interoperability between the VidiPath Server and the VidiPath Client, the DLNA VidiPath specifications define a required set of Media Format profiles for both VidiPath Server and Client for a particular geographic region (e.g., North America, Europe). This set of media format profiles is representative of premium content sourced by service providers in that particular region.

MPEG-2, as well as AVC/H.264 video encapsulated in MPEG-2 TS with resolutions up to 1080p, are required. Support for audio codecs such as AC-3, E-AC-3, AAC, MP3, and MPEG Layer-1 & 2 is

required as a part of this media format profile set. Additionally, AVC video encapsulated in MP4 containers needs to be supported to enable interoperability with portable devices. VidiPath Server and Client devices are also required to support DLNA specified trick modes (byte seek, time seek and playspeed) and DTCP-IP link protection for this set of media format profiles. Due to this mandatory set of media format profiles, as long as MVPDs offer their content using one of the media format profiles from the VidiPath server implemented in the video gateway, a VidiPath Client device will be able to play back the content over the home network.

DTCP-IP Link Protection

In order to meet content provider expectations and requirements, DLNA VidiPath specifications leverage Digital Transmission Content Protection over Internet Protocol (DTCP-IP) Link Layer protection technology to secure content from unauthorized copying and misuse within the home as it is streamed from a MVPD video gateway to a VidiPath client device. DTCP-IP is a link protection specification published by Digital Transmission License Administrator [66].

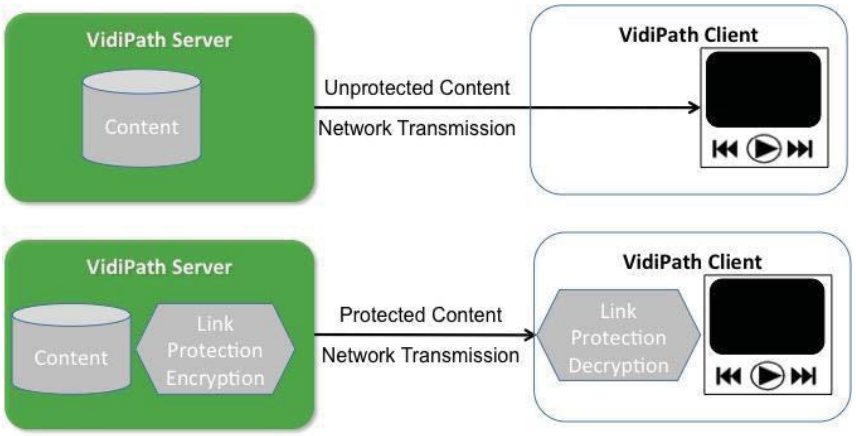


Figure 22 - Secure content transmission using DTCP-IP

This is a critical enabler for multi-device viewing experiences involving premium subscription TV content. DTCP-IP is automatically negotiated between devices and has been designed to provide certain content protection as content moves across the local home network. In accordance with the VidiPath specifications, digital content can be shared securely between products in a user's home, but not with third parties outside the home network.

DLNA VidiPath Diagnostics

As premium video content is streamed over the home network from a video gateway to retail devices, MVPDs need a mechanism to diagnose and troubleshoot home network related issues remotely. Such a mechanism needs to support the ability to test the home network's connectivity between a video gateway and retail devices, provide network topology, and information about network throughput. In addition, the ability to query information about retail

devices such as device model, manufacture, and, firmware version needs to be enabled by this mechanism.

The DLNA VidiPath Diagnostics feature focuses on the collection of data about the home network conditions and devices through a set of actions and queries, so that a MVPD or a user can take appropriate steps to troubleshoot and diagnose service-related issues. The VidiPath diagnostics feature relies on UPnP Device Management [67] as a required functionality, and IEEE 1905.1 [68] as an optional functionality. UPnP Device Management provides the ability to collect layer-3 & layer-4 diagnostics information such as IP-connectivity, network bandwidth, device information, and device status. IEEE P1905.1 provides layer-2 diagnostics information such as layer-2 link information, status, and layer-2 topology information.

Figure 23 shows various DLNA Diagnostics logical entities and their functions.

- A Diagnostics Endpoint (+DIAGE+) capability has the role of offering diagnostics services and responding to diagnostics action requests by implementing UPnP Basic Management Service v2 [69] as a required service and UPnP Configuration Management Service v2 [70] as an optional service. DLNA VidiPath Specifications requires certain actions to be implemented, such as Ping, Trace Route, and NSLookup. Both the VidiPath Servers and Clients are required to support diagnostic Endpoint capability.

- Diagnostics Controller (+DIAGC+) has the role of providing a diagnostics application and a control point for issuing action requests to a +DIAGE+. However, a Diagnostics Controller is optional for VidiPath device profiles, although it is expected that a Diagnostics Controller may be included on a VidiPath server to allow the service provider's support staff to diagnose issues within the consumer's home. The diagnostics application drives the Diagnostics Controller to access diagnostics data and capabilities. Cable operators remotely access the diagnostics application running on the VidiPath server using a TR-069 or SNMP management interface. Alternatively, a MVPD technician or end-user may access the diagnostics application through a browser or screen interface as shown in Figure 23.

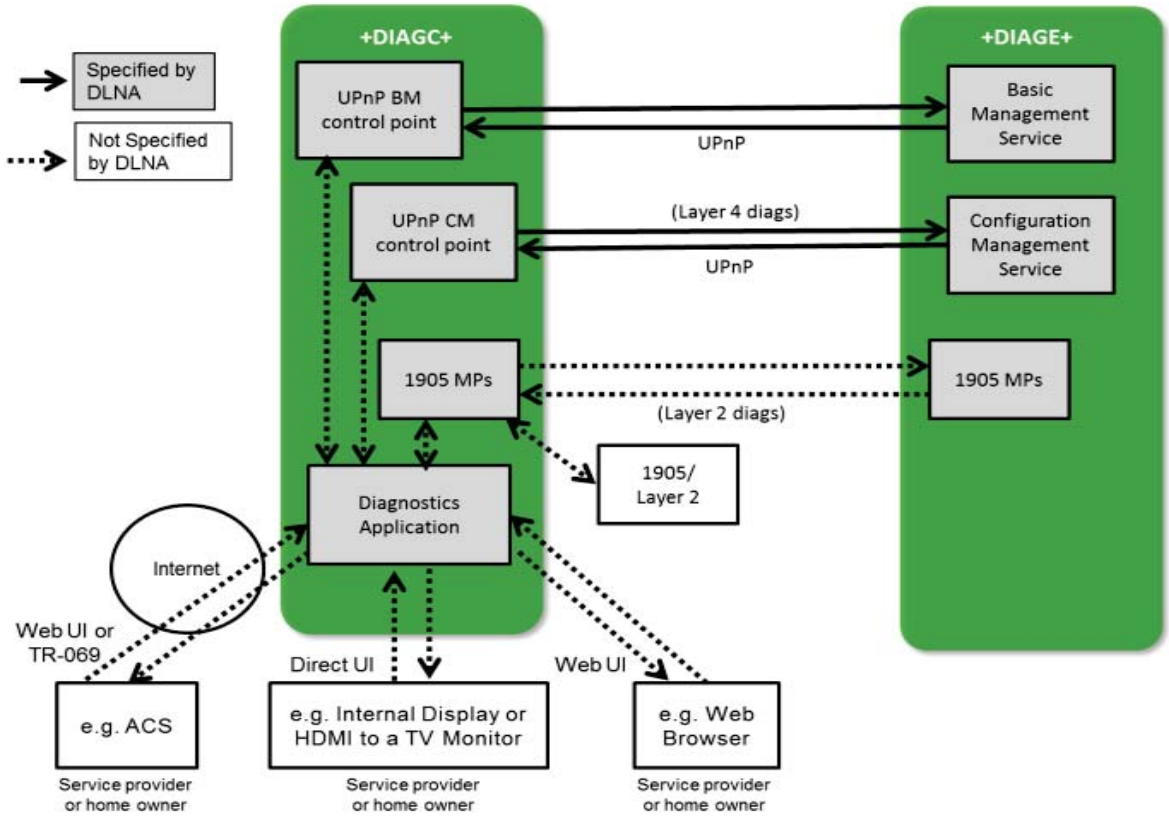


Figure 23 - VidiPath Diagnostics Architecture

Low Power

In order to meet consumer expectations and MVPD requirements for energy efficiency, MVPD STBs and gateways implement energy saving operations, including various types of sleep modes. To avoid a consumer having to explicitly wake up the video gateway when the consumer wants to watch video content on a retail device, it is necessary that the retail device is able to wake up the video gateway from sleep mode.

To account for service provider STB/video gateway devices implementing energy saving operations, e.g., different levels of sleep modes, the DLNA VidiPath specifications provide wake-up or reservation mechanisms to VidiPath client devices. The specifications enable DLNA devices to convey energy management and sleep-mode capabilities for each of its network interfaces. This facilitates the awareness of the availability of DLNA functionality, even in the presence of power-saving mode operations. The VidiPath Low Power feature is based on the UPnP Energy Management Service [71].

Power savings is modular within a physical device. In the context of DLNA networked devices, as shown in Figure 24, each physical network interface can have various power modes. Some of these power modes can allow layer-2 or layer-3 connectivity to still be present even when many other device components are powered down. Other physical components, such as screens, hard drives and similar resources, can also support different power modes.

The VidiPath Low Power feature consists of the following entities:

- Low Power Endpoint (+LPE+) capability implements UPnP Energy Management Service and has the role of responding to action requests, including requests to provide information on network interface mode, and requests to access services based on subscriptions.
- Low Power Controller (+LPC+) capability implements a control point for the UPnP Energy Management Service and has the role of issuing action requests to a Low Power Endpoint or a Low Power Proxy.

The VidiPath Server is required to implement Low Power Endpoint (+LPE+) capability, and the VidiPath Client is required to implement Low Power Controller (+LPC+) capability. This enables VidiPath Clients to query information about power save mode operations of a service provider's VidiPath Server and invoke appropriate actions to wake-up the VidiPath Server when its services are needed for the consumer. Waking up a VidiPath Server from the low-power mode can introduce some latency and longer response time, so it is expected that a VidiPath Client provides appropriate messages to the user to provide a good user experience.

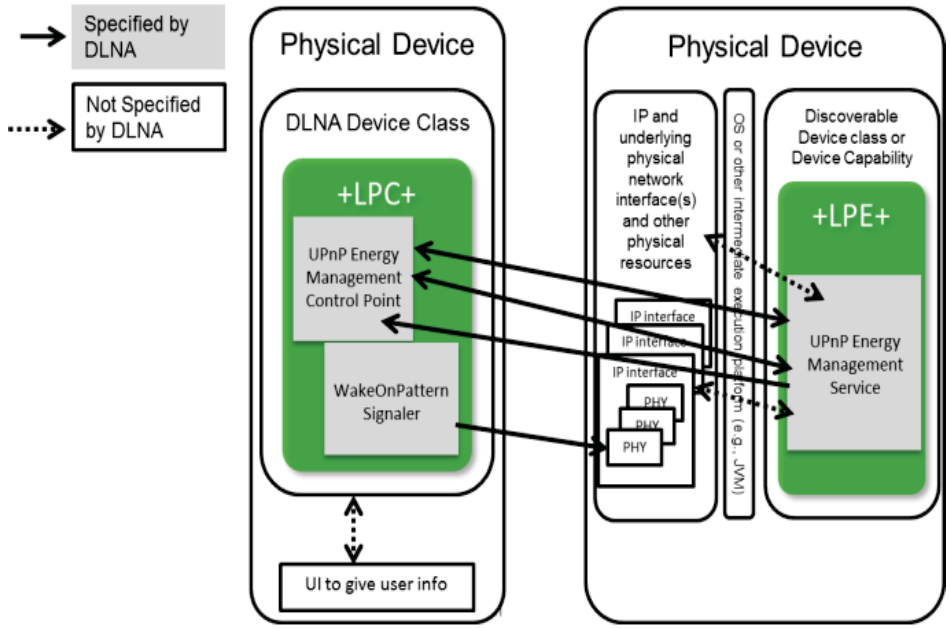


Figure 24 - DLNA Low Power Architecture

HTTP Adaptive Delivery

The HTTP Adaptive Delivery feature of VidiPath enables service providers to describe content as adaptive content; i.e., in timed segments at various bit rates and in various media formats. In the event of network congestion, which is likely to happen over Wi-Fi, a client rendering devices can maintain smooth streaming of content for display by switching between streams at different

bitrates. A Media Presentation Description (MPD) file provided by a server includes segment information such as timing, URL, and, media characteristics (e.g., video resolution and bit rates). This feature leverages Moving Picture Expert Group Dynamic Adaptive Streaming (MPEG-DASH), over HTTP (ISO/IEC 23009-1) standard [40]. Additionally, DLNA VidiPath specifications mandate support for ISO-based media file format (ISOBMFF) Live, ISOBMFF On-Demand, and MPEG-TS Simple profiles defined in the MPEG-DASH specification [40].

Different logical entities of the HTTP Adaptive Delivery feature are shown in Figure 25.

VidiPath Clients are required to support HTTP Adaptive Delivery device option and aforementioned HTTP Adaptive media format profile. Support for HTTP Adaptive delivery is optional for a VidiPath Servers, but if it is supported, then the VidiPath Server is required to support at least one of the HTTP Adaptive media format profiles.

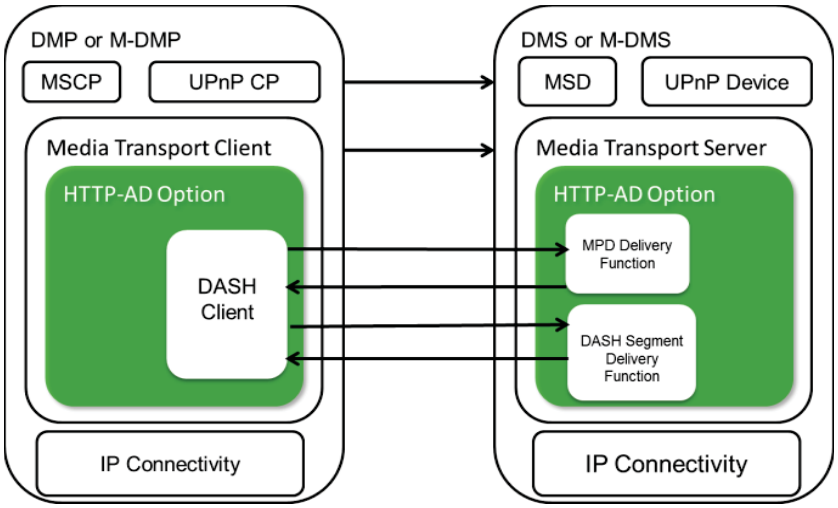


Figure 25 - HTTP-Adaptive Delivery Entities

On the VidiPath Server, the HTTP Adaptive Delivery device option has the role of exposing and sourcing content using the HTTP Adaptive Delivery mode. This includes exposing and sourcing both the MPD and the media itself (segments for different representations). This functionality maps to the MPD delivery function and segment delivery function in MPEG-DASH. On the VidiPath client side, the HTTP Adaptive Delivery device option has the role of requesting appropriate content MPD and media representation (segments), and assembling and rendering the media while adapting to changing network conditions.

Authentication

By utilizing the VidiPath Authentication feature, service providers can verify that the VidiPath client has been certified to the DLNA VidiPath specifications. This provides confidence to service providers that a VidiPath Client is able to display their HTML5 RUI guide, meet regulatory requirements, and deliver content services appropriately to meet consumer expectations.

The VidiPath authentication feature also supports authentication of a VidiPath Server by a VidiPath Client. A VidiPath Client can optionally authenticate a VidiPath Server to ensure that the Client is talking to a legitimate VidiPath Server to protect consumers from rogue servers.

Upon DLNA certification of a VidiPath device (Client or Server), a device manufacturer obtains a DTLA VidiPath Certificate, which has the same format as the legacy DTLA DTCP certificate used for DTCP-IP link protection, except that it has a special field that indicates the device is DLNA VidiPath certified. The same certificate is used by the device for VidiPath device authentication as well as for DTCP-IP link protection. This avoids including additional certificates in the device and saves cost for the device manufacturer. If a service provider authentication server is located in the cloud, then it obtains a VidiPath X.509 certificate from DTLA.

DLNA VidiPath Authentication uses Transport Layer Security Supplemental Data (TLS-SD) extensions, defined in RFC 4680 [72], to carry VidiPath client's DTLA VidiPath certificate over Hypertext Transfer Protocol over Transport Layer Security (HTTPS). Standard Transport Layer Security [73] protocol only supports transport of X.509 certificates. A TLS-SD extension [72] allows transport of arbitrary pieces of information over the TLS protocol.

The HTML5 RUI browser implemented by the VidiPath Client is responsible for performing authentication using HTTPS with MVPD Authentication Server. Cable operator Authentication Server verifies that the device requesting service is a DLNA Certified VidiPath device based on the DTCP VidiPath certificate supplied using the DLNA VidiPath authentication protocol.

Error! Reference source not found. shows various VidiPath authentication logical entities:

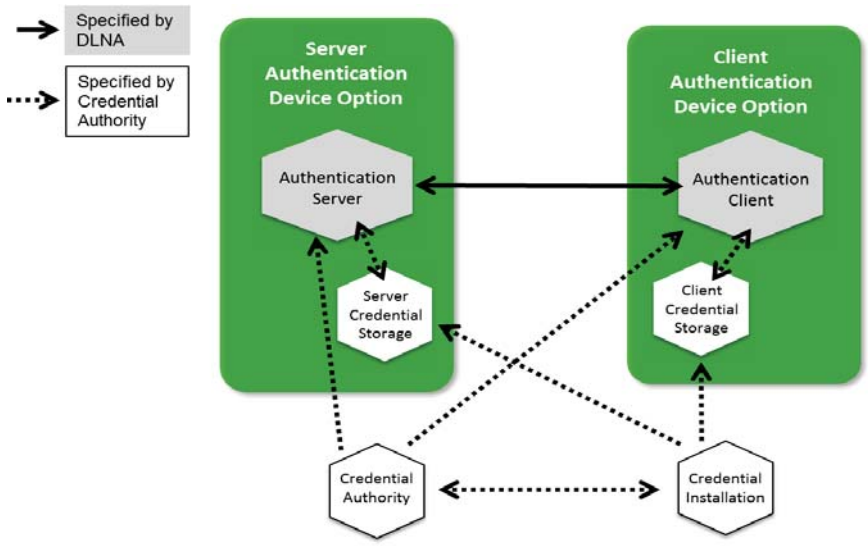


Figure 26 - VidiPath Authentication Entities

- Client Authentication is a device option that supports client credentials and the protocols to allow a client to be authenticated by an Authentication Server.

- Server Authentication is a device option that supports server credentials and the protocols to allow a server to be authenticated by an Authentication Client.

The DLNA VidiPath Authentication supports two different scenarios for the Client/Server Authentication:

1. In the first scenario, shown in Figure 27, the Authentication Server is in the cloud and authentication must be accomplished with a cloud-based server. In this scenario, the server uses trusted X.509 VidiPath certificate and client uses DTLA VidiPath certificate.

2. The second scenario is shown in Figure 28, where the Authentication Server is located in the home (in a video gateway/STB) and all authentication protocol exchanges are performed within the home network. In this scenario, the server uses trusted or self-signed X.509 certificate signed with DTLA VidiPath certificate, and client uses DTLA VidiPath certificate.

Other VidiPath Features

- **Digital Media Server (DMS)**: VidiPath Server is required to support DLNA DMS device class. This provides essential functions of device discovery, content streaming with support for trick modes (pause, rewind, forward).
    - There is no exported Content Directory Service (CDS) for access of video content outside of the MVPD RUI.

- **Digital Media Player (DMP)/Digital Media Renderer (DMR):** VidiPath Client is required to implement DLNA DMP and DMR device classes. These provide essential functionality for content streaming with support for trick modes. DMR provides device discovery and “Play To” scenario where a phone or tablet can establish and control content streaming between a DMS and DMR.

- **Priority-based Quality of Service (QoS):** DLNA VidiPath requires prioritized QoS solution where video streams are given a higher priority over data/background traffic over the home network. The majority, if not all, of home networking technologies (e.g., Ethernet, Wi-Fi, MoCA, HomePNA, and HomePlug) support traffic prioritization when packets are marked with layer-2 802.1 p/q tags. The VidiPath Server is required to mark video packets with diffserv codepoints (DSCP), as well as with layer-2 802.1 p/q tags, so that video traffic receives appropriate priority when streamed over the home network.

MVPDs and content providers, want to ensure that their services are offered with the highest quality when the content is streamed over the home network from a video gateway to retail devices. Thus, it is necessary to avoid congestion or interference of home network traffic that could degrade the quality of user experience. Therefore, it is necessary to consider that a video gateway and retail devices support a home network technology with throughput in excess of

100 Mbps (enough to support 3 MPEG-2 video HD streams). In addition, support for either priority-based or parameterized quality of service (QoS) needs to be considered.

- **3D Media Formats:** DLNA VidiPath specifications conditionally mandate support for 3D media formats for VidiPath Clients and Servers. DLNA has defined a set of frame-compatible stereoscopic-3D media formats (Side-by-Side and Top-and-Bottom), which are representative of content supplied by service providers. If the VidiPath client supports rendering of 3D video, then it is required to implement support for these DLNA defined 3D media formats.

VidiPath Deployment Scenarios

The DLNA VidiPath Specifications support two deployment scenarios: Hybrid In-Home + Cloud scenario, and In-home only scenario.

In the hybrid In-home+Cloud Scenario, the MVPD's HTML5 RUI server and authentication server reside in the cloud, but all other functions of VidiPath server reside on an in-home video gateway or STB. A VidiPath

Client discovers URL of the MVPD's cloud guide from an in-home VidiPath gateway/STB. The VidiPath Client is authenticated with a cloud Authentication Server, which may be co-located with the cloud RUI server (server uses trusted X.509 VidiPath certificate). Upon authentication, the VidiPath Client downloads MVPD HTML5 guide from the cloud. The HTML5 guide has links to video content that point to the in-home gateway/STB. Thus, actual video content is served from in-home gateway/STB to the VidiPath Client.

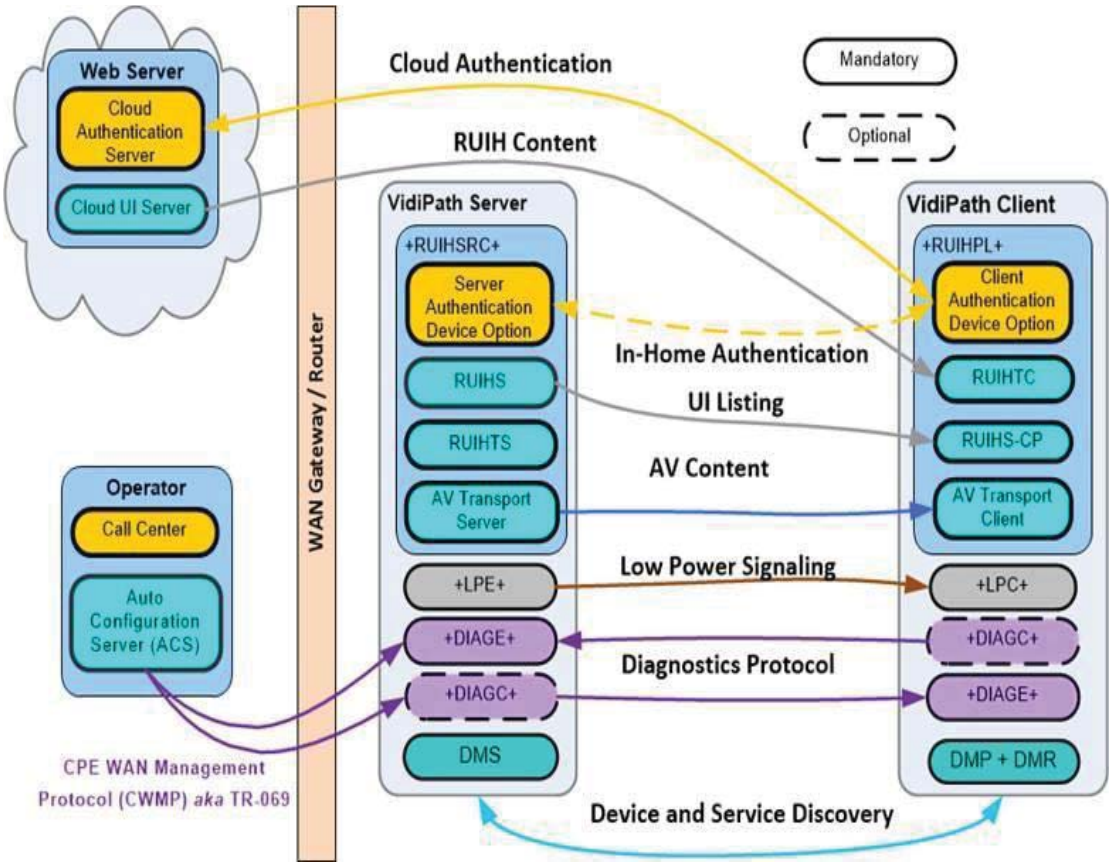


Figure 27 - Hybrid In-home + Cloud Deployment

In the In-home only deployment scenario, the MVPD's HTML5 RUI server and Authentication Server reside in the in-home gateway/STB along with all other VidiPath Server functions. A VidiPath Client discovers URL of the MVPD's guide from an in-home VidiPath gateway/STB, which is served from within the home from the same gateway/STB. The same gateway/STB also hosts the Authentication Server.

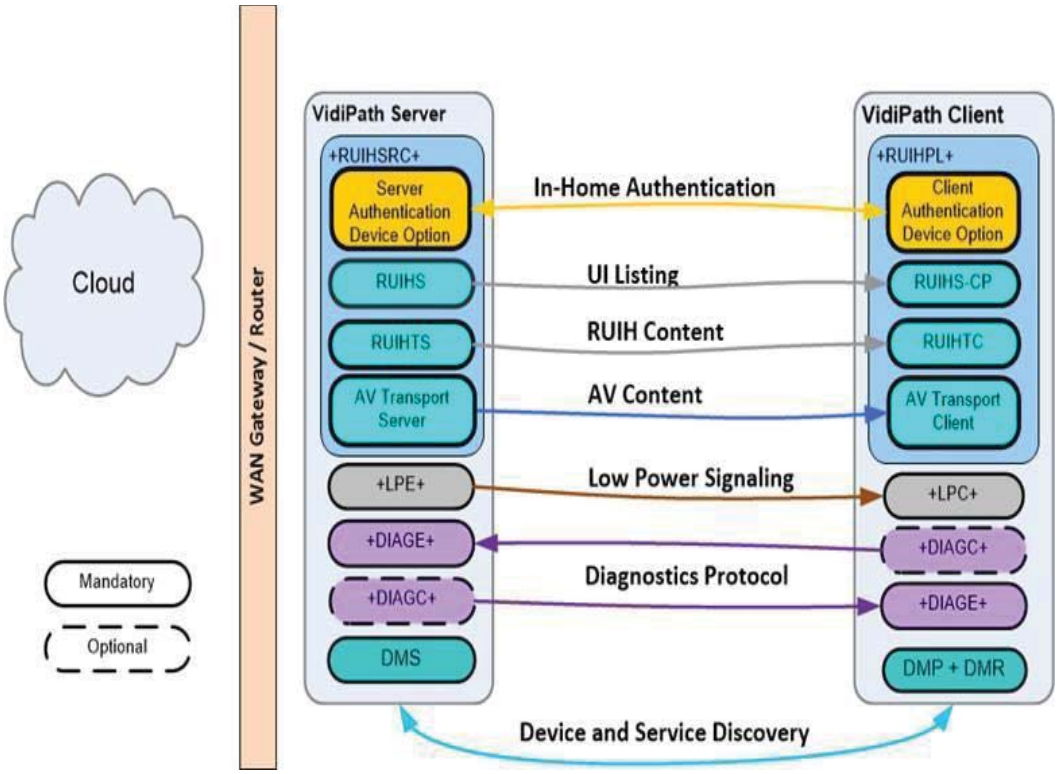


Figure 28 - In-home only Deployment

The VidiPath Client is authenticated with the in-home Authentication Server (the server uses self- signed or trusted X.509 certificate signed with VidiPath certificate). Upon authentication, the VidiPath Client downloads MVPD HTML5 guide to access content services from the in-home gateway/STB VidiPath Server.

Standards

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

Open Source Implementations of CVP-2 Server and Client, CableLabs, http://html5.cablelabs.com/dlna-cvp-2/index.html [55]

Reference Device Kit (RDK), http://rdkcentral.com [56]

HTML5 - A vocabulary and associated APIs for HTML and XHTML, W3C Recommendation, World Wide Web Consortium, http://www.w3.org/TR/html5/ [39]

RemoteUIServer:1 Service Template Version 1.01, For UPnP™ Version 1.0, September, 2, 2004, http://upnp.org/specs/rui/UPnP-rui-RemoteUIServer-v1-Service.pdf [63]

Mapping from MPEG-2 Transport to HTML5, I03, CL-SP-HTML5-MAP-I03-140207, Cable Television Laboratories, Inc. Specifications, Web Technology, February, 7, 2014 [64]

Server Sent Events, W3C Candidate Recommendation, 11 December 2012, http://www.w3.org/TR/eventsource/ [65]

DTCP Volume 1 Supplement E, Mapping DTCP to IP, Revision 1.4 ED3, June 5, 2013, Digital Transmission License Administrator, http://www.dtcp.com/documents/dtcp/info-20130605-dtcp-v1se-ip-rev-1-4-ed3.pdf [66]

UPnP Device Management: 2, http://upnp.org/specs/dm/dm2/ [67]

IEEE 1905.1, IEEE Standard for a Convergent Digital Home Network for Heterogeneous Technologies, 2013, http://standards.ieee.org/findstds/standard/1905.1-2013.html [68]

BasicManagement:2, Service Template Version 1.01, For UPnP™ Version 1.0, February 16th, 2012, http://upnp.org/specs/dm/UPnP-dm-BasicManagement-v2-Service.pdf [69]

ConfigurationManagement:2, Service Template Version 1.01, For UPnP™ Version 1.0, March 4th, 2013,http://upnp.org/specs/dm/UPnP-dm-ConfigurationManagement-v2-Service.pdf [70]

EnergyManagement:1, Service Template Version 1.01, For UPnP™ Version 1.0, August 30, 2013, http://upnp.org/specs/lp/UPnP-lp-EnergyManagement-v1-Service.pdf [71]

ISO/IEC 23009-1:2012: Information technology -- Dynamic adaptive streaming over HTTP (DASH) -- Part 1: Media presentation description and segment formats. [40]

S. Santesson, TLS Handshake Message for Supplemental Data, IETF RFC 4680, September 2006, http://tools.ietf.org/html/rfc4680 [72]

T. Dierks, et al, The Transport Layer Security (TLS) Protocol, Version 1.2, IETF RFC 5246, August 2008, http://tools.ietf.org/html/rfc5246 [73]

Gnome's Rygel Project, https://wiki.gnome.org/action/show/Projects/Rygel?action=show&redirect=Rygel

dLeyna Project, Intel Open Source Technology Center, https://01.org/dleyna

The WebKit Open Source Project, http://www.webkit.org [74]

The GTK+ Project, http://www.gtk.org

GStreamer, Open Source Multimedia Framework, http://gstreamer.freedesktop.org

Protocols

The protocols used include:

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

Information

The DLNA VidiPath Guidelines can be obtained at: DLNA Guidelines, http://www.dlna.org/dlna-for-industry/technical-overview/guidelines [60]

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.

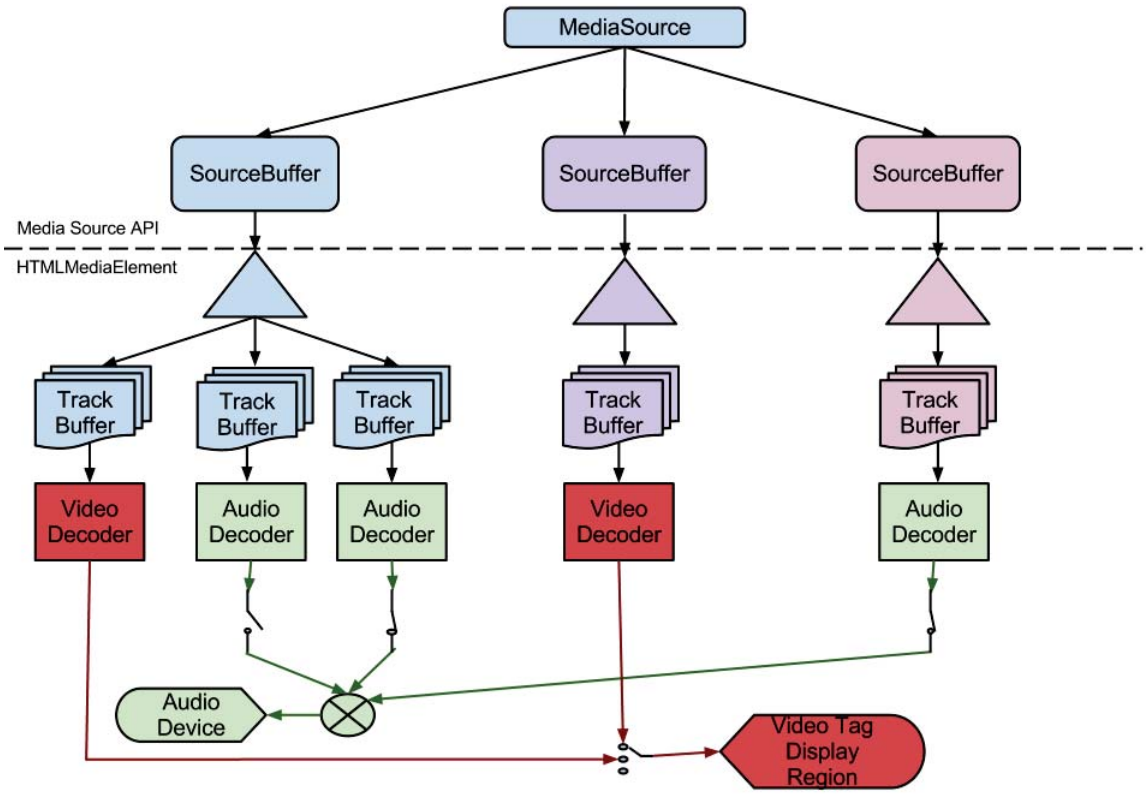


Figure 29- Media Source Extensions Architecture

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).

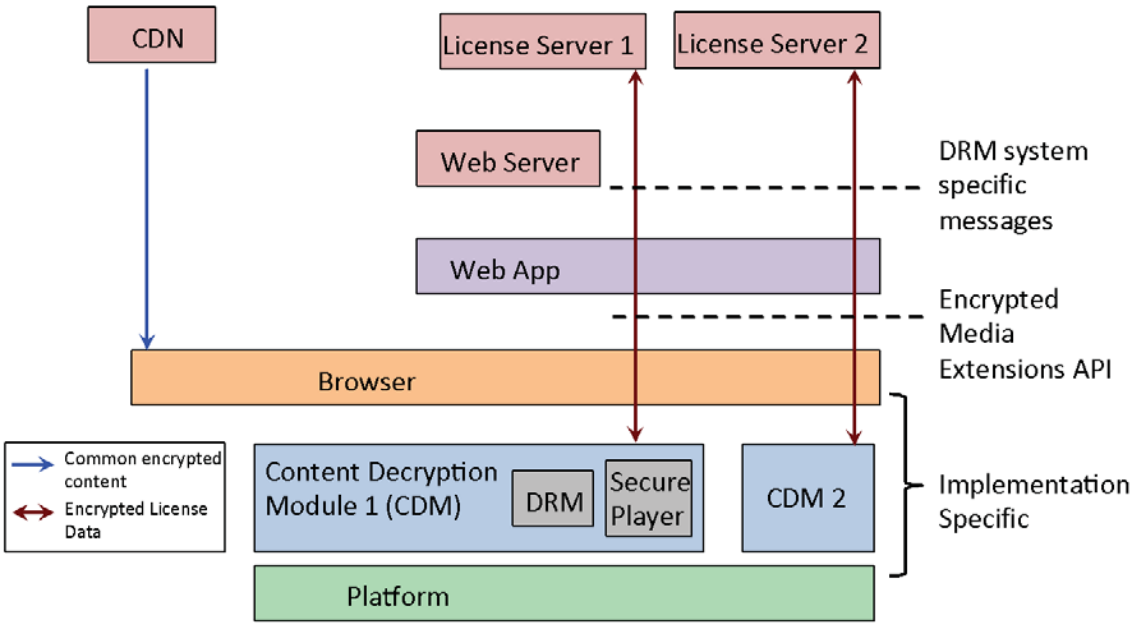


Figure 30- Encrypted Media Extensions Architecture

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.

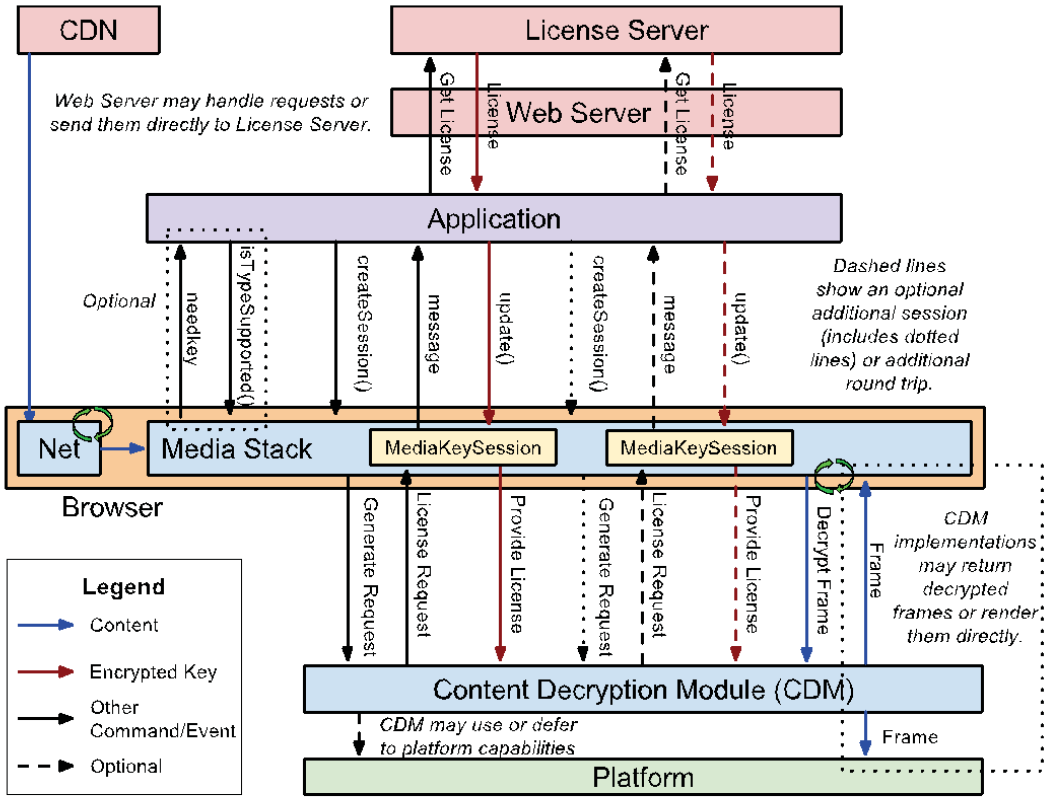


Figure 31 - Detailed EME Architecture with APIs

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

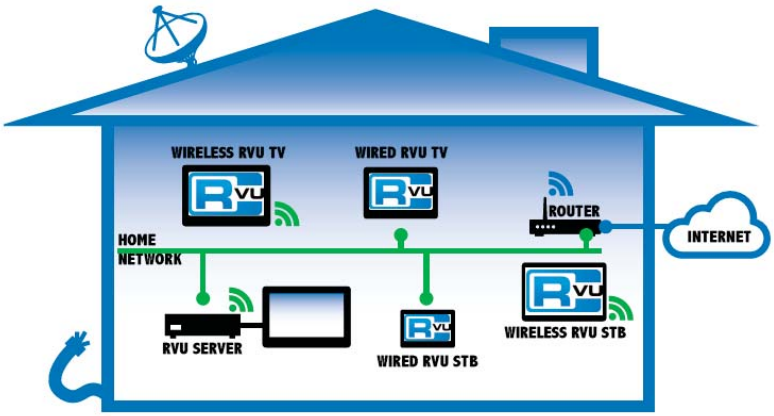
HTML5 with EME and MSE is applicable to any device that implements these specifications including: smart/connected TVs, game consoles, PCs, tablets, and smart phones. HTML5 can support a browser user interface (e.g. Chrome or Firefox on a PC) or HTML5 can support an application environment that looks 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.

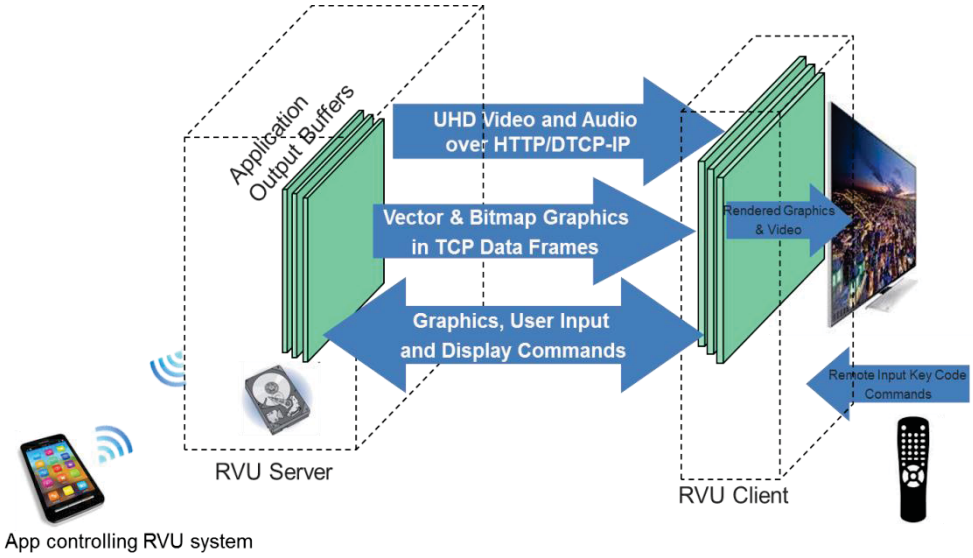


Standards

The RVU protocol specification is built upon UPnP device discovery, DLNA media streaming and DTCP-IP content protection.

Protocols

The RVU remote user interface (RUI) protocol complements devices implementing content streaming protocols of the DLNA guidelines [60]. The concept of a remote user interface for clients is not new. However, the idea that clients should be able to provide a full-featured user interface by implementing minimal functionality, leaving most of the "hard work" to the server, is unique to RVU. The objective of RVU is to keep clients as process-light as possible. The RVU RUI delivers bitmapped and/or vector graphic user interface data for a robust, consistent UI experience throughout the home via thin clients as opposed to implementations with an entire UI via client-side software. Clients implement relatively simple software to send key events to the server and display the RUI graphics and video/audio received in response.



Information

The RVU Alliance is a non-profit technology standards alliance comprised of service providers, consumer electronics manufacturers and technology providers to develop and maintain the RVU protocol specification for a small footprint full-featured Remote User Interface (RUI). Board level promoter members include Broadcom, Cisco, DIRECTV, Samsung and MaxLinear. Other members are LG, Sony, Toshiba, Sharp Electronics, Dolby Laboratories, Humax, JetHead Development Inc, Awox, MStar, Pace PLC, Sky Brasil, ST Microelectronics, Arris and Technicolor.

Applicable Devices

For a list of certified devices, including 4K/UHD clients, see www.rvualliance.org/products.

Section VIII: Passage

Description

Passage is a technology that enables security interoperability similar to DVB Simultcrypt. It is suitable for broadcast linear streams where a service provider supports simultaneous distribution to receivers with legacy Conditional Access (CA) and new security such as Digital Rights Management (DRM).

While the in-stream signaling for Simulcrypt and Passage are similar and the results are the same - allowing receivers with different security systems to receive the same transport stream - it is accomplished through different means.

Simulcrypt accomplishes interoperability through key sharing. The scramble key content is delivered separately through proprietary means to receivers with different security systems. The content is 100% encrypted and both systems share low-level descrambling capability.

However, key sharing may not always be possible or desirable. Legacy scrambling uses out-of-date algorithms such as DVB Common Scrambling Algorithm (CSA), DES or DES-CBC. Often the security extends into the descrambling by keeping certain information secret, e.g. Initialization Vectors for DES-CBC or scrambling mode variations, to create anti-cloning mechanisms. Another anti-hack feature of some legacy security systems is very rapid key changes which makes key sharing with other security systems problematic.

Passage accomplishes interoperability through selective multiple encryption. A small amount of critical content data, typically less than 2% of the bandwidth, essential for decompressing the rest of the content (sent in-the-clear), is duplicated and scrambled two ways – one for legacy CA and one for DRM. Each receiver gets the same transport stream, selects its respective scrambled content, and share the remaining clear common content.

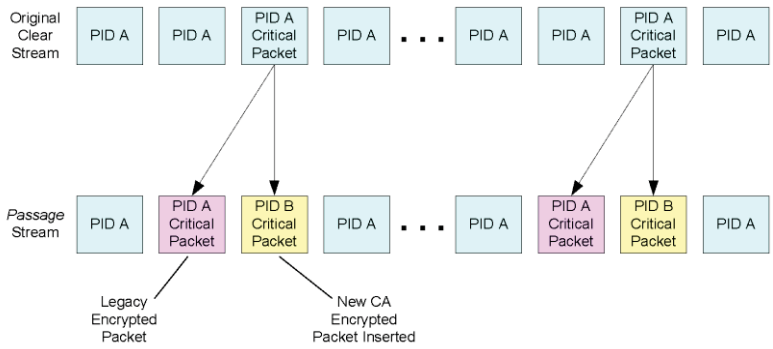


Figure 32 - Creation of Passage Selective Multiple Encrypted Stream

Unlike Simulcrypt, since Passage allows for the independent scrambling of critical packets of content, there are the following benefits:

- The security of the large base of legacy receivers in the field is not put at risk.
    - Divulging and licensing of the legacy descrambling know-how, e.g. Initialization Vectors, are not required. This lowers the risk of inappropriate divulging of the information and also of legacy clone hardware being available.
    - Knowledge of a scrambling key leaked from the new security system cannot be used to reverse engineer and attack the legacy security system. Alternatively, a key leaked from the legacy security system cannot be used to attack the new security system.
    - There is no need to "slow" key changes on the legacy system or share a higher level of the legacy key derivation protocol thereby reducing overall resilience to a hack in order to be compatible with the new security security.
- Since no secrets need to be shared between security systems, there should be no legacy CA provider security indemnity concern for the service operator.
    - Breaches should be readily identifiable as to which keys and which scrambled packets are being hacked.
- The alternate packet may be scrambled using efficient implementations of the AES-128 algorithm which may be more readily supported by DRMs and mobile device platforms.
- As with Apple HTTP Live Streaming [38], Passage's use of selective encryption may make efficient software-only implementations possible for new classes of devices and services.
- Legacy CA can be bypassed in new devices along with any licensing issues.
- Content rights need not be limited to the Copy Control Information (CCI) bits. Content rights associated with the DRM encrypted alternate packets can maintain persistent control over content by the service operator from broadcast to rendering – enabling new use cases.

Passage Headend Encoding

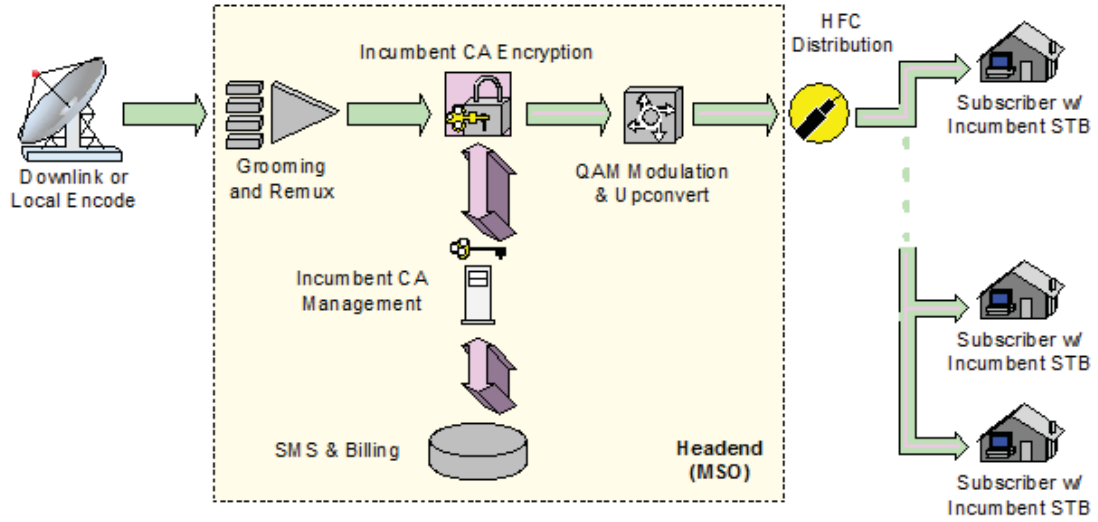


Figure 33 – Typical Digital Cable System Architecture

Passage Technology

Passage technology enables equipment from multiple vendors to be deployed on legacy digital cable networks—without the need to duplicate content or bandwidth. Passage technology recognizes MPEG compression as a form of encryption.

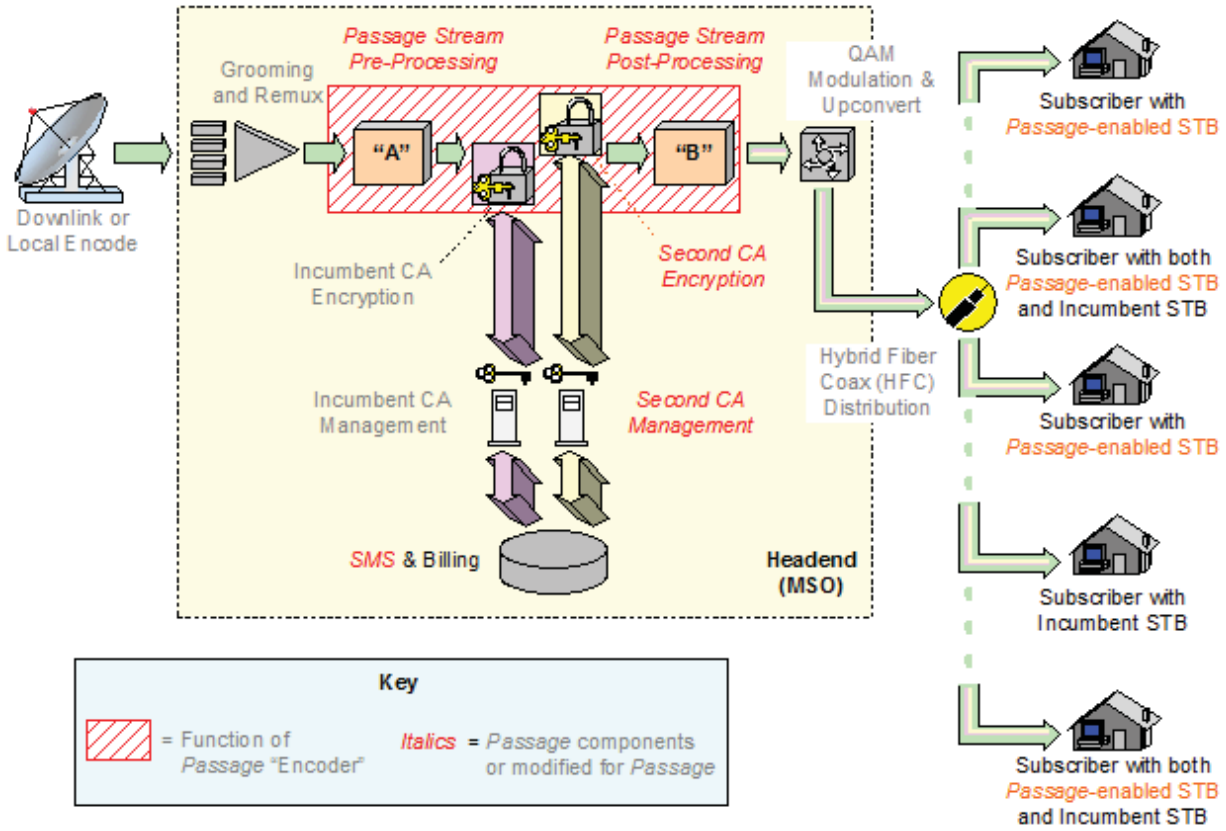


Figure 34 – *Passage*-enabled Digital Cable System

Passage technology supports multiple security systems, and it treats each security system independently. Passage allows each security system to operate on its own encrypted data. As explained in more detail later, Passage encoding carefully chooses the data that is encrypted. This process allows multiple security systems to co-exist in an existing cable plant.

Passage technology supports DVB open standards. Support of DVB open standards allows interchangeable headend equipment operation, and interoperability of multiple security systems.

New equipment adhering to the open standards architecture will process the data encrypted by the new security system. At the same time, the legacy equipment, using proprietary methods, processes the data encrypted by the legacy CA as before.

System Architecture

The Passage system architecture enables the deployment of field-configurable, modular systems. Passage technology also avoids the geographical or spectral partitioning usually required when introducing non-legacy components to an existing plant and the licensing or interoperability problems associated with multiple CA systems. With Passage technology, there is no need for key sharing or CA licensing. Secret proprietary information needed for descrambling need not be shared between the legacy CAS vendor and the new security system.

Vital data, essential for decoding, is selected, duplicated, and encrypted in two ways: once for legacy devices, e.g. STBs, and once for Passage devices, e.g. STBs, TVs, and mobile devices. Each device receives the same transport data and appropriately selects its encrypted data. The remaining content is shared by all devices. Only the critical data necessary for recovering video or audio content needs to be encrypted. The Passage system only encrypts critical data. If a decoder cannot receive the critical data, then the video image cannot be decompressed.

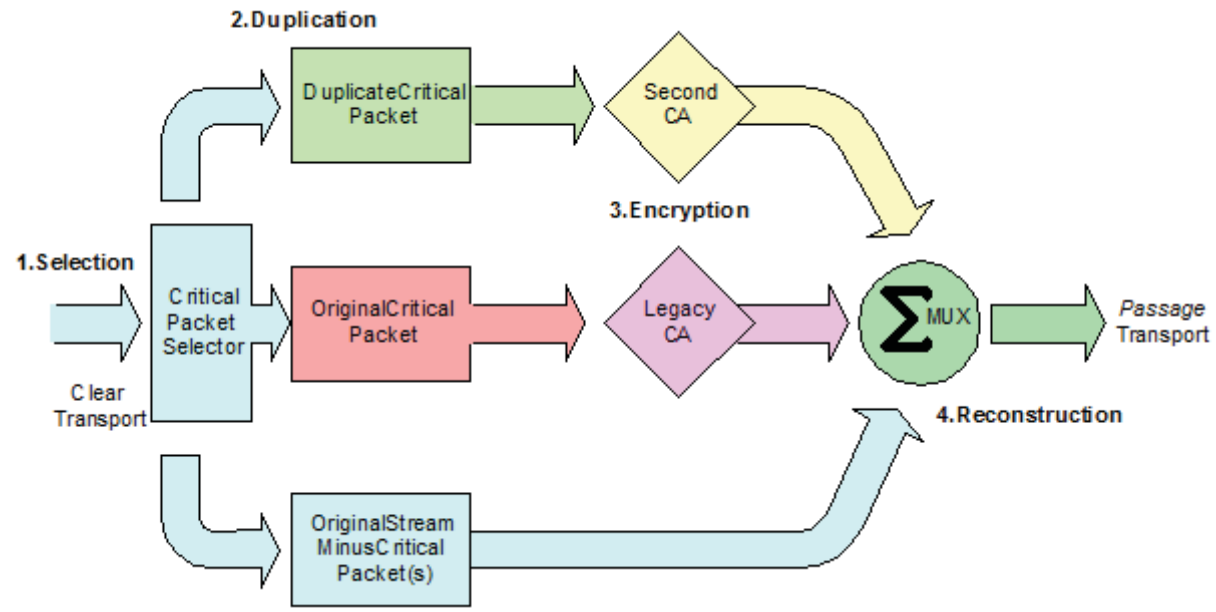


Figure 35 – The Headend Encoding Process - 4 Steps - Selection, Duplication, Encryption and Reconstruction

Managing Bandwidth

Passage recognizes that content might be treated differently based on the value of the content. With this in mind, Passage is designed to allow the Multi-channel Video Program Distributor (MVPD) to adjust the level of encryption on a per-channel and program-by-program basis. Passage allows the operator control over packet encryption. The algorithms designed by Sony that choose critical data are hierarchical and progressive and can be changed at any time. In addition, the modes used on each program in a transport stream are completely independent of one another.

Thus a MVPD has the option of trading bandwidth for increasing degrees of robustness. The lowest level of Passage encryption provides protection against decoding by commercially available MPEG decoding

devices. This mode carries the lowest bandwidth overhead, on the order of .2 percent. It is typically used on content such as syndicated programs.

More robust protection for content with a higher value—such as VOD, live PPV events, premium services, etc.—is provided with higher-level modes of Passage security. These higher-level modes carry a larger bandwidth overhead; to a practical maximum of 2 percent for combined audio/video (see Figure 36). No significant increase in robustness is gained when increasing the total Passage replicated packet bandwidth beyond 2 percent.

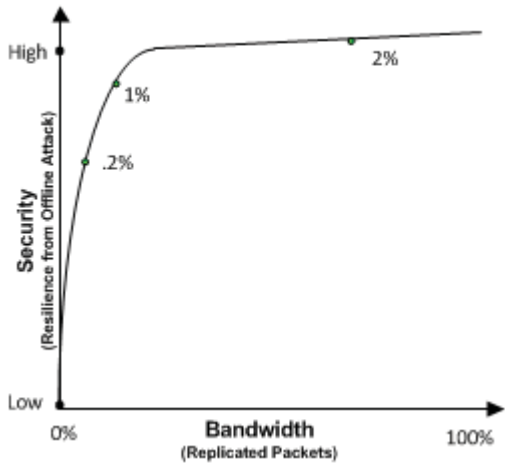


Figure 36 – *Passage* Bandwidth Usage

Implementations

Passage is proven technology. There have been a number of field and lab trials as well as deployments with the Cisco CA Overlay system. As discussed in the Analysis Section of this report, the preferred approach would be to Passage Encode content at the point of commercial distribution – prior to reception by the MVPDs.

Security

While not a security system in and of itself, Passage use of selective encryption is approved by Merdan Associates and Sarnoff Laboratories. Reports are available under NDA from Sony Electronics.

Protocols

Passage utilizes the DVB Simulcrypt standard to standardize interfaces at the broadcast center as well as the signaling the security system in in-band stream. Additional messaging is required to signal the alternate video and audio packets in a program. This is described in the "Passage Set-top Box Specification", available from Sony Electronics. Also see the "Passage Decoder IC specification" and "Passage Test Streams specification", available from Sony Electronics.

See also references [5], [6], [7], [8] and [9].

Part III: Alternative Systems that Enable New Categories of Navigation Devices

The DSTAC WG4 has documented two systems for implementing a software-based downloadable security system. Proposal 1: "*Competitive Navigation*", was authored by multiple DSTAC participants including Hauppauge and Google, and Proposal 2: "*Application-Based Service with Operator Provided User-Interface*" was authored by multiple DSTAC participants including Cablevision, Comcast, DISH, AT&T, Charter and MPAA. Following the systems are analyses authored by DSTAC members.

Section I: "*Competitive Navigation*" System

To support the operation of commercial competitive devices to receive all MVPD content on all MVPD systems, as required by Section 629[12] and as a congressionally directed task,[13] DCAS solutions as discussed in WG reports[14] should abstract the differences in MVPD network technology into a common interoperable format. In an IP environment this is technically evolved, but conceptually similar to the common, secure DFAST interface solution employed in the CableCARD solution presently relied upon by both cable MVPD and third party sourced devices. An interoperable architecture implementing such a system could provide for specific functional APIs plus a generic man/machine interface (MMI) that allows devices to communicate through these defined APIs to interact with the DCAS, communicate upstream and respond through private messaging, while supporting both a competitive UI and that of the MVPD, as selected by the consumer.

Many MVPDs are in the process of migrating to (or simultaneously enabling) IP transmission of content, through either direct Cloud to Ground delivery or an interim gateway solution that converts to IP in the home.[15] As reported to DSTAC Working Groups, this has enabled the use of growing numbers of devices that do not connect directly to or rely on the operator's proprietary network technology. Transitioning to IP technology will continue to entail the reliance on a number of network, encryption, codec, and other technologies, so as to enable diverse choices and implementations, but also make the use of a single, proprietary DCAS solution inconsistent with the operators' present investments. The migration to IP delivery by operators provides the technical opportunity for a common solution that relies on more than a single implementation of DCAS while providing full access to MVPD content and services.

Competitive Navigation Device Executive Summary

To provide consumers with a third party, competitive device which 1) works across disparate MVPD networks and 2) allows the user interface (UI) to differentiate itself from the UI provided by the MVPD, a

[12] 47 U.S.C. § 549(a).

[13] DSTAC Charter, Dec. 5, 2014.

[14] *See* WG1 Report, MVPD Requirements, Device Manufacturer Requirements; WG2 Report, Part III [45]; WG3 Report [descriptions of downloadable CAS systems].

[15] [Comcast's] Viper can handle all of Comcast's multi-screen needs today but it can also be leveraged as the company's all-IP platform whenever Comcast is ready to cut over.
http://www.cedmagazine.com/articles/2014/03/comcast-uncoiling-viper-across-video-services

well-defined set of protocols and APIs between the MVPD system and the consumer device is needed. This proposal for a competitive UI uses existing standards for these protocols and APIs, chosen so the competitive UI can interoperate across all MVPDs in the U.S. Some of the proposed protocols and APIs are derived from CableCARD specifications, and some are based on cable TV, broadcast TV or Internet APIs and protocols.

This proposal gives consumers the same choices in television viewing devices that they enjoy today, and expands that choice in experience beyond cable to other video service providers. The consumer devices and technologies proposed in this section are conceptually similar to current consumer devices based on CableCARD in that they receive TV content on one end, decrypt the TV content using the secure technology (described by DSTAC Working Group 3), re-encrypt using an approved encryption scheme as described by WG3 and then pass the encrypted data to the application which is creating the competitive UI for recording or output through an HDMI port or a home network to other consumer devices.

To support this competitive UI, we describe three main interfaces inside the device: a Service Discovery Interface, an Entitlement Information Interface and a Content Delivery Interface.

Service Discovery Interface: This interface provides the necessary information for the competitive navigation device to discover and display the content services delivered by the MVPD headend and provided to the subscriber. This includes the following functions:

- Lists of available services
- Metadata about those services
- Messaging from the MVPD

The Service Discovery Interface described in this document provides a common platform for publishing, accessing, and searching metadata sources. In addition, an MVPD interactive “widget” is required for service provider data and device information to be relayed to the end user, along with providing a way to supply interactive widgets. Currently CableCARD provides a Man Machine Interface (MMI) which is used to provide simple widgets for consumer devices. This proposal expands on the CableCARD MMI interface to provide a bi-directional set of APIs based on HTML for MVPDs to send and receive information from the competitive third party device. This provides a secure method for the MVPD’s to retain control over part of the user interface and support functions such as Pay Per View, Service changes, Billing and MVPD Upsell programs.

Entitlement Information Interface: This interface provides information on the entitlement status of the services described in the Service Discovery Interface. It defines a common platform for publishing, communicating, sharing and transferring rights information. A consumer device can be identified through use of a standardized security certificate before obtaining rights information.

Content Delivery Interface: This secure, protected, interface delivers Live, Linear, VOD, and network DVR content streams. It defines baseline requirements of the content formats (e.g. MPEG4), container formats (e.g. MPEG2) and stream protocols (e.g. HLS) to ensure interoperability between the MVPD

system and the competitive device. This Interface also defines the content protection mechanism, and secure transfer of metadata such as entitlement and copy control information. Suitable content protection formats would be DTCP-IP or or another similarly approved secure digital ouptut.. The DCAS system should terminate MVPD CAS/DRM (digital rights management) and translate the content into a protected, interoperable format. This is how the CableCARD DFAST currently operates. CableCARD DFAST shows that converting various network encryption technologies into a single common format works with varying CA systems throughout the country, across all cable MVPD's. Using this transcryption approach, legacy systems do not require replacement in field, the DCAS and Provider Interfaces transcryption operation handles this. Replacing legacy devices was a concern stated by multiple MVPD's, so this approach would allow for the easiest transition and could apply to newly deployed devices.

Diversity in Direct Connection Delivery Networks

As is documented in the DSTAC WG2 [45] report and in this WG4 report, there is a wide diversity in delivery networks, conditional access systems, bi-directional communication paths, and other technology choices across MVPDs.[16] It should not be necessary to disturb the potentially multiple present and future CA/DRM system choices made by cable, DBS and IPTV systems, which leave in place several proprietary systems for delivering digital video programming and services across MVPDs. Unless all MVPDs replace these proprietary CA systems with some common and interoperable means of termination, only such devices as are designed for these proprietary systems and authorized by the specific MVPD can connect directly to the MVPD network to achieve full access. The only example in the DSTAC record of an architecture through which comparable access to all cable MVPD programming can be accomplished is that of CableCARD, which provides for diverse and upgradable or downloadable point to point security but which also incorporates a common security termination and third party user interfaces. The deficiencies of the CableCARD system are also well documented:

- It enables access only to cable systems.
- As licensed for third party use, it is forbidden to employ upstream signaling or provide access to the operator's UI.
- As employed in operator-leased devices it provides separability that is rarely employed.
- It was designed for cable architectures and infrastructure.

The DSTAC task is to recommend solutions that improve rather than recapitulate or degrade the existing environment, in light of the deficiencies and coming changes to the CableCARD environment.[17] It would

---

16 WG2 Report Part III.

17 The STELA Reauthorization Act of 2014, which directed the FCC to establish DSTAC, effectively allows cable operators to terminate their reliance on CableCARDs in leased devices in December of 2015. Commission policy has been based on a conclusion that such common reliance will "align MVPDs' incentives with those of other industry participants so that MVPDs will plan the development of their services and technical standards to incorporate devices that can be independently manufactured, sold, and improved upon" and make it "far more likely that [MVPDs] will continue to support and take into account the need to support services that will work with independently supplied and purchased equipment." Implementation of Section 304 of the Telecommunications

not be a step forward or economically viable to require an environment in which, to offer access comparable to that of MVPD-sourced devices across all MVPD programs and services a competitive manufacturer would have to equip a device with RF tuners for cable and satellite, varied semiconductor platforms to support the dozen-plus proprietary CAS technologies that may be used,[18] and IP connections for IPTV implementation, and provide for all associated application and field testing. Nor is it reasonable to expect that all operators will radically re-architect their networks, and converge on a common solution for all direct connection, in order to avoid the obstacles to competitive solutions, therefore an approach in which MVPD CAS is terminated and transcrypted to a common output format is required to be least cumbersome on all parties.

Migration to IP Delivery Underway

Some MVPDs are putting significant effort and resources into defining IP protocols and working with standards bodies and consortia such as DLNA, as well as testing/interoperability facilities such as CableLabs[19]. Many MVPDs have been actively working on protocols that support either direct "Cloud to Ground" delivery, or interim gateway solutions that convert to IP in the home.[20] Under the Cloud to Ground model an operator terminates its proprietary network so as to interface with the user's home network over IP. Such termination devices are often called data gateways, or simply "gateways." Examples include DOCSIS modems on Cable plants and DSL modems or Optical Network Terminals (ONT) on Telco and Fiber IPTV systems. The MVPD's services are then made available over the IP home network using standards-based protocols to various consumer devices. The consumer devices do not need to implement any network-specific technology such as physical tuners.

In an interim gateway model, the MVPD provided direct-connect termination device converts video services to IP in the user's home instead of upstream in the MVPD's network. For example, VidiPath and RVU servers can translate a variety of access technologies into common IP protocols. Cable and DBS operators have demonstrated and fielded RUI technologies through gateway devices as solutions that provide content services to non direct-attached devices, such as SmartTVs and tablets. These devices all use IP protocols over home networks to provide content and information to other devices in homes. Many MVPDs already have equipment in consumers' homes that may theoretically be convertible to an interim gateway by enabling the Ethernet interface already on the device.

Act of 1996; Commercial Availability of Navigation Devices, 20 FCC Rcd 6794, 6802-03, ¶ 13 (2005) ("2005 Deferral Order"), pet. for review denied, Charter Communications, Inc. v. FCC, 460 F.3d 31 (D.C. Cir. 2006), as cited in MO&O, Colorado Tel. Co. *et al*, July 23, 2007, par. 3 and n. 17.

[18] [WG3 cite]

[19] The VidiPath Interoperability lab provides an opportunity for VidiPath Client manufacturers to develop, test, and capture pre-certification videos while interoperating with VidiPath servers from major MSOs. http://www.cablelabs.com/resources/development-lab/

[20] Comcast's Cloud-Based UI Makeover, http://www.lightreading.com/cable/cables-cloud-based-ui-makeover/a/d-id/716978

Limitations of Architectures Thus Far

A migration to IP enables an interoperable architecture in which MVPD CA systems terminate in ways that can support competitive devices across MVPD service categories, as well as over diverse CAS implementations within categories. Such architecture can support product innovation and differentiation, which can be competitively decisive.[21] However, solutions such as VidiPath and RVU appear to have been deliberately designed to not allow a fully independent user experience on competitive devices. There are no apparent specifications that describe how another device can obtain all the necessary information needed to create a competitive user experience. Rather, they are aimed at "consistency" of a single MVPD user experience across various devices.

The current approach to monolithic presentation of an MVPD's user interface through a remote UI technology like RVU and VidiPath can be supplemented or extended so as to also allow an independent (not controlled by the MVPD) client-side user interface to access the audio and video content and micro-services presented in an MVPD's user interface. For example DirecTV already extends RVU to allow client control over the server through a RESTful approach, called the SHEF protocol. With SHEF, a client application or user interface can launch RVU and tune to a channel, a feature that DirecTV enables via an HTTP server embedded and tied to the RVU server. And, being based on http protocol, this approach can be extended to cloud solutions also. Additional extensions would be required to support a full competitive navigation system however. Similarly, VidiPath, which may have a different combination of LAN and cloud delivery of content and services, could be extended to enable independent client user interfaces using a RESTful approach. With VidiPath, the HTTP server may be located in the cloud or on the home network but either way should provide to the client a method to browse, select and launch the content items or micro-services provided by an MVPD through VidiPath. Unlike RVU, which is primarily a push technology, the VidiPath client often pulls content from the server. In this case, the HTTP server may be supplying a URL extension (like a query parameter) that the VidiPath client then uses to pull content or micro-service. A local application or user interface can then launch its VidiPath client with the extended URL information without navigating through the monolithic guide. And, since VidiPath mandates support for HTML5 push technologies like Dynamic HTML, AJAX, Web Sockets and Server Sent Events, an MVPD may choose an approach more closely resembling how SHEF works with RVU. Separating the control and data planes as in these examples of extensions to current MVPD efforts so as to support a competitive UI would be necessary to support third-party implementations. Some problems currently preventing VidiPath, HTML5 EME and RVU from being suitable interface protocols for an independent third party to utilize are detailed here:

[21] *See, e.g.,* Slade Kobran, *How To Differentiate Yourself When You're Not That Different*, http://www.chiefoutsiders.com/blog/bid/99344/How-To-Differentiate-Yourself-When-You-re-Not-that-Different ("Apple's … focus on both the physical appearance of its devices and their user interfaces have turned Steve Jobs' passion for design and simplicity into the most valuable company in the world.")

- VidiPath uses an array of protocols with which a third party client device may communicate with the server. However, VidiPath as currently defined does not meet the requirements to enable competitive navigation devices. In particular VidiPath:
  - Does not allow for discoverability of the video services such as linear channels, VOD and PPV
  - Does not allow for an independent user interface to access most content directly, such as VOD, PPV, and network DVR - all content is available exclusively through the MVPD's VidiPath RUI
  - Does not allow independent clients to record streams
  - Does not allow independent clients to navigate to and schedule a recording
  - Does not provide independent clients details on entitlements for video services

- RVU offers similar functionality to VidiPath, but supports different operational interfaces. However it shares some of the same limitations that do not allow for a competitive third party user interface that can directly access content.
  - The RVU protocol's utility for supporting third party devices is limited by a requirement to licensing guide data to interoperate with current devices, and an inability to record through the user interface.
  - It does not provide standard APIs for an independent application to obtain the list of available services and available assets
  - It does not allow an independent application to record live content

- HTML5 EME, MSE and WEBCRYPTO define a set of protocols that enable a HTML5 application to access embedded browser security elements to enable downloadable security. However they are not sufficient to enable a competitive navigation user experience on the client device.
  - Only monolithic applications from the MVPD that integrate both user experience and security are currently supported. There are no interfaces that allow competitive user interface applications to access the same security APIs as the MVPD's proprietary application.
  - There is no clear definition of what requirements are mandatory in the browser to support a MVPD's given choice of downloadable security. For example currently each popular browser supports only one DRM under EME. Unless each MVPD offers support for every DRM, a retail device can't be guaranteed access.

Limitations Where User Experience Is Too Closely Controlled

Common interfaces and defined protocols, as implemented through CableCARDs, are necessary but not sufficient to support and sustain competition by third party devices. In case of the OCAP [23] (aka "tru2way") architecture, allowing upstream communication through a CableCARD was conditioned on business requirements antithetical to a competitive experience. The architecture required that the MVPD control all software related to two-way cable services, forestalling any ability for a third party device to offer its own UI to access two-way services. Moreover, manufacturers were unable to assure that MVPD-deployed software would operate as predicted. Such outcomes are not inevitable. Defined protocols between layered components have successfully enabled innovation in devices and networks. They are foundational to the Internet and have been highly successful at bringing services and devices to

market rapidly. The use of protocols can minimize requirements for network and device interoperability, and does not impose requirements on internal implementation of the devices themselves to support the protocols. Such architectures avoid the necessity to mandate and test detailed, internal operations of individual MVPD systems.

Hence this proposal focuses on interfaces for an interoperable architecture, and defined protocols that enable full innovation of the consumer experience. This section outlines such an architecture.

Interfaces Necessary to Enable Competitive Interoperability

To enable competitive navigation devices and user experiences, an architecture should provide

1. information on video services available to the consumer and devices
2. access to content over a common network interface
3. entitlement and usage rights information of the available services

We call these the **Service Discovery Interface**, the **Content Delivery Interface**, and the **Entitlement Information Interface**. These **Provider Interfaces** would be offered by each MVPD in a common defined standard, but the DCAS and other elements that the MVPD chooses to implement them are left up to the MVPD to allow for continued innovation and diversity in implementations.

Each Provider Interface can be defined in a set of interfaces with defined protocols and formats. Standard Internet protocols would be used, all built on top of TCP/IP and HTTP. The formats would use standards such as XML for data exchange, HTML for graphics, common codecs for audio and video content such as MPEG-4, etc. These protocols and formats are common to most networked consumer devices today. This proposal defines required functional interfaces and outlines various similar technologies that exist, but recognizes current standards cannot be used directly without evolving in some cases.

Service Discovery Interface

This interface provides the necessary information for the competitive navigation device to discover and display the content services delivered by the MVPD headend and provided to the subscriber. A common protocol across MVPDs allows competitive devices to work across MVPDs. For example in the CableCARD architecture, service information is delivered in text tables defined in a SCTE specification.[22] The navigation device can then display this service and content information in any chosen format such as a grid guide, series of recommendations, or a visual mosaic. The interface provides the list of services, and sufficient metadata to uniquely identify the content in each video service to the user.

Content Delivery Interface

[22] ANSI/SCTE 65 2008 “SERVICE INFORMATION DELIVERED OUT-OF-BAND FOR DIGITAL CABLE TELEVISION”

As noted in the WG2 report [45], MVPD content formats and CA/DRM systems vary. In this interface the provider implementation and DCAS components terminate the network CA/DRM and translate them into a finite set of defined, interoperable formats. Both CableCARD and DLNA systems define such interfaces today. For example by defining a finite set of defined formats, DLNA and CableCARD frameworks ensure portability across MVPDs and across content service types. Note that content here described also includes optional and mandatory ancillary streams such as multiple audio tracks and closed caption data.

Entitlement Information Interface

This interface provides the competitive navigation device information on the entitlement status of the services described in the service discovery interface. For example in the CableCARD system, the ca_pmt() Application Protocol Data Unit provides information on whether the device is authorized for a particular service. Entitlement implies some form of authentication of the device and/or user by the DSS.

Each of the interfaces is described in more detail in the following sections.

The following diagram, based on the one in WG3's report, illustrates the interfaces that are provided from the provider to consumer devices. The interfaces are labeled Interface C, D and E in the diagram.

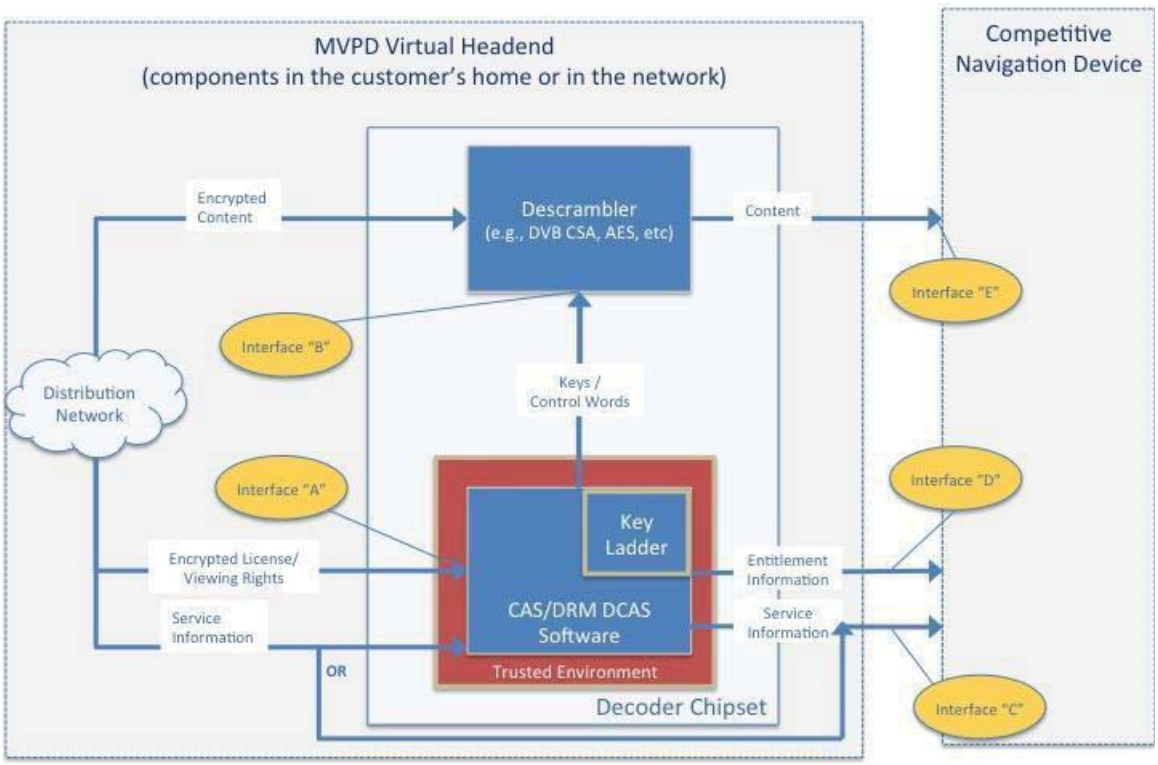


Figure 37 - Interfaces

Physical Interconnection and Basic Networking

The Provider Interfaces shall be implemented by the MVPD using open standards. The physical interconnection standards for home networks are grouped under the IEEE standard 802[23]. The standards specifically involved with wired Ethernet fall under the 802.3 subheading.

Standards for the software layers of home networking are promulgated by the Internet Engineering Task Force (IETF[24]) through the RFC (Request For Comment) mechanism. For instance, RFC 1122[25] describes the basic TCP/IP protocols that universally underlie the Internet. A large number of open-source implementations of these protocols are available. HTTP, the foundation for web browsing is standardized as RFC 2616[26], which is carried by TCP/IP. In the simplest home networks, RFC 3927[27] is used to automatically configure the gateway and third-party devices on the home network. More

[23] http://standards.ieee.org/getieee802
[24] http://www.ietf.org
[25] http://tools.ietf.org/html/rfc1122 - **Requirements for Internet Hosts -- Communication Layers**
[26] http://tools.ietf.org/html/rfc2616 - Hypertext Transfer Protocol -- HTTP 1.1
[27] https://tools.ietf.org/html/rfc3927 - Dynamic Configuration of IPv4 Link-Local Addresses

sophisticated consumers may have DHCP (Dynamic Host Configuration Protocol) servers on their network (for instance, in a wireless router) which configures the network, as described in RFC 2131[28].

Service Discovery Interface

This interface provides the necessary information for the competitive navigation device to discover and display the content services delivered by the MVPD headend and provided to the subscriber. This includes the following functions:

- Lists of available video services
- Metadata about those services
- Messaging from the MVPD relating to these services

The two required operations of the basic Service Discovery Interface implementation are: interface detection/advertisement, which allows an Interface to announce its presence to consumer devices on the home network; and service browsing, in which a consumer device can browse and access the available services and metadata from the MVPD.

Interface Detection

It is important that consumer devices be able to automatically detect the Provider Interfaces on the home network, as well as automatically discovering what services are available. A gateway device typically advertises the services it makes available on the local network via an Internet standard suite of protocols called Zeroconf[29], such as Avahi[30]. The Provider Interface can present certain defined URLs across MVPDs that support the interfaces described here, with the IP address of the URL described in the service announcement. This could be supported in both the gateway and cloud to ground model implementations of the Provider Interfaces. In the case of bidirectional systems, because the Interfaces are provided on the MVPD's managed network, the MVPD can ensure that the interfaces are only visible to their customers.

Service Types

While many different services are possible over time and can be added by extensions to the interface protocol, this proposal envisions two basic services: linear broadcast/multicast video (i.e., digital television), and unicast video-on-demand. In each case, the metadata describing available video services would be accessed from an MVPD source directly by a consumer device using standard protocols. In addition to discovery of linear services, available PPV and VOD services should be accessible via the same format."Pay Per View" content availability transitions require higher precision and frequency, but content could be otherwise transported similarly to channel-based content. Both PPV and VOD purchases will require some sort of audit trail. While phone/web/online purchase is a historically preferred option for some MVPD subscribers, an MVPD supplied MMI widget could execute

[28] http://www.ietf.org/rfc/rfc2131.txt - DHCP
[29] http://www.avahi.org/
[30] http://www.zeroconf.org/

interactive bidirectional communication with the end user while keeping the user interface unified. The MMI support widget is described at the end of this section.

Video content catalogs must be canonicalized for discovery via browsing, searching, and other possible navigation mechanisms. Protocol-based approaches to this include, but are not limited to, Project Open Data[31] (POD), Data Catalog Interoperability Protocol[32] (DCIP), and XML.

Service browsing could be performed using an HTTP GET on a given URL, which returns an XML[33] (eXtensible Markup Language) document formatted according to the conventions of RSS 2.0[34] (Really Simple Syndication). Each content item is described using the format defined for the RSS 2.0 Media Module[35]. This allows normal Web browsers to fetch the list, and aids in debugging and identifying problems. The RSS protocol is widely used on the Internet to provide just this kind of information (iTunes for example), and is supported by almost all Web browsers, as well as a large number of specialized applications.

Service Information Metadata

There is no requirement today that cable MVPD's provide additional metadata about service information over CableCARD outside of channel identifiers and call sign[36]. Data about linear content that may be available in the future (i.e., program guide information) is not provided, although it is part of the CableCARD service information specification (SCTE 65 service information profiles 4-6).

To assure the accuracy of the presentation of programming data on competitive navigation devices, we recommend the requirement of in-band or common-medium delivery of, at a minimum, basic identifying programming data for all content types. This data could be optionally augmented on competitive navigation devices, and it must be sufficient for effective user navigation when secondary internet connectivity is not available. Basic metadata allows a device to still be navigable in one way mode or in cases without network connectivity.

[31] https://project-open-data.cio.gov/
[32] http://spec.dataportals.org/
[33] http://en.wikipedia.org/wiki/XML
[34] http://www.rssboard.org/rss-specification
[35] http://video.search.yahoo.com/mrss
[36] December 12, 2002 Memorandum of Understanding Among Cable MSOs and Consumer Electronics Manufacturers

Basic (Mandatory) Metadata includes:

- Channel identifier and call signs
- Show title and episode title
- Parental control information
- Start time and program length
- EIDR ID[37] for rich metadata retrieval

The ability for a service provider to provide enhanced metadata, such as descriptions, actors, and graphics, must be an optional part of the delivery mechanism. An MVPD may choose to provide enhanced metadata as a differentiator for their service. While linear channels should carry at least a week of basic metadata in order to allow for scheduling, enhanced metadata must be provided for all VoD and PPV assets to describe in detail what is available on a dynamic schedule. Manufacturers can externally license guide and metadata to provide enhanced information based on knowing a linear program's title and episode number or EIDR ID.

Currently there are two standards available for use by MVPDs for service information metadata delivery, SCTE65 binary tables and CEA-2033[38] xml data. SCTE65 service information profiles use a layered approach to associate 'event' program ID's with channel source ID's. Each layer expands on the previous to provide additional level of metadata. Service information profiles 4-6 relay program metadata associated with a channel such as start times and length, show title, episode title, and show description. ATSC[39] and DVB[40] compliant systems both use similar service information tables to provide up to two weeks of detailed metadata, including episode descriptions. CEA-2033 is a much expanded and detailed metadata system, containing all service metadata in one blob. Due to the nature of XML, each node can be expanded to provide additional child nodes with service information, without modifying the protocol. To satisfy MVPD evolution of service information metadata offerings, an XML based approach similar to CEA-2033 might be the most extensible solution for the future. Any chosen solution should carry at least the minimum required basic metadata described above.

Support Messaging / Man machine interface (MMI)

Upstream communication and the ability to run MVPD unique 'apps' has been one of the contested areas of DSTAC. For example if an MVPD has a unique promotional offering (up-sell, weekend special deal, etc) that isn't defined in a standard Entitlement Interface, an interactive "widget" may be required. Suggested here is a rich bi-directional interface to allow for service provider data and device information to be relayed to the end user, along with providing a way to supply interactive widgets.

[37] http://eidr.org - Entertainment Identifier Register

[38] CEA-2033 - OpenEPG: A Specification for Electronic Program Guide Data Interchange

[39] ATSC A/65:2013 - Program and System Information Protocol for Terrestrial Broadcast and Cable

[40] ETSI EN 300 468 v1.4.1 - Digital Video Broadcasting; Specification for Service Information in DVB Systems

Currently CableCARD provides a Man Machine Interface (MMI), implemented by the MVPD. The CableCARD MMI currently provides the following service:

- Status/information pages
- CCI information associated with a program being decoded
- Service information
- Notifications about program entitlements
- Notifications about device authentication issues

Proposed here is expanding the same MMI model to be far more robust. An expanded MMI with bidirectional capabilities would be able to handle:

- HTML5 widgets to facilitate MVPD-unique consumer interactions
  - support for javascript
- Display of widgets must be conditionally optional, based on user input, regulatory requirements, and user actions
  - For example, mandatory EAS messaging
- Allows for single API to interact with the DCAS and Provider Interface components
- DCAS can communicate privately to an MVPD component and respond
- Suitable for all communication with MVPD network "back office" components
- Billing, Upselling, and other unique entitlement interactions supported

The CableCARD MMI currently only supports a baseline HTML profile, which is its main limitation when being used as a widget interface. Widget requirements would need analysis to determine the level of HTML that the MMI should support. Hyperlinks inside an expanded MMI widget could support targets on the greater internet to communicate directly with an MVD web service. Once defined, MVPD's could implement any bi-directional services desired that are supported by the protocol. This provides a secure method for the MVPD's to retain control over part of the user interface, while allowing for competitive user interfaces to flourish. The MMI widget interface is not proposed or designed to replace an entire UI, but to allow some interactive MVPD features to be available through an independent third party UI. Features that would be suitable for such an MMI widget interface could be:

- Caller ID
- Sports statistics
- News ticker

Entitlement Information Interface

This interface provides the competitive navigation device information on the entitlement status of the services described in the service discovery interface. It defines a common platform for publishing, communicating, sharing and transferring rights information.

Entitlement implies some form of authentication of the device and/or user and/or household by the Provider Interface. If the MVPD chooses to require that a consumer device be authenticated with the Provider Interface before providing services, a consumer device can be identified through a standard

X.509 security certificate. This certificate would be issued by a common trusted authority, to prevent requiring individual certificates for every MVPD DFAST currently operates similarly, where one single certificate issued by a trusted authority allows a host to authenticate and then communicate securely with the CableCARD.

The following scenario is an example of how a consumer device would obtain a certificate for communication with the gateway:

- Each unique consumer device type has a certification number obtained after meeting compliance requirements which is included on the device label, as well as a unique, per-device, serial number.
  - Compliance and testing regimes to be determined with industry feedback.
- The consumer browses to the MVPD certification site using their device, said site providing a simple HTML-only page for device authentication.
- After validating the consumer service level and certification number, the MVPD generates a certificate for the consumer device, which is then downloaded to the device where it is stored in an appropriate local certificate store.
  - Unidirectional systems would require obtaining the authentication certificate offline and sideloading it into the system.
- The consumer device certificate would have a reasonably short expiration such as one month. The consumer device would be responsible for requesting a new certificate some time before the current one expires. This should be an automatic operation, whereby the device contacts a standard MVPD URL, and the server responds with a new certificate if the consumer is still a proper subscriber to the MVPD service. The renewal URL is contained within an extension field in the certificate.

The certificate that the competitive navigation device must present to the Provider Interface is described in RFC 5280. A good overview of these certificates and what they contain is described on wikipedia[41] . The certificate shall be represented in DER format according to the ITU-T X.690 standard[42]. The MVPD Interface only needs to verify that the certificate is valid, and signed by the appropriate certificate authority. It is not desirable, nor possible, for this proposal to specify the exact procedures or systems that an MVPD would use to manage certificate administration duties including certificate revocation. It is expected that each MVPD will have unique operational requirements and needs.

An implementation of X.509 certificate handling that is in broad use today is the open source OpenSSL [62] implementation. An MVPD might choose to delegate certificate provisioning to a third-party certificate authority (CA) such as Verisign.

Content Delivery Interface

This interface delivers content to IP connected devices. It provides individual stream access for Live, Linear, VOD, and network DVR content streams. It defines baseline requirements of the content formats

[41] http://en.wikipedia.org/wiki/X.509

[42] http://www.itu.int/ITU-T/studygroups/com17/languages/X.690-0207.pdf

(e.g. MPEG4), container formats (e.g. MPEG2) and stream protocols (e.g. HLS) to ensure interoperability between the Provider Interface and the client devices. This Interface also defines the content protection mechanism, and secure transfer of metadata such as entitlement and copy control information. As an example of a content delivery interface, the DLNA media format model defines a set of required and optional media formats for each of the three classes of media: image, audio, and video with audio.

Content Formats and Encoding

A service may provide streams in encodings not included in the basic set above to allow for future formats. Obviously, a consumer device should not attempt to access a stream which it does not know how to decode, and may choose simply to ignore them. Initially, only a small number of content formats is needed, but more could be supported over time.

Container Formats

Media formats would be encapsulated in an MPEG2 Transport Stream (see ISO 13818) delivered over HTTP. Video would be further encapsulated as MPEG2 or H.264 streams, limited to standard resolutions and frame rates to be defined. A standard set of audio formats would also be defined. ATSC and SCTE standards bodies already define such formats and could be used as reference. Compatibility with open and interoperable formats currently in use by MVPDs today should be maintained where possible.

Adaptive streaming formats such as HLS or DASH could also be used. Video-on-demand services may additionally provide support for the RTSP (Real Time Streaming Protocol) RFC 2326[43] . An extension header is returned in the HTTP POST response for a VOD stream giving a URL on the gateway upon which an RTSP session can be established. RTSP commands can then be given to cause the video data being returned from the HTTP POST to pause, or to come from a different place in the program, and so forth.

Stream Protocols

The on-demand services such as video-on-demand and network DVR should additionally support stream control by the competitive user interface. The RTSP (Real-Time Streaming Protocol), HLS or DASH protocols allow a consumer device to provide VCR-like control over the on-demand stream.

Content Protection

As noted in the WG2 report [45], MVPD content formats and CA/DRM systems vary. Sixteen different CA schemes were presented, making interoperation with all of them a cumbersome task. The proposed DCAS should terminate network CA/DRM and translate into an interoperable format similar to how DFAST currently operates. DFAST is proof that converting various network encryption technologies into a single common format works with varying CA systems throughout the country, across all cable MVPD's. Using this transcryption approach, legacy systems do not require replacement in field, the DCAS and Provider Interfaces transcrypting operation handles this. Replacing legacy devices was a concern stated by multiple MVPD's, so this approach would allow for the easiest transition and could

[43] http://en.wikipedia.org/wiki/Real_Time_Streaming_Protocol

apply to newly deployed devices. Suitable content protection formats would be DTCP-IP, or subsequent versions, for content sourced locally via a gateway. DTCP-IP transfers contains embedded copyright control information receiving clients must abide by, this includes copy count for exporting recordings. In the case of 'cloud to ground' delivery an approved secure digital output format such as Microsoft Playready DRM would allow for interoperation with a wide variety of client devices..

Use Case Analysis

In this section the use cases from Section VII are analyzed with respect to the solution.

Tuning and Viewing a Linear Channel

Viewing linear television is a vital operation required by consumers. Due to the widely differing MVPD architectures and delivery mechanisms, however, it is not straightforward to easily interoperate with all of them. To solve this difficulty the MVPDs DCAS and Provider Interfaces terminate an MVPD's CA/DRM and transcrypt to common output protocols. CableLabs DFAST is an excellent example of technology offering such termination from differing MVPD CAS into one common security interface for third parties to interoperate with. Cable industry already has one protocol, OCUR's DRI, that behaves similar to the proposed Provider Interface. DRI abstracts all hardware details from clients and instead offers operations like TuneChannel and Play, along with supporting trick modes over RTP. DTCP-IP is used as a link protection protocol along with PlayReady DRM.

The Provider Interfaces would harmonize on IP outputs interoperation with third party consumer devices across MVPDs. While some Cable operators would be able to implement the Provider Interfaces directly from "Cloud to ground" as interfaces on their cable modems, some MVPD's due to their architectural complexities or proprietary system issues might require an additional device in the home that Provides the Interfaces for devices on the home network. Giving MVPDs options on how to implement the Provider Interfaces while making them common across MVPDs is a way to reduce complexities on all parties and keep the burden of implementation and licensing concerns minimal to a third party.

In the case of DBS systems, where system complexities dealing with multiple satellites, transponders and dynamically changing content locations a prosthetic serving the Provider Interfaces would provide a canonicalized list of such content assets and deliver them through the common Content Delivery Interface. SAT-IP is an example of such a system used in Europe. US-based DBS systems already provide such gateway devices today delivering RUI with embedded video assets using RVU or a proprietary system based on HTML5. Access to a canonicalized list of assets with associated rights is required to interoperate with both of these gateway technologies and use them as a Provider Interface embodiment, and this content list not a mandatory feature of either technology.

In the case of IPTV providers such as AT&T the DCAS and Provider Interface implementation would provide termination of their proprietary DRM and channel change protocol, and transcryption to a common Content Delivery Interface which is widely interoperable. Due to the IP/QAM based nature of AT&T an additional device should not be required to implement the Provider Interfaces.

Since the DCAS and Provider Interfaces are implemented by each MVPD and knows their systems limitations, they handle any concurrent stream management required by the IPTV network. Upon exhausting of available streams signals can be sent to the consumer using the MMI. The MMI would

support signaling to deliver varying events to consumer devices. This signaling would deliver entitlement information, EAS alerts, and copyright control information.

Linear television is looked at by this proposal as video only. Any ancillary data offerings and overlays should be either delivered through the MMI or embedded in the program as an optional HTML5 widget. Subscription features like caller ID display, sports statistics, et cetera, should use the MMI HTML5 widget interface to reduce the burden of interoperation on the CE company.

Any client device with a decoder can support trick modes internally while obtaining data over IP. Server devices with decoders can also offer trick play to clients as well with DLNA protocols and/or RTSP operations.

Switched digital video is already abstracted away from retail cable set top box offerings using an external tuning resolver which translates various MVPD implementations of SDV into a common protocol. This tuning resolver is provided by the MVPD and runs internal software to convert the different protocols of their own network into a common one. Communication with the tuning resolver by a client device is handled using a binary protocol over USB to obtain tuning instructions. Tuning resolvers require upstream communication with the headend, therefore they contain DOCSIS modems which must be provisioned by the MVPD. Third party devices should not be required to include a DOCSIS modem to support SDV. Tuning resolvers should continue to be external devices with defined protocols or MVPD's must accept upstream communication originating from the general internet and agree upon a unified cloud tuning resolver protocol. Because all of the Provider Interfaces are bi-directional communication protocols using IP, no DOCSIS modem or other MVPD-specific network technology is required. A unified and interoperable cloud tuning resolving protocol is the ideal software only solution for third parties.

MVPDs can continue to support advertising features such as ad replacement by implementing them within the DCAS and Provider Interface. The client end device receives a stream on the Content Delivery Interface with the MVPD selected advertising already inserted into the stream. The proposed solution places no restrictions on the evolution of ad insertion by the MVPDs. All requirements for acceptable advertising, ad boundaries, ad lifecycle management, audience measurement, ad measurement and reporting are supported because they are implemented by the MVPD in their DCAS and Provider Interface implementation.

To support required operations like geo-filtering and geo-fencing, detailed metadata must be provided by the MVPD along with sources of alternate content to display in place. Messaging about entitlement rights and unauthorized channel redirection instructions should be signaled from the MMI to the client upon access. The client device abides by all copyright controls and output restrictions as part of the DTCP-IP protocol. Parental control can continue to be handled by presentation clients to satisfy legal requirements (See "USE CASE #1 - Tuning and Viewing a Linear Channel"). Captions should continue to be embedded in-stream or attached in the media container to assure synchronization and compliance with appropriate rules and regulations (47 C.F.R. § 79.1 and 47 C.F.R. § 79.4).

Blackouts are replacement/unavailability of channel content specific to Television Market Areas (FCC TMA's) and/or Designated Market Areas (Nielsen DMA's) based on operator contract. Enforcing blackouts is a Provider Interface operation and should be part of service discovery. The MVPD has an obligation to provide metadata for service discovery, this metadata should indicate a service is unavailable or provide alternate sources of appropriate information. During blackout events the MVPDs

DCAS and other systems determines if a service is currently unavailable or replaced in the user's market and via the service discovery interface indicates either to the receiving devices. Both Dish and DirectTV for example currently distribute gateway modules that already enforce these functions when providing content to 3rd party devices.

On-Demand Content

On-Demand content catalogs contain lists of content assets, sometimes grouped by the MVPD or content provider into categories. The Service Discovery Interface from the MVPD should at a minimum provide:

1. a list of all titles available to the user
2. metadata on the titles including pricing information
3. a way to search the metadata across the on-demand catalog.

The MVPD may also include the category information which the competitive navigation device may integrate into its unique user interface.

Some On-Demand services require confirmation of request for purchase. An HTML5 widget delivered though the proposed MMI could support access to dynamic on-demand content. The bi-directional communication with the MVPD could support transaction, subscription and free VOD. Since communication would be directly with the MVPD an audit trail would be ensured. Features like Start Over, and Look Back could be offered through the same widget. If VOD content is delivered as a playlist pre-roll advertising could be inserted fluidly.

Pay Per View (PPV) events

PPV also requires verification of user intent to purchase. An HTML5 widget delivered through the bi-directional MMI would allow for secure communication directly with the MVPD and could allow free preview, purchase and cancellation windows, secure purchase credits and purchase limits. The Service Discovery Interface would provide all required metadata on content available in the PPV service to present to the user in the competitive user interface and enable the user to make a purchase decision.

Navigation

A competitive user interface is how third parties differentiate themselves today in the market place. Offering a unique experience allows consumers choice in difference of presentation of content. This proposal utilizes common defined protocols in the Provider Interfaces to communicate between the MVPDs network and competitive navigation devices. These protocols separate data and control planes, enabling an independent user interface. The data plane is described previously as the Service Discover Interface, Content Delivery Interface, and Entitlement Information Interface. The control plane is where navigation occurs and is orthogonal to security. A device would securely communicate with the data plane, and then using its own choice of user interface technology present the list of content to a consumer. There are currently no limitations on UI technology in CableCARD today and this outlet of innovation must continue to exist as an option for independent third parties.

Devices should be allowed, dependent on copy control information, to securely record, copy and transfer this content using approved digital outputs, no less than what CableLabs today allows through CableCARD. The protocols CableCARD today offers allows PC applications to display content over the network securely using DTCP-IP, while using a native app on the PC. The protocols abstract any network-specific technology to a common protocol and the application deals with the data plane however it

requires. Tablet apps can be similarly implemented. Hauppauge[44] displayed an IPAD app during a WG2 presentation that utilized DLNA for discovery, DRI for tuner statistics, DTCP-IP for link protection during delivery, along with a grid guide for navigation. Protocol based approaches lead the most flexibility and implementation options for CE companies to innovate leading to unique features and devices.

Recording Linear Content

Recording content is a vital competitive navigation device feature that must continue to be allowed, if a device manufacturer desires to include content storage such as a hard drive and where content rights information permits. Hard drives should not be a requirement for recording implementations though, cloud recording innovations allow for local and network DVR's. Recording to portable and/or RUI clients could be accomplished by transcryption on the client device; currently in the CableCARD regime CableLabs approves transcryption of DTCP-IP to Microsoft PlayReady for example.

Portable devices like tablets, phones, and laptops are an important part of an end users experience, therefore recordings must be exportable to secure clients, either as copies from local storage in a recording device or transfers of the recording. Microsoft Playready is a suggested DRM, where copyright controls indicate protection is required, and allows for playback on most common portable devices today.

Ninety minute timeshift/pause buffers shall continue to be allowed and minimally restricted for normal use cases. Additionally, Copy Control information for a program, such as COPY NEVER, should not restrict the ability to use a timeshift/pause buffer.

Remote Management by Consumer

By definition competitive navigation devices have their own differentiated remote management systems. Managing MVPD related account settings could be proxied through to an MVPD's web service on their customer website.

Set-Top Box set-up

By definition competitive navigation devices have their own differentiated set-up and configuration wizards. These handle preferences, device settings, parental controls and accessibility.

Customer Support and Remote Management by Service Provider

The MMI allows the service provider to troubleshoot service delivery by messaging to the user if communication is required.

Cloud Delivery

The source of content material does not matter when obtaining an asset list from the Service Discover Interface. Material that originates in the cloud would be canonicalized and could be displayed through a client devices RUI. Cloud delivery requires that an agreed upon protection scheme for cloud assets is employed, such that the widest amount of interoperation is available. Microsoft PlayReady is already deployed in many cloud to ground scenarios and is widely interoperable.

[44] Brad Love presented for WG1 <FC docket #>{ref}

Closing and Summary

The proposed system is intended to secure content to the home and allow for the use of third-party competitive user interfaces to display MVPD content. The proposal does not reach into policy issues such as any requirements as to how MVPD content is presented to users. That particular issue is beyond the mission of this working group.

As facilities-based MVPD services move to end-to-end IP transport of video data, the proposed system can provide a "no hardware" solution to operator content availability on competitive navigation devices. DOCSIS, ADSL, and wireless providers can leverage software supporting these protocols to provide on-premises access (via WiFi or Ethernet) via competitive navigation devices. Other managed-medium services (OSI Layer 1 and 2) may not support bidirectional DCAS authorization, key exchange, and provisioning. Furthermore, some systems (such as satellite) may never provide a purely "hardware free" solution to access of their primary unicast satellite transmission.

These legacy and one-way systems can make use of a Provider Interface Device or Gateway to provide the same functionality as end-to-end systems on a local network. (Note: This requirement exists in both protocol-based and remote-UI-based systems.) Currently-implemented examples of this modular functionality include, but are not limited to, Dish Hopper, DirectTV Genie, SiliconDust HDHomeRun (CableCARD to Ethernet), Hauppauge WinTV-DCR-2650 (CableCARD to USB), and the Simple.TV 2 (ATSC to Ethernet).

By implementing DCAS and Provider Interfaces as described, users can enjoy client manufacturers' alternative methods of navigating the remote UI services without losing any intended functionality. This approach would provide a search capability, a launch capability and state management, with access to same live, linear and VOD as MVPD applications.

Section II: "Application-Based Service with Operator Provided User-Interface" System

Introduction

The apps approach developed in the marketplace through responses to consumer behavior and preferences. As the apps model moved from the PC/Mac platform to smartphones, tablets, and other mobile devices, it grew rapidly in just the last few years in adoption, popularity and major support from MVPD and OTT app developers.

All of the major MVPDs now support an iOS and Android App to access their service on smart phones and tablets. All of the major MVPDs support their service on Microsoft Windows and Apple Mac OS X either through an application or a Web app (using a plug-in model for content protection today and transitioning to an HTML5 EME Web App in the future). Some of the major MVPDs already support Smart TVs (LG, Samsung, Sony, Toshiba), game consoles (PlayStation 3 & 4, Xbox 360 & One), and set-top boxes (Roku). Table 1 summarizes the supported retail devices, and MVPDs are also devising still more ways to expand the range of devices and platforms that can support MVPD apps. VidiPath Certification was launched in September 2014, and certified VidiPath client devices are expected in the market later in 2015. Many of the major MVPDs either support DLNA VidiPath today or plan to in the near future. ABI is projecting that VidiPath Certified devices will be available in approximately 40 percent of all U.S. cable households that subscribe to advanced services by 2016, and 70 percent by 2020. RVU, developed and maintained by the RVU Alliance (and included in DLNA guidelines), is supported by DirecTV, developed and maintained by the RVU Alliance, is supported by DirecTV. And MVPDs are continuing to expand their support for more devices and platforms.

MVPD apps follow the same approach as the apps that Netflix, Amazon, Hulu, Google, YouTube and other OTT providers use for delivering service on retail devices and platforms. The apps approach abstracts the differences between varied and rapidly changing consumer electronics platforms and varied and rapidly changing multichannel services that has evolved far beyond the simple broadcast video service on which CableCARD was based.

MVPD apps are by far the most widespread method for delivering service to retail devices and platforms today. Compared with the fewer than one million retail CableCARD devices today, there have been over 56 million downloads of MVPD apps as of July 23, 2015, with millions more occurring every month. Roku, a retail set-top box that relies entirely on apps (including a cable operator app with a cable-operator supplied guide), has sold over 5 million units, outselling TiVo (with its "third party" TiVo guide) five-to-one.

As shown above in Table 8, there are over 450 million retail video devices in the US that can be served by an MVPD app—about twice the number of set-top boxes in use by MVPDs. 94% of them can be served by one or more MVPD apps. 66% can be served by an app from all of the top 10 MVPDs.

The specifics of how MVPDs deliver their service to PCs and MACs (either as a Web or as an app written to the PC or MAC operating system), as well as the number of subscribers for each MVPD is shown in Table 9.

MVPD	Subs (M)[45]	PC (Windows/Mac OS X)[46]
Comcast	22.6	Web app
DirecTV	20.3	Web app
DISH	14.1	Web app (DishAnywhere.com) and Native app (Slingplayer App)
TWC	11.4	Web app
AT&T U-verse	5.7	Web app
Verizon	5.3	Web app
Charter	4.4	Web app
Cox	4.3	Native app (Cox TV Connect)
Cablevision	2.7	Native app (Optimum)

Table 9 - MVPD Subscriber Count and Support for Personal Computers

This Apps-based System proposal leverages this technological advancement and the development work in Internet (W3C) HTML5, iOS, and Android; the cross-industry standards developed in DLNA and RVU for interoperability among MVPD and retail devices; and current efforts for implementing HTML5 apps to reach additional retail devices.

By utilizing the most widespread approaches employed by MVPDs and OTT providers, and software components widely adopted by CE manufacturers, this proposal enables retail device manufacturers many choices for how to receive MVPD services. In this System, the retail device manufacturer can choose one or more of the following techniques to build a retail device that can provide the MVPD service through a downloaded MVPD app or MVPD RUI:

- Device Specific Apps (e.g. iOS, Android, Samsung Smart TV, LG, Xbox, PlayStation, Roku)
- HTML5 Web Apps
- DLNA VidiPath
- RVU
- DISH Virtual Joey
- Sling Media Technology Clients

The MVPD or OTT video provider can use a common cloud infrastructure to deliver content in an optimal fashion to the broad diversity of retail devices and platforms using one or more of these six app-based approaches. Device Specific Apps can take advantage of the latest features in the latest devices and tailor the user experience to the specific device, e.g. multi-touch, accelerometers, finger print identification, and speech recognition. Web Apps executing on a standard HTML5 platform can reach a broad set of devices with a rich set of application features. DLNA VidiPath leverages the W3C HTML5

[45] SNL Kagan
[46] Either as a browser plug-in or as a Windows & Mac OS X application (in the future HTML5 EME/MSE will deprecate browser plug-ins)

Web App model, but also integrates with other devices on the home network offering a rich home user experience.

There is a high degree of commonality across all six app approaches:

- IP video transport to the end device
- IP-based DRMs for content protection
- A rich, competitive, omnipresent CE user interface shell controlling the device
- Multiple, competitive, app-based MVPD and OTT video service user interfaces
- CE services are enhanced and updated by updating the platform
- MVPD and OTT services are enhanced and updated by updating the applications

Because of these commonalities, retail devices can also implement multiple approaches to accommodate multiple MVPD approaches rather than just a single approach. For example, VidiPath, HTML5, and Sling are all HTML5-based. One integrator (Jethead) has implemented both VidiPath and RVU in a single smart TV stack, as was shown at the 2015 INTX Conference.

Error! Reference source not found. shows this approach as each MVPD or OTT video provider hosts a set of cloud services and provides an app for the relevant app platforms (Android, iOS, Windows, OS X, game consoles, etc.). Content is protected using the DRM used on the respective platforms and the corresponding hardware.

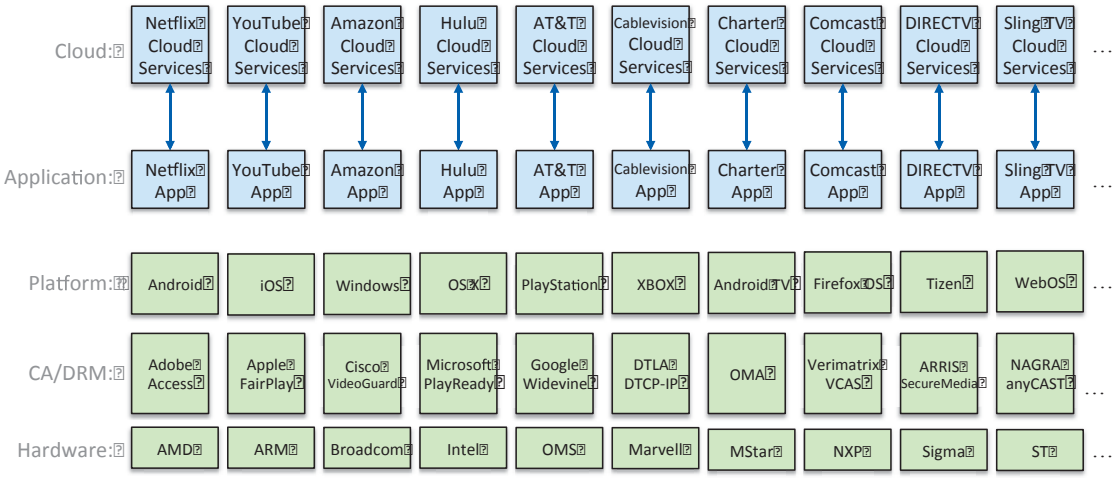


Figure 38 - Overview of App Approach

Collectively, this System abstracts the diversity and complexity of service providers' access network technologies and customer-owned IP devices and accommodates rapid change and innovation by both service providers and consumer electronics manufacturers. This application approach may also make use of a combination of software-downloadable security and (when available) a hardware root of trust, as described in [WG3], and may utilize the application to enforce other limitations on access, copying, distribution, and usage in a similar way to how they are currently enforced through leased MVPD device applications (such as blackouts, geo-filtering and geo-fencing, alternate content, messaging and

redirection for unauthorized channels, and parental control) and not exclusively through the security system. This diversity and flexibility enables the broadest coverage of retail devices, optimizes the consumer experience on the latest devices and technologies, and takes advantage of a wide range of market-tested security measures including downloadable DRMs.

The following sections discuss these app approaches.

Device Specific Apps

Today almost all of the relevant retail devices provide an app platform (e.g. iOS, Android, Samsung Smart TV & Tizen, LG WebOS, Xbox, PlayStation, Roku, TiVo, etc.) with an associated Software Developer Kit (SDK) that includes the platform APIs, developer's program, and app store to enable apps to be downloaded to their devices. These app platforms either provide access to one or more embedded platform DRMs and/or allow for an app developer to provide a DRM of their own choosing integrated into their app. The robustness of the various DRM implementations, embedded or integrated with app, varies and will impact the quality of the content that can be displayed on the device subject to content license requirements. In order to support their App marketplace these platforms have developed various security capabilities to insure that the content and applications are protected appropriately.

While these app platforms all provide an app developer program with an associated SDK and app store, they differ in the specifics of the licensing involved, the app development process, and the app approval process. These differences reflect a competitive marketplace where device manufacturers attempt to provide the best app development platform and device volume to encourage the development of compelling applications that will attract consumers further increasing the value of their products. These differences in the respective app ecosystems also reflect the diversity of device capabilities (e.g. smart TVs versus smart phones versus game consoles) provided by the platforms. The device manufacture chooses its own app platform and provides a set of app guidelines with an app approval process that is defined and managed by the platform developer. These guidelines and app approval processes control what apps make it on to their platform via distribution in their app store.

In developing apps for different app platforms, MVPDs are no different from any other app developer. They participate in the app platform just as any other app developer for that platform. MVPDs take into consideration the same factors as any other app developer when deciding which platforms to use, platform capabilities, reach, ease of development, device popularity, license terms, etc.

App Development

App Developer programs

The app developer program is intended make it easy for app developers to develop applications. The better programs provide extensive documentation of their SDK, example code, as well as development tools, such as Integrated Development Environments (IDE) and device emulators. Some of these platforms use HTML5 and JavaScript as the platform, while others provide scripting languages, and still others develop in Java or other programming languages. This also provides another point of

differentiation. Devices that support these platforms can expose various resources of the device to app developers, such as multi-touch and speech recognition.

Platform	Description
iOS	Apple's developer program iOS and Mac OSX is available at: https://developer.apple.com/programs/ and provides extensive documentation and resources for application developers. Xcode is Apple's integrated development environment (IDE). Xcode includes a source editor, a graphical user interface editor, and many other features. Apple provides an iOS Simulator that simulates multiple iOS and watchOS environments.
Android	Google's Android developer program is available at: http://developer.android.com/index.html and provides extensive documentation and development resources for application developers. There are two integrated application development environments (IDEs) available for Android, Eclipse or Android Studio with Java as the development language. The Android SDK includes a mobile device emulator.
Samsung Smart TV & Tizen	Samsung supports two app developer programs for its smart TVs with its Smart TV platform or its Tizen platform. The Samsung developer program is available at: http://www.samsungdforum.com/ and provides extensive documentation and support. Samsung is in the process of phasing out the Smart TV platform in favor of the Tizen platform. The Smart TV platform supports Web applications, while Tizen supports Web applications, native applications and hybrid applications. However, Samsung Tizen TV provides only a Web application environment for app developers. App developers in Tizen also develop applications based on Web technology (HTML5, CSS3, Javascript). Tizen also supports Samsung's mobile devices, tablets, smart phones, and smart watches.
LG webOS	LG's webOS developer program is available at: http://developer.lge.com/webOSTV/ and provides documentation and support. LG uses the Eclipse IDE for development. LG provides a webOS TV Emulator that emulates webOS TV on a computer enabling the developer to test and debug apps on a computer.
Roku	Roku's developer program is available at: https://www.roku.com/developer and provides documentation and support. Applications on the Roku player are developed in BrightScript, a scripting language, using an Eclipse IDE.

Table 10 - App Developer Programs

Supported DRMs

The app platforms also support different DRMs. Platforms with a broader set of DRMs potentially support content from more sources.

Platform	Supported DRMs
iOS	FairPlay and third-party DRMs such as Video Guard
Android	Any, provides a DRM framework supporting third-party DRMs as plug-ins
Samsung Smart TV & Tizen	PlayReady, Widevine, Verimatrix, SecureMedia, SDRM, and SCSA
LG WebOS	PlayReady, Widevine, Verimatrix
Roku	PlayReady for Smooth Streaming and AES-128 bit encryption for HLS

Table 11 - Platform Supported DRMs

App Guidelines

App platforms also differ in the guidelines they provide to app developers to provide the criteria by which applications are evaluated in the app review process. Some provide very explicit and comprehensive guidelines that are strictly adhered to and others provide looser guidelines with less strict enforcement. In general, these guidelines are living documents and subject to revision over time.

Platform	Description
iOS	The Apple app guidelines can be found at: https://developer.apple.com/app-store/review/guidelines/ Applications for the iTunes Store are developed, tested, and distributed using guidelines and tools that Apple provides to all developers. Apple regulates applications and their functionality by enforcing a testing process that occurs upon submission of an app to the iTunes Store. While there is no guaranteed maximum duration of this process, Apple tries to review all submitted applications within a week. During this time, their testers evaluate the app against a strict set of requirements which ensures that the submitted applications perform as desired on selected platforms, do not violate any of Apple's terms and conditions, and do not provide an outlet for any illegal activity.
Android	The Android App ecosystem is not as stringently managed as the Apple iOS app ecosystem. Android apps are not strictly approved by Google and are self-signed only. Apps can be delivered from the Google Play Store over Google protocols, or the Amazon Fire Store, or they can be side-

Platform	Description
	loaded directly onto the device. Google provides a set of developer guidelines to assist in the development of Android apps, as well as a set of design guidelines that help developers to make apps that not only work well but also look good. The developer guidelines for Google Play can be found at: http://developer.android.com/distribute/tools/launch-checklist.html#understand-policies
Samsung Smart TV & Tizen	In order to distribute applications on Samsung TVs and make them available through the Samsung Smart Hub Apps TV store, it is necessary to register the application and it must go through a certification process provided by Samsung or its Affiliate at the Application Seller Office before being launched on the Samsung Apps TV store. To request certification, it is necessary to prepare the Tizen widget package and metadata and submit it in the Samsung Apps TV Seller Office
LG WebOS	The LG application quality assurance team evaluates the performance, function, and UIs of submitted apps to verify the suitability for publishing on LG Content Store (LG STORE). Valid apps are published on LG Content Store (LG STORE). Every app submitted to LG Smart World will go through a Quality Assurance (QA) process before sale is permitted. Those Apps that do not meet the QA criteria can be rejected for sale. The QA criteria applies to every app submitted but certain Apps such as game, video, education, etc, can be subjected to additional criteria by category.
Roku	Roku television design guidelines can be found at: http://sdkdocs.roku.com/display/sdkdoc/Design+Guidelines. The specific restrictions and terms for publishing content to the Roku Channel Store are found in the Roku Developer Agreement.

Table 12 - App Development Guidelines

Operation of the App

The functionalities comprising the MVPD service, including a user interface, are provided via the application operating on the device. The MVPD service is enhanced and updated by updating the application. The interface between the MVPD app and the device is provided through the device manufacturer's platform SDK. The interface between the MVPD app and the DRM is either provided as part of the platform SDK or is the one selected by the MVPD and built into its app. Figure 39 shows examples of these two models. In the case of Device 1, the platform provides an embedded DRM client (DRM A). In the case of Device 2, the DRM client is integrated into the MVPD's app. The MVPD then operates a DRM server for each DRM used, one for DRM A and one for DRM B, and the MVPD service is provided using either DRM.

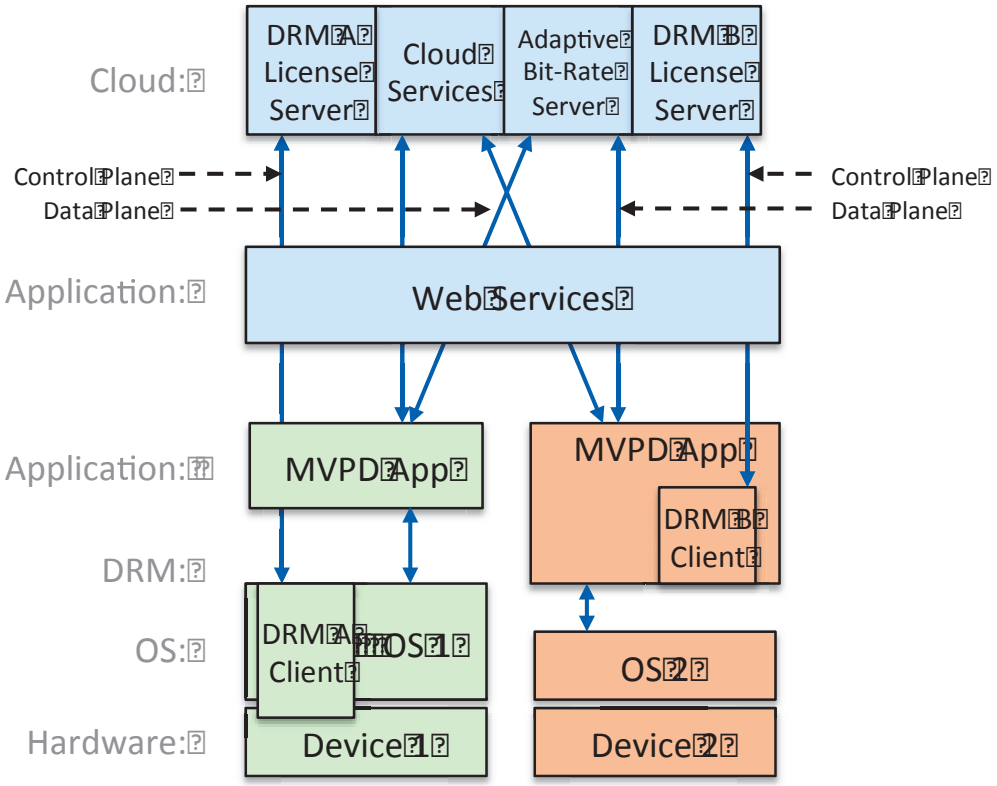


Figure 39 - Example App Interfaces

The essential downloadable security component is the DRM client, that is downloaded and updated either as part of the operating system of the platform on Device 1 or as part of the MVPD application on Device 2. The DRM control plane and the secure video content data plane are identified in this diagram.

Information

The device specific platforms include:

- Apple iOS - https://developer.apple.com/programs/
- Android - http://developer.android.com/index.html
- Samsung Smart TV & Tizen - http://www.samsungdforum.com/
- LG WebOS - http://developer.lge.com/webOSTV/
- Microsoft Xbox - http://www.xbox.com/en-US/developers
- Sony PlayStation - https://www.playstation.com/en-us/develop/
- Roku - https://www.roku.com/developer

Applicable Devices

As outlined above Apps can be developed for almost every class of retail device, including:

- Smart or connected TVs
- Game Consoles
- Retail set-top boxes or HDMI sticks

- 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.

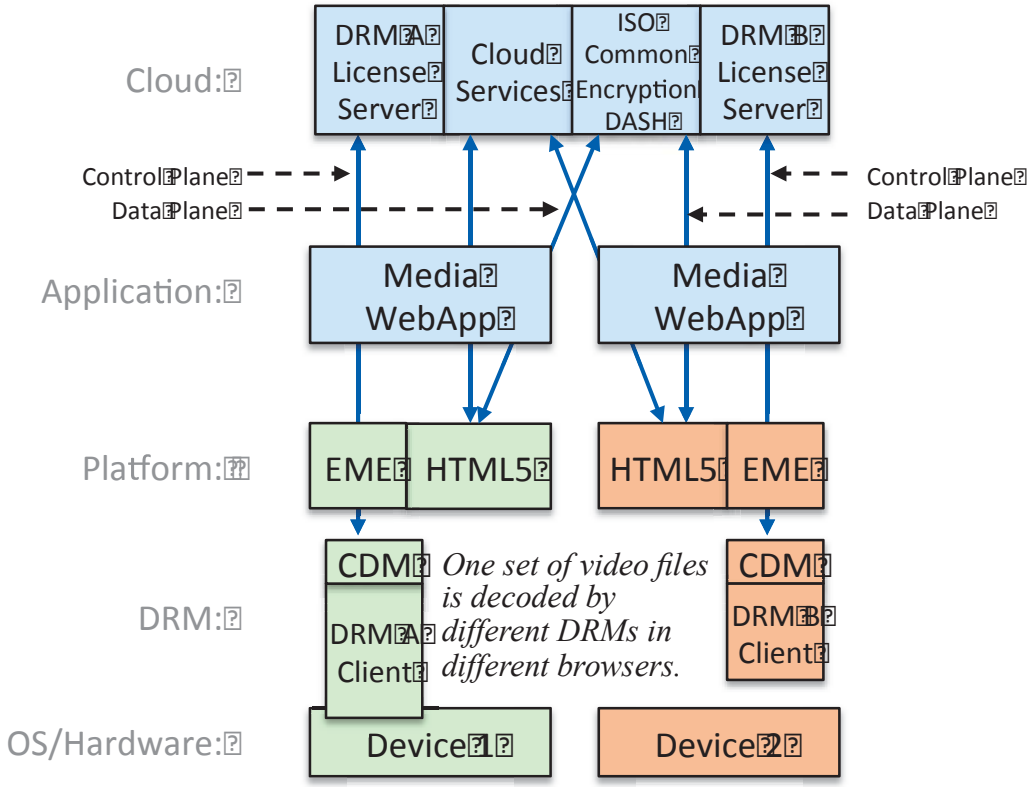


Figure 40 - HTML5/EME Implementation

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

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

Information

The DLNA VidiPath Guidelines can be obtained at: http://www.dlna.org/dlna-for-industry/technical-overview/guidelines

Applicable Devices

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

RVU™

The RVU protocol addresses the digital video industry's need for commonality and flexibility. See "RVU™".

Information

The Version 1.0 RVU Specification has been publically available since Fall 2009, Version 2.0 since Fall 2012, and a comprehensive certification program has been in place since Spring 2011. RVU is implemented on a wide variety of technology platforms, and has won awards at major trade shows and conferences around the world. RVU devices have been fielded to consumers nationwide since Fall 2012, in the form of 9 million DIRECTV Genie branded servers and several times the number of servers in Genie branded clients as well as RVU-certified Smart TVs from Samsung, Sony, LG and Toshiba. 4K/UHD services became available on RVU servers and Smart TVs from Samsung during 4Q/2014.

Virtual Joey

DISH Network provides and supports a number of in-home devices for its subscribers to enable reception and navigation of its service. These include the Hopper® Whole-Home HD DVR and the Joey, which enables Hopper DVR features in every room. Additionally, DISH supports the Virtual Joey client software on Sony PS3™ and PS4™ systems. A virtual Joey is authenticated during connection to the associated Hopper, which allows the Hopper to rely on additional robustness and other security features. The Virtual Joey behaves like a (real) Joey client, and enables navigation of DISH's broadcast system and Hopper DVR recordings.

Standards

The Virtual Joey is built on home network standards, including Ethernet and WiFi; UPnP device discovery; DLNA media streaming (and proprietary extensions); DTCP-IP content protection; and HTML5. Virtual Joeys are co-developed among DISH, EchoStar, and a device manufacturer pursuant to negotiated business terms.

Protocols

HTML 5 for RUI, TLS certificate processing; IP

Information

See http://www.dish.com/virtual-joey/

Applicable Devices

Playstation®3 and PlayStation® 4 systems

Sling Media Technology Clients

DISH Network provides and supports the Hopper® with Sling® Whole-Home HD DVR. DISH also supports the Sling Adapter connected to its Hopper, ViP 722, or ViP 722k DVR receivers. DIRECTV similarly offers a GenieGo device, which connects via the home network to its HD DVR receivers. The ARRIS MS4000 (Media Streamer 4000) enables MSOs to use the same technology to serve their customers.

Standards

Ethernet; 802.11n WiFi. SlingBox clients are co-developed between EchoStar and a device manufacturer pursuant to negotiated business terms, or by EchoStar on platforms that support independent development environments.

Protocols

IP

Information

DISH or MSO subscribers load the applicable Slingplayer App on their chosen retail device, which can then watch and navigate live or recorded TV and access program guide and DVR content, and operate other features of the related service.

Applicable Devices

ARRIS MS4000 (Media Streamer 4000); DISH Hopper, ViP 722; ViP 722k; Mac or Windows PC; iOS, Windows, Amazon Fire and Android tablets and phones; Apple TV; Roku or Roku TV; Google Chromecast; Amazon Fire TV.

Use Cases Supported

Unlike the CableCARD/UDCP model, which was designed for reception of linear cable channels from digital cable systems for reception on cable-specific UDCP devices, applications as an approach are platform and technology neutral, allowing retail devices to operate across MVPD and OTT platforms, and support linear, on-demand, interactive, and other advanced features of the MVPD service, while respecting the usage limitations associated with licensed copyrighted content. See “Essential Customer Experiences”; and Report of WG1, MVPD Requirements and Content Providers Requirements [76].

Tuning and Viewing a Linear Channel

The apps models abstract the transmission methods for the MVPD’s network and deliver the service in IP, using the audio and video codecs and the picture resolutions and formats supported by the retail device. The robustness and capabilities of the App platform may affect what content is available to devices that are supported by the App platform. The application also handles any concurrent stream management required by the network or content agreements. The application supports any applicable switched digital video.

The application tunes the channel and presents integrated applications associated with the tuned channel, such as camera angles, as well as subscription applications such as sports statistics, interactive advertising, and caller ID on TV.

The application also presents the broadcast, zoned or targeted advertising inserted into the linear channel. Interactive request for information and telescoping ads are supported. All requirements for acceptable advertising, ad boundaries, ad lifecycle management, audience measurement, ad measurement and reporting are supported.

The application supports blackouts, geo-filtering and geo-fencing, alternate content, messaging and redirection for unauthorized channels, and parental control. The application manages copy controls and output restrictions.

The application supports trick play capability.

The application supports the network's technology to reduce channel change latency.

The application supports all regulatory requirements, including delivery of EAS and statutory privacy requirements.

On-Demand Content

In addition to supporting linear content and features, applications support transaction, subscription, and free VOD; EST; Start Over and Look Back. They also meet advertising requirements as required by content providers who license the content and advertisers who fund the dual-revenue MVPD business, e.g., dynamically inserting pre-roll advertising or disabling fast forward during advertisements included with VOD content. In addition, applications support limitations on in-home and out-of-home viewing, and limitations on simultaneous viewing e.g. across a viewer's authorized devices.

Pay Per View (PPV) events

Applications also support PPV requirements such as free preview, purchase and cancellation windows, secure purchase credits and purchase limits.

Navigation

Apps use a UI designed by the MVPD for interacting with the MVPD's experience. Consumers receive a common, familiar MVPD experience across devices, such as the ability to navigate and see recent tuning history regardless of which device was used. This is similar to how consumers experience Netflix and other OTT video services. 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. This is consistent with the approach used by OTT video providers and with public pronouncements by Thomas Riedl, head of Google's Android TV, *"Content owners and distributors are one of the key stakeholders for us. For them, what's crucial is they want to deliver the best user experience and make sure that the content they provide to the user is displayed exactly as they broadcast it. Also in their role as app developer, they need to be able to completely control the experience. Android TV allows them to do all of these things based on our proven technology platform." IPTV News 4/21/15, http://www.iptv-news.com/2015/04/google-google-tv-has-evolved-into-android-tv/*.

Apps present the modern features of MVPD navigation, such as mosaics, recommendations from what's trending or popular in the neighborhood, view by genre, and recommendations from a user profile across devices. DLNA VidiPath and RVU offer the ability to navigate to and discover content or services on the home network.

Apps enforce content license requirements from content providers, including channel presentation in required neighborhoods (e.g., news channels) and channel assignments (e.g., broadcaster carriage on channel); channel logos; and search requirements (such as a network-branded point of entry). There is no standard feature for a retail device to conduct deep search from outside of the MVPD app. YouTube previously provided an API that permitted DIRECTV and other third parties to deep link to and play YouTube content without seeing the YouTube UI; it subsequently removed that API and substituted a new API through which the YouTube UI presents YouTube content, even when accessed from a link.[47] Facebook and Twitter apps do not automatically enable deep search by web browsers. However, marketplace search deals can be done by mutual agreement, as Twitter agreed to do with Google and Netflix agreed to do with TiVo. Requiring negotiation is an established means for assuring that the "search" does not artificially raise or suppress rankings in search results. There are also opportunities for business-to-business deals for new user interfaces. For example, Xbox One uses a UI that was designed to be familiar to TWC subscribers and to Xbox users. It also integrates MSFT connect voice and gesture control. Likewise, TWC built a grid guide for Roku.

Recording Linear Content

The DLNA VidiPath spec provides a recordable DTCP-IP output, so that a retail DVR can record programming received by VidiPath. RVU servers similarly provide a recordable output, with copy control information set in accordance with content agreements. DLNA continues to evolve, and may augment this in the future.

Content providers generally do not currently permit apps on mobile devices to provide a recordable output. Similarly, Netflix does not present a recordable output to CE devices. Apps to Smart TVs may present recordable outputs. Content providers licensing terms may continue to evolve, and downloadable Apps/DRMs can be updated accordingly.

---

[47] Under Google terms of service, Google also demanded that Microsoft shut down its use of YouTube because "The app blocked ads on videos, and it allowed users to download videos directly to their devices. Additionally, Google has said that the app also violates another rule, because it allows users to watch videos that have been set by the publisher to only play on certain devices (ie. some videos are blocked on mobile.)"
As predicted: Google asks Microsoft to shut down new YouTube app
http://www.phonearena.com/news/As-predicted-Google-asks-Microsoft-to-shut-down-new-YouTube-app_id43091 The Google YouTube Developer agreement now includes requirements that the developer protect Google's brand and not "separate, isolate, or modify the audio or video components of any YouTube audiovisual content made available through the YouTube API." https://developers.google.com/youtube/terms?hl=en
Netflix likewise terminated its public API. Gigaom: Netflix is shutting down its public API today
https://gigaom.com/2014/11/14/netflix-is-shutting-down-its-public-api-today/. We have not found any evidence of a public API through which Amazon permits third party sites to play Amazon Prime Video outside of the Amazon experience.

Remote Management by Consumer

Apps for the Smart TV and other devices enable consumers to change channels and manage their account via a network-connected mobile device. Such apps also allow consumers to manage their caption settings and other accessibility features and select their language through the mobile device.

Set-Top Box set-up

Apps for the Smart TV support establishing menu preferences, device settings, parental controls and accessibility.

Customer Support and Remote Management by Service Provider

Apps permit the service provider to troubleshoot and support device experiences.

As a common cross-platform MVPD experience is delivered across all retail devices via the MVPD App, MVPDs are able to offer better and consistent support and diagnostics to consumers.

Cloud Delivery

By using applications with popular device platforms, MVPDs can make VOD, live linear, recorded content, and download-to-go content available to customer-owned devices on a cloud-delivered basis, as permitted by content and distribution rights.

Section III: Implementation Analysis

Evaluation of "Competitive Navigation" System Proposal by Proponents of Application-Based Service

The "CE Device "Competitive Navigation" System" proposal ("Device Proposal") offers an approach designed to permit device manufacturers to substitute their own user interface and guide for interacting with MVPD services and to draw from the MVPD the program guide information from which they could construct a different guide. The proposal is incomplete and omits many necessary elements necessary to assure that consumers receive the services for which they have paid, that the contractual rights of content owners are honored, and that MVPDs can continue to innovate and improve their services for the benefit of all customers. On July 31, 2015, the proponents amended portions of their proposal. This analysis has been updated to address those new portions.

How the Device Proposal Constrains the Tools of Innovation

The Device Proposal invokes some of the technologies that have been developed for innovative platforms, but then removes the tools that make them platforms for innovation. For example, the Device Proposal invokes Hypertext Transfer Protocol (HTTP), which serves as a content agnostic form of transport for web content and video streams. But the Device Proposal restricts HTTP to the transport of video and descriptive metadata, stripping the original and main purpose of HTTP - delivery of full web pages and web applications.[48] The Device Proposal does not welcome the delivery of higher-level protocols or applications. It wants only the video bits, and provides nothing at the application layer that allows applications to operate in the manner that makes the Internet such a rich environment for services.

The Device Proposal recognizes that the MVPD UI operates as integral part of service, but then calls for the extraction of discrete elements of the UI, delivered via "HTML widgets" through an expanded CableCARD MMI that is yet to be invented. The CableCARD MMI does not define how a hyperlink is navigated and selected. Unlike the application environment we see today, the CableCARD has no provision for JavaScript or other application execution environment in the Host device on the other side of the CableCARD interface. The Device Proposal suggests the potential for interactivity in an expanded MMI, but as the proposal stands today it does not offer any specifics; does not promise any capability for maintaining state information in the retail device necessary for application data to persist across widgets instances of the capabilities of this MMI; and provides no retail device query capabilities for

[48] The amended proposal invokes misstated examples and misplaced analogies from the web. It claims justification for using HTTP only for video transport by claiming that Netflix, YouTube and other online video providers limit HTTP to such transport. In fact, Netflix, YouTube, Hulu and other online video providers use web pages to distribute their content to PCs at a minimum. They may also provide native apps for platforms such as iOS and Android that use HTTP for video and web services, relying on the native app platform for their UI. The proposal also claims that hypertext and hyperlinks, the basis for modern web browsing, are intentionally defined separately from the browser or other navigation technology to allow both sides of the interface to be flexible. But the amended proposal is based on a set of yet to be defined network protocols and XML schemas designed to prevent both sides of the interface from being flexible.

adapting to different retail devices to different MVPDs. An MMI has to have an execution environment in the client to provide any form of interactivity, or it fails. But the Device Proposal provides for no execution environment within which the widgets delivered through the MMI can operate. The amended proposal states that the MMI offers a predictive execution environment; but the proposal specifically states an intention not to offer a predictable execution environment on the device and avoids specifying any standards for such an environment. All of these requirements have been addressed in the MVPD app based proposal which proposes a full HTML5 web application environment on the retail device.

The Device Proposal proposes "to determine the level of HTML that the MMI should support," but offers no reason why existing specifications like HTML5, EME, MSE and Web Crypto, all developed through the W3C open standards processes, would not be a more appropriate solution, as proposed in the MVPD WG3 and WG4 proposals. Instead, it would require essentially starting from scratch to determine the requirements for the Device Proposal's hypothetical MMI.

Moreover, the Device Proposal ignores the app-based model that has been widely deployed in the marketplace. Consumers have eagerly and widely embraced apps as the dominant means of accessing content and resources on their third-party consumer electronics devices. MVPDs have delivered on this consumer demand, making available apps that enable their customers to access and view their services on tens of millions of retail devices such as PCs, tablets and smartphones. MVPDs invest hundreds of millions of dollars to deploy a network and CPE to provide service. These networks have constraints based on the physical nature of the network medium (RF wirelessly or over coax, twisted pair copper, light signals over fiber). The physical constraints drive network architectures and the capital investment necessary to build and deploy the network and CPE devices. The app model helps preserve these network optimizations by allowing the applications to be partitioned according to the network architecture. Today's most successful retail devices offer APIs that allow innovation on both sides of the platform APIs (device side and application side)—but there are no APIs offered in the Device Proposal. Instead, it removes any APIs and fails to provide an application execution environment, with the expressed purpose of stripping out features of MVPD service.

The Device Proposal cites RFC 3439, but itself runs contrary to the End-to-End Argument and Simplicity section in RFC 3439 (https://tools.ietf.org/html/rfc3439#section-2.1). It does this by establishing network protocol interfaces to the proposed Virtual Headend at the application layer, thus requiring coordination between all of the MVPDs and retail device manufacturers to affect any changes to these interfaces. The End-to-end Argument recommends against these kinds of protocol definitions because of the inherit inflexibility and burden it places on applications and the network. The MVPD Proposal in contrast follows the OTT video distribution model by not introducing any new network protocols, thus preserving the flexibility at the application layer that has resulted in the tremendous growth of the Internet.

The Internet and Web protocol models are based on innovation at the edge of the network, e.g. at the server and the client ends of the network and not with a dependency on some intermediary in the

middle of the network between these endpoints. These innovations on the server and the client app happen together. Web applications have experienced explosive innovation because they have a predictive execution and display environment on the client device (HTML) and a reliable communication channel between the client and server (HTTP) free from intermediation or disaggregation by a third-party in the middle.[49] Websites on the Internet are able to author web applications (through web pages) that take advantage of the services provided by their web and back office servers and evolve them together without the need to negotiate with a third-party when the client/server interfaces evolve. The same is true of the mobile app ecosystems today. The mobile app platforms provide a predictable execution environment on the client and the application developer can evolve their client apps along with their server functionality without the need to negotiate with a third-party when the client/server interfaces evolve. The retail proposal proposes to disintermediate or interfere with this time proven model, by removing a predictive execution environment and freezing the client/server protocols and interfaces.

How the Device Proposal Would Constrain Service

The approach of the Device Proposal would impose substantial losses in the multichannel services ecosystem.

The Device Proposal strips out the very features with which MVPDs compete, improve service and market to consumers, on every retail device envisioned by the proposal. Satellite customers would lose sports scores and statistics for satellite. U-Verse customers would lose instant channel change. Cable customers would lose StartOver and LookBack, telescoped and interactive advertising. Cable program networks would lose the interactive enhancements they have built into their programming, such as shop by remote and multiple camera angles. The amended proposal suggests that "some" interactive MVPD features (such as Caller ID; sports statistics; News ticker) could be made available through an MMI widget for optional incorporation by a third party UI. All MVPD features that Device Proponents do not consider to be multichannel service would have to be entirely re-written and maintained in a new MVPD "widget" format. Even then, the mechanism to make it available is not defined,[50] and the device manufacturer is free to eliminate or block those features in its discretion, even if it is part of the MVPD's

[49] The Device Proposal flags a concern that current browsers support only one DRM each. While PC browsers today only appear to support one DRM, CE devices, such as Samsung and LG TVs support multiple DRMs. Mobile devices based on iOS and Android allow multiple third-party DRMs to be implemented. Retail devices can clearly do the same, or can permit the download of different browsers as desired or as they evolve. This is part of market evolution, and market forces will continue to apply.

[50] Most UI is tightly coordinated with the video display, including overlays like caller ID and tickers. The Device Proposal offers no mechanism for, say, the Caller ID to know where the top of the video is, for the ticker to know where the bottom of the video is, when the video has been reduced from full screen, or how to coordinate with captioning. All MVPD UI elements, including EAS and captioning are coordinated and tested together. A widget running inside arbitrarily different device UIs offers no comparable reliability.

service as provided to subscribers. The Device Proposal does not offer a method for actually delivering MVPD service as it has evolved or as it is offered, advertised, subscribed to and delivered. Nor does it offer a means for accommodating the continued evolution of services, as applications do.

Because the Device Proposal does not deliver MVPD services as they are offered today, it calls for MVPDs to invent a new and different service that includes far less. The Device Proposal defines three interfaces through which service must pass: Service Discovery Interface, the Content Delivery Interface, and the Entitlement Information Interface.

The Service Discovery Interface is limited to three elements: lists of available services; metadata about those services; and messaging from the MVPD relating to these services. The metadata and messaging related to these services significantly constrain innovation. The metadata in this interface is limited to describing the service, but does not permit any method of enhancing the service itself (e.g. interactive enhancements, multiple camera angles, request for information, telescoping ads, shop-by-remote etc.). The messaging in the proposal is described as expanding the limited CableCARD MMI model that can optionally displayed based on user input. While this appears to be describing a constrained HTML "widget" model, the specific constraints are not explicitly identified. By contrast, the MVPD proposal adopts the full W3C HTML5 model without constraints and thus includes much greater extensibility that is achieved through the app model.

The Content Delivery Interface constrains the types of content and the method of protecting those types of content to a limited set. Interactive enhancements to the content are not addressed or envisioned in this proposal. Nor is there a process identified for how any of these interfaces would evolve over time, in order to phase out obsolete technologies/features and introduce new technologies/features. DLNA and other multi-stakeholder organizations facilitate the evolution of their specifications and standards to keep up with technology evolution. The application model allows for rapid innovation and change. The Content Delivery Interface and regulatory mandates have none of these mechanisms.

The Entitlement Information Interface is described as "defin[ing] a common platform for publishing, communicating, sharing and transferring rights information." The proposal does not provide any details for how these rights are expressed or transferred. The expression of rights through a limited set of Copy Control Information (CCI) bits has proven to be one of the most limiting factors in the CableCARD model.[51] There is no indication of how modern business models could be expressed if the only interface from an in-home device is DTCP. After this was pointed out, the Device Proponents shifted their content protection analysis to invoke DTCP-2, which is in development. But they have not addressed what DTCP-2 entails or how it will support the extensive and dynamic business models that are today handled by multiple competing DRMs as in the apps model. The proposal provides much more detail about device authentication through the use of X.509 certificates, yet fails to provide the critical and necessary details

[51] For example, CCI bits do not cover EST, expiration date, or communicate license restrictions on in-home or out-of-home distribution.

about how these certificates are managed, the required trust infrastructure, certification, and any policies necessary to make the certificates useful.

The amended proposal acknowledges that standards do not exist for the interfaces it envisions, which it tries to characterize as a forward-looking virtue. In fact, assuming an un-invented standard ignores the technological variation in systems. MVPDs use apps to deliver services because apps can be tailored to the very different technologies and resources used in widely varying MVPD networks. The many different VOD systems, for example, can operate on mobile devices because specific MVPD code can be downloaded to apps platforms. The "virtual headends" and standardized protocols envisioned by the Device Proposal would require MVPDs to rearchitect and duplicate their networks to serve such devices.

These interfaces are all uni-cast and preclude any multicast efficiencies that could offered in a cloud based virtual headend. The Device Proposal claims to permit an MVPD to operate a Virtual Headend in the cloud, and use multicast for bandwidth efficiency. But the proposed interfaces are unicast, and offer no method by which multicast gets carried on the home network. This forces the MVPD to put a gateway (virtual headend) in the home even if it would be more efficient to use multicast over the access network.

The Device Proposal would impose burdens, costs, and losses onto service providers, consumers, and content owners, just to convert MVPDs from service providers into delivery vehicles for raw video programming (and program guide metadata) feeds from which Device Proponents may build their own services with no license from or responsibilities to the content providers who own and license that copyrighted content.

All of this is offered in supposed service of facilitating a third party program guide (and a third party service), but no evidence whatsoever has been presented to the DSTAC to indicate that such a guide is the recipe for success of competitive navigation devices, or that customers want the device maker to block available MVPD services. CableCARD devices have enjoyed very limited commercial success. TV manufacturers stopped supporting CableCARD interfaces early on,, and Microsoft is terminating support for the Media Center PC,[52] for which the CableCARD OCUR was designed. In contrast, the apps approach has radically expanded the number of video devices on which consumers can enjoy their MVPD and OTT services. With an applications 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, network interfaces, drives, speed and price. Further, the retail device manufacturer is free to choose all of the specifics regarding the app platform, the DRMs supported, the app store, and the app approval process for their retail devices. Roku has sold over 5 million of its retail set-top boxes that rely entirely on apps (including a cable operator app with a cable-operator supplied guide), outselling TiVo (with its "third party" TiVo guide) five-to-one. The Apple iOS platform, cited by Device Proponents as the most successful, follows the same app-based approach. And VidiPath and RVU were developed in open multi-

[52] "Confirmed: Media Center is Dead," https://www.thurrott.com/windows/3319/confirmed-media-center-is-dead (May 5, 2015)

stakeholder consortia that included CE and MVPD participants. Rather than being "deliberately designed" to preclude a third-party user experience, these apps-based solutions represent what the open and competitive marketplace determined were the appropriate standards for extending MVPD services to retail devices.[53]

Nor is the Device Proposal consistent with Section 629. While Congress authorized the FCC to require unbundling of incumbent Title II local exchange carrier network elements, it did so only with carefully crafted limitations to which the FCC has been strictly held to by the courts. The FCC has no such unbundling authority under Title VI. Section 629 addresses the availability of retail devices that can receive multichannel services and other services "offered" and "provided" by MVPDs, not to disassemble those services for third parties to create new services. Title VI bars the FCC from "impos[ing] requirements regarding the provision or content of cable services, except as expressly provided in [Title VI]."[54]

CableCARD is Not the Starting Point for DSTAC

The Device Proposal frequently invokes CableCARD and CableCARD technology as a benchmark for future retail navigation devices.

The CableCARD/UDCP model adopted more than a decade ago was designed only for reception of one-way linear cable channels from digital cable systems,[55] 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 resulting devices met with very little consumer acceptance.[56] Compared

---

[53] VidiPath was developed in DLNA by major retail device manufacturers (including Samsung, Panasonic and Sony); major chip manufacturers (Intel and Broadcom) and major MVPDs (including Comcast, TWC, and AT&T). Although the Device Proposal calls VidiPath "interim," there is nothing "interim" about VidiPath or other gateway solutions. For example, ABI is projecting that VidiPath Certified devices will be available in approximately 40 percent of all U.S. cable households that subscribe to advanced services by 2016, and 70 percent by 2020. The Device Proposal also mischaracterizes VidiPath as some sort of transitional black box that "converts" video services to unbundled IP streams. As detailed in the Report, VidiPath is app delivery vehicle. Nor does cloud to ground delivery "terminate" an MVPD's proprietary network. It delivers an app that interacts with the server(s). The RVU Alliance standards organization reported to the FCC that successful market-driven technology like RVU is less likely to be able to bring the advantages of the RVU RUI technology to consumers if that technology becomes a target of regulation. http://apps.fcc.gov/ecfs/comment/view?id=60001059431

[54] The amended proposal claims that STELAR is a Congressional directive for the FCC to replace apps-based delivery of MVPD service. When STELAR was being negotiated in Congress, a proposed amendment would have assigned DSTAC an expansive mission to develop a new technology mandate for the FCC to adopt by rule. The sponsor lacked support for that proposal, withdrew the amendment, and that provision is not part of the law.

[55] CableCARD was designed for cable architectures, business practices and infrastructure, not for satellite and IPTV distributors. It was only implemented by cable systems.

[56] The amended proposal takes issue with the support provided for CableCARDs. The extensive support is catalogued at Comments of NCTA, CS Docket No. 97-80, http://apps.fcc.gov/ecfs/document/view?id=7020514104 (Timeline of Cable Industry Support for CableCARDs)

with the fewer than one million retail CableCARD devices today, there have been over 56 million downloads of MVPD apps (as of July 23, 2015), with millions more occurring every month.

Notwithstanding the limited successes of TiVo Series 3+, SiliconDust and Hauppauge devices, CableCARDs have been neither "upgradeable" nor conducive to innovation. As reported by WG2, the requirement to use CableCARDs in leased devices delayed cable operators' transition to all-digital and use of switched digital video. Verizon had to bolt on a redundant method for delivering entitlements to UDCPs using CableCARDs – using a slower carousel approach for which CableCARDs were designed rather than the instant entitlement designed for FiOS. Verizon also had to add additional EAS and OOB signaling just to address UDCPs using CableCARDs. FiOS IP services do not pass through the CableCARD. The CableCARD's limitation to 1995's MPEG-2 Transport Streams is incompatible with modern video delivery formats (e.g. ISO Base Media File Format) used by competing video providers. Very limited innovation has occurred in CableCARD devices. For example, the CableCARD was changed to support multi-stream and SDV tuning adapters, but only with time consuming re-engineering and high cost. CE device manufacturers and MVPDs have innovated *around* the CableCARD to reach a wide variety of retail devices, with hundreds of new MVPD services, using the more widely adopted web- and app-based approach.

From the outset, the presence of a third-party program guide on UDCPs was designed to be transitional. By the terms of the MOU and the FCC's implementing rules, UDCPs were designed as one-way devices. As they transitioned to interactive devices, they were to present the full cable service using an apps-like approach running on common middleware, not on protocols.[57] By rooting itself in technology that is more than a decade old rather than in modern applications, the Device Proposal would impose even more constraints on innovation.

Use Cases Supported

Tuning and Viewing a Linear Channel

Although the Device Proposal claims to support the delivery of linear services, it is impossible to determine that it would. It identifies a number of protocols, but does not specify which would be the preferred embodiment. It invokes standards that are not implemented (e.g. SCTE 65 Profiles 4-6 and CEA 2033) or standards that are implemented only by some MVPDs (e.g, Zeroconf which implies a

[57] 2002 Memorandum of Understanding, FCC 03-3, 18 FCC Rcd 518, 548, http://telecomlaw.bna.com/terc/core_adp/get_object/FCCRCD18-518.pdf ("for Advanced Interactive (two-way) Digital Cable Products … Cable operators' EPG will be provided for advanced interactive digital cable products via OCAP or its successor technology.") For some reason, the Device Proposal detours to call OCAP 'antithetical to a competitive experience." Panasonic built a two-way OCAP TV, but CableCARD-enabled TVs disappeared because consumers rejected the $300 or larger markup that retailers attached to them. See First Panasonic Tru2way TVs hit stores in Chicago, Denver, CNET (October 16, 2008), available at http://www.cnet.com/news/first-panasonic-tru2way-tvs-hit-stores-in-chicago-denver/ . ("The Panasonic Tru2way models will be priced at $1,600 and $2,300 for the 42-inch and 50-inch model, respectively … a premium of $500 to $670." The editor added his prediction: "Few people are going to accept a 45 percent surcharge for the privilege of losing their cable box. The premium for Tru2way compatibility needs to get closer to the $100 range--at maximum.") The market has since moved on to apps on Smart TVs, which operate as in the MVPD proposal.

particular provision, management, and fault detection system in the MVPD's network.) It is not sufficient to simply name a standard without a more detailed description of what parts of the standard are implemented, and how, preferably with a certification program and reference implementation as is done with VidiPath and RVU. The Virtual Headend System proposal – which is not even reflected in its supposed schematic -- will in fact require that all operators radically re-architect their networks. Among the service features that would need to be re-architected are: Instant Channel Change (ICC),[58] Switched Digital Video (SDV), Video-on-Demand (VoD) in all forms (transactional, subscription, free, etc.), Electronic Sell Through (EST), Pay-Per-View, blackouts, zone based ad insertion, promotions (e.g. buy-one, get-one-free or try-and-buy or upgrade service, etc.), and any interactive service features (e.g. interactive shopping, interactive advertising, request for information, telescoping ads, etc.). It would represent a significant, burdensome, and time-consuming development effort to standardize these protocols. It also represents an entirely redundant architecture to the solution MVPDs are actually using today to delivery such features.

The Device Proposal does not even support linear channels within its own terms. It explicitly acknowledges reliance on "prosthetic" auxiliary devices for satellite and IPTV, at the very least – meaning more boxes (and more energy consumption). It also assumes a separable tuning adapter box to support cable SDV, rather than considering an application based approach that has already solved this problem.[59] These additional MVPD-provided devices would be required for any consumer who sought to use a retail device in their home. By comparison, the apps model today delivers a full user interface for an MVPD service to a smart TV with no set-tops or gateway devices required at all beyond the basic network modem.

The Device Proposal acknowledges that it is unacceptably burdensome to rebuild all MVPD systems.[60] But the Device Proposal does not take account of the technological differences among them, and thus

[58] The amended proposal claims that U-Verse could implement fast channel change under in its implementation of the Content Delivery Interface in the Device Proposal. This is incorrect. In order to implement instant channel change, the retail device must implement the proprietary Media Room protocols, otherwise, ICC cannot be implemented, nor can it be implemented in a U-Verse gateway. The amended proposal also states that ADSL modems serve as Provider Interfaces in AT&T U-Verse. U-Verse is actually provided through VDSL gateways, which are not strictly a bridging modem, and implement the proprietary Media Room protocols that facilitate multicast and ICC.

[59] As an alternative, the Device proposal seeks to reduce the various competing SDV systems to one universal web based approach, with no assured mechanism for the retail device to release the channel—which is essential to recovering bandwidth for reuse. We are benefiting from a competitive and evolving market in SDV technology, already evolving beyond QAM delivery. AT&T's Media Room implementation uses a proprietary version of multi-cast IP and ICC. CableLabs recently published multicast IP specifications for video distribution based on NORM (available at: http://www.cablelabs.com/specs/specification-search/), which is currently under consideration within DVB. Imposing a single uniform approach will arrest this innovation in dramatically improving bandwidth utilization.

[60] The Device Proposal notes that in general, only such devices as are designed for the various proprietary systems and authorized by the specific MVPD can connect directly to the MVPD network to achieve full access. In some cases, this can be part of security. Pirate devices are best dealt with if they can't "connect" to DBS broadcast service.

would require exactly that kind of rebuild to engineer a Virtual Headend, widgets apps, and other unspecified technologies..

The Device Proposal asserts that because one MVPD is using a particular protocol or architecture, all MVPDs can use the same protocol or architecture. As one example, its premise is that all of these technologies are transitioning to IP and may readily converge on one solution in IP. This view ignores the diversity of MVPD network technologies and architectures. Because of that diversity, while MVPDs are adding IP delivery to their service, they are not all doing so at the same pace or through the same architectural approach. DBS systems will never evolve to IP carriage or encapsulation of their broadcast.

As another example, the Device Proposal calls for unicast delivery to a retail device. The AT&T service architecture is based on a proprietary Media Room implementation that uses a multicast IP distribution to the end client that makes use of a proprietary Instant Channel Change protocol as well. The entire system is built around a distributed model that shares stream coordination to manage the U-Verse service within the limited bandwidth available on VDSL. For AT&T to build a Virtual Headend as called for in the Device Proposal it would need to re-architect its multicast end-to-end model to one that breaks the multicast at a new gateway device and translates it into multiple uni-cast streams.

As a third example, the Device Proposal calls for MMI to deliver a widget to the device side of its interface, but DirecTV's RVU does not message its MMI—it is presented to the screen. The Device Proposal would add substantially to the complexity of in home DBS equipment in order to convert it to a "Virtual Headend"—something such equipment was never designed to be.

As a last example, the Device Proposal states that because many MVPDs already have deployed equipment in the home, they "may be convertible to an interim gateway by enabling the Ethernet interface already on the device." This optimistic theory is unsupported by any analysis, even a cursory one, and runs counter to the decades of experience of MVPDs who continually deploy new generations of in-home hardware after previous generations are found to lack the ability to accept new, more complex and larger software downloads that expand capabilities and provide new features. This is one of many ways in which the Device Proposal minimizes the effort required to separate out the various components that make up linear programming and make those components compatible with its proposed static architecture. The Proposal does not consider the burden imposed on the MVPD's system to deliver features, ad insertion and other components of the MVPD service over the proposed interfaces. Different networks use different approaches to optimize their technology for delivering competitive service. MVPD service is not a collection of "content items" and "micro-services." Most MVPD apps will or have the capability to hit multiple servers for data necessary to provide the service as an integrated whole. Different networks use different approaches for sound technical reasons. It is no trivial task to create and utilize an interface different than the one that has been optimized for the MVPD's specific network. For example, the Device Proposal does not even attempt to replicate rights protection like geo-fencing that occur in the device for networks that are optimized to broadcast all services to the device. That is why applications have developed as the bridge. Application code this diversity and complexity inside the app, delivering to an ever-increasing number of retail devices, without ever having to build a parallel network or slow network innovation.

The Device Proposal supports advertising inserted at the network source into the linear channel, but not interactive requests for information, telescoping ads, or promotions. It provides no local support for ad lifecycle management, audience measurement, or ad measurement and reporting, all of which is

measured in the home and requires an app or return path. The Device Proposal does not provide the tools to support the advertising that funds the dual-revenue MVPD business, or to provide an interactive and accountable ad platform that can continue to compete for those ad revenues. By contrast, Roku's app-based approach supports audience measurement, interactive advertising, its own ad business and the MVPD's app-based business.[61] Advertising is a $25 billion annual business for multichannel services; without support designed into a system proposal, ad dollars and financial support will flow to other platforms, to the detriment of MVPDs and their subscribers.

Cable operators are required to restrict the display of commercial web links in association with programming directed to children. The Device Proposal offers no restriction against prohibited ad overlays, whether agreed upon with content providers or required when airing children's programming.

The Device Proposal offers no support for EAS. EAS is delivered through a variety of means across MVPDs (e.g. in-band vs. out-of-band signaling, presentation differences, text crawl with audio override, forced tune, barker channel, etc.). Those differences can be abstracted through an application-based approach, but there is no indication that the EAS via MMI can be implemented across all MVPDs. In fact, if MMI display is only allowed as an option, EAS could not operate as intended. After this was pointed out, the Device Proponents proposed that consumers could not opt out of EAS—but that device manufacturers could still opt consumers out of virtually every other feature of service.[62]

Cable operators provide parents the ability to block channels they consider offensive regardless of rating. The Device Proposal offers no support for parental controls, including device restrictions (e.g., by channel, rating, time-of-day, etc.). Parental control entered through the MVPD's user cable box or MVPD website would not prevent delivery of restricted service to the retail device. Each retail box would need to be independently programmed for a consumer to be assured of receiving the protections they sought.

Cable and satellite operators are required to protect the privacy of the video records and other personally identifiable information of their video subscribers, particularly against government intrusion. The Device Proposal offers no support for statutory privacy.

<u>Analysis of use of Sat-IP</u>

Sat>IP was developed for a European DTH model which features satellite operators, device manufacturers and service providers acting independently to serve a variety of consumer television regional markets and business models (e.g. free to air). The US DBS model, on the other hand, consists of two vertically integrated (i.e. each acting as a service provider, a satellite operator and a device

[61] "Roku Unveils Advanced Video Advertising and Measurement Solutions," https://image.roku.com/ww/press/2015/Roku_Unveils_Advanced_Video_Advertising_and_Measurement_Solutions.pdf

[62] The amended proposal erroneously states: "The VidiPath and RVU section of this document states that despite the 'variety of means' for delivery of EAS, they abstract them to a common protocol (W3C's Server Sent Events (SSE)) such that the VidiPath and RVU clients do not have to implement all of the different methods." This is incorrect. SSE are included in VidiPath and are one option that an operator can be used for EAS, but there is no standardization of EAS protocols in VidiPath. The VidiPath app code allows each operator to connect to their different EAS protocols and present in their different user interfaces.

manufacturer) companies competing in a single consumer market. As a result, the benefits that the Sat>IP standard might allow in the European DTH model do not necessarily accrue to the US model. In fact, when applied to the US model the Sat>IP standard introduces new problems that would have to be addressed.

For example, the key benefit of the Sat>IP standard for the European DTH model is how it allows the satellite RF tuner and demodulator functions to be separated from the in home receiver, making these functions available as a single resource to other devices on the home IP network. As both US DBS operators have embraced whole-home architectures (in which a single STB performs all satellite RF tuner and demodulator functions, and then performs IP streaming to simple IP devices in other locations in the home), this primary benefit of Sat>IP has already been addressed.

At the same time, this separation of the satellite RF tuner and demodulator functions from the decrypting/decoding functions of in home receivers introduces many new issues, including:

- Tuner resource allocation: In a system having only two tuner resources, for example, if one device will be needing two tuner resources and another device will be needing a tuner resource later in the day, there isn't a mechanism via Sat>IP for the conflicting uses to be prioritized and resolved. In comparison, resource management is handled very simply and effectively in a whole-home Genie or Hopper architecture. In fact, Sat>IP would not have necessarily allowed Dish's innovative "Primetime Anytime" feature, in which a single tuner resource enables simultaneous recording and/or viewing of four different TV channels, to have been launched.
- Signal security: Either the Sat>IP tuner resource must perform CA/DRM descrambling, or each of the devices on the home IP network must do it: in either case security risks are increased when compared to the whole-home model that's already proven cost effective and secure.
- Rapid technology changes: The vertical integration of each US DBS service has allowed each to continually optimize signal capacity and installation efficiencies through rapid introduction of new and typically non-standard technologies. Historical examples include new modulations (e.g. Dish's proprietary 8PSK/Turbo) and frequency plans (e.g. DIRECTV's transponder bonding and "reverse band" operations). Each of these would have required changes to Sat>IP, changes which wouldn't necessarily have been possible in the time frames required by either US DBS operator.

On-Demand Content

Even assuming many required inventions that are undescribed, the Device Proposal would support delivery of VOD, but not a robust verification and audit platform required for the delivery of VOD assets. It would not support EST, Start Over or Look Back. EST grew 30% in 2014 alone, but the Device Proposal would not permit the MVPD to continue growing these purchasing options for consumers.

The Device Proposal does not support dynamically locally-inserted pre-roll advertising or disabling fast forward during advertisements included with VOD content as is often required as a condition to offering certain content on an on-demand basis.

The Device Proposal does not support user authentication (e.g. PIN and/or password entry).

Pay Per View (PPV) events

The Device Proposal includes no local support required for purchase and cancellation windows, secure purchase credits and purchase limits.

The Device Proposal does not support user authentication (e.g. PIN and/or password entry).

Navigation

Since the Device Proposal intentionally prohibits the MVPD's user interface, there is no MVPD UI for interacting with the MVPD's experience.

The Device Proposal proposes to reduce the MVPD UI to a small set of widgets. But the MMI or widget model envisioned is event driven from the MVPD side only. There is nothing that envisions a subscriber-initiated communication to the MVPD, such as upgrading or downgrading service, ordering technical assistance, subscriber profile changes, parental controls, or a subscriber paying a bill. The Device Proposal claims that HTML widgets are suitable for communicating with all backend systems, but nothing has been described that would assure that functionality across all systems. The proposal states that "display of widgets must be optional" so there is no guarantee that any MVPD or consumer interaction will occur. The UI is not some "monolith" overlaid as a "micro-service" on top of "content." It is integral to service. Most of the modern MVPD UI exists in a context that extends within and across video channels—such as saving a subscriber's viewing history for purposes of navigating back through his viewing history or making recommendations across devices. Even if an adequate number of widgets could be identified, such functions need to operate in context—which is why their functionality is integrated into full UIs.

With the loss of the MVPD's user interface, consumers do not receive a common familiar experience across devices—TVs, tablets, smartphones, and set-top boxes. Thus, the consumer must learn anew the navigation of an MVPD services for each different retail device they have purchased.

After this was pointed out, the Device Proponents added a vague suggestion that the MVPD's full UI could be presented to run on the device. But the proposal continues to eliminate the APIs and application platform to make that work; would require most elements of the UI to be rewritten into widgets, and the others to be exported to the web; and even then, the device manufacturer could block it.[63]

The Device Proposal fails to enforce requirements from content providers, including channel presentation in required neighborhoods (e.g., news channels) and channel assignments (e.g., broadcaster carriage on channel); channel logos; and search requirements (i.e., all shows accessed from a program network-branded folder).

Under the Device Proposal, third party devices could rearrange channel or program placement, insert different advertising into or on top of programs or use search functionalities to promote illegitimate content sources over legitimate ones. A user about to purchase an on-demand movie might be directed to a lower-cost pirate option. A programmer's title might be placed next to an X-rated offering, in violation of the programmer's carriage agreement. The retail device might also use search

[63] The amended proposal elaborates on a to-be-invented MMI (a subset of HTML5) as sufficient for all MVPD user interface purposes. The W3C has worked since 1994 to create a platform neutral Man Machine Interface, and HTML5 with the EME, MSE, and Web Crypto extensions is the only MMI that works across virtually all devices. Other efforts to create MMI systems are largely device specific. Android, iOS, and Tizen are among the few platforms that support a range of devices (TVs, tablets, smart phones, and smart watches), but they represent apps platforms in and of themselves. To assume the ready creation and sufficiency of a new widget-based MMI is wishful thinking.

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).

Recording Linear Content

The Device Proposal asserts that it supports local recording while VidiPath and RVU do not. That is mistaken. Both VidiPath and RVU present recordable outputs that are accessible by a third-party UI. The ability to record the video output from either a VidiPath or RVU server is controlled exclusively by the rights conveyed by the content protection system in use, either DTCP-IP or DRM. Nothing in VidiPath or RVU prohibits this recording. Output is in standard audio-video formats defined by DLNA. If the rights allow for recording the content, the device can record the content (provided they support the content protection system in use). Once the user has navigated to the content of interest on the client device, there is nothing that prevents the client device from recording the content provided the content rights allow it. Neither VidiPath nor RVU specify how this recording is to be performed or played back. The client device choses its method for implementing this functionality using its own UI outside of the RUI provided by either VidiPath or RVU.

The Device Proposal suggests unrestricted transfers of recorded content to mobile devices. There is no indication of an intention to respect restrictions by content providers on distribution generally or distribution to mobile devices.

The Device Proposal seeks access to an MVPD's network DVR. Network DVRs are implemented differently, according to rights and technology. MVPD's network DVR utilization is inextricably linked to the MVPD UI and to applications that encapsulate these differences. The Device Proposal has rejected both the UI and apps.

Remote Management by Consumer

The Device Proposal does not support remote management of tuning or of the account by a network-connected mobile device.

As detailed above, the Device Proposal does not support user-initiated management functions such as billing systems or a subscriber's ability to upgrade service from the screen.

Customer Support and Remote Management by Service Provider

The Device Proposal would leave MVPDs without important customer service tools. The proposal claims to offer an MMI channel for communications, but there is no continued presence on the device to support customer inquiry, no tools to know how service is being rendered on the device or to diagnose problems, and no tools for solving the customer's problem. After this was pointed out, the Device Proponents proposed that any service support be exported to an MVPD web service on the general Internet. This would require a redesign of service support and remove key elements of the UI and service support from the screen where it is most useful to consumers. Every major MVPD offers FAQs and online support for the delivery of their service (in its entirety) and as presented via their UI. Some even offer mechanisms to take control of CPE to obtain more technical detail and diagnostics. Increasing efforts to promote customer service and customer satisfaction is an imperative for MVPDs, but because there is no support for remote diagnostic service there is no assurance that the CE device will be a reliable platform for customer service. Customer support for an ongoing service differs from customer support for a device. For example, Google abandoned its first mobile phone because it was

unaccustomed to the retail service space. The Device Proposal fails to support MVPDs' efforts to assure quality of service in delivering video and to diagnose problems remotely.

Installation and Provisioning

Device Operation Requirements

User Authentication

The Device Proposal does not support these use cases.

Evaluation of Burden

Consumer Experience

The Device Proposal rejects the successful apps model developed in the market and widely adopted by consumers. As noted, the Device Proposal does not offer a method for delivering modern MVPD service as it is purchased by consumers.

The proponents of the Device Proposal have tried to characterize these features as optional or extraneous to the MVPDs' services, that the consumers who would use their retail devices would be happy to forgo. The MVPDs disagree, but however an individual customer values a particular feature, the MVPD business depends on its ongoing ability to rapidly make new features available to existing customers so that it can continuously strive to improve its service in a fast-evolving, competitive market. A customer that accesses only disaggregated portions of the MVPD's service under the Device Proposal would thus remain stuck in the past, potentially unaware of new distinctive differences in features, offerings, and look and feel of their MVPD's service. Application and feature updates are occurring multiple times a month, effected with an application update, as consumers have grown accustomed to on tablets and smartphones. The Device Proposal accepts only the raw linear and VOD that passes through its limited interface with no mechanism for updates or improvements.

Ordinary expectations—such as that parental controls entered into the MVPD UI will block programming on other connections in the home—will not be fulfilled. Each retail box needs to be independently programmed.

Cable operators are required to put their service phone numbers on every bill. But the Device Proposal will not enable customers to receive adequate troubleshooting, remote management, or technical support from their MVPD to fix service problems on their retail devices.

Development and Testing

The Device Proposal hypothesizes a Virtual Headend System that does not exist; invokes standards that are not implemented at all or and standards that are implemented only by some MVPDs; and calls for the rebuild of existing architectures. It negates the successful app development work that every one of the top 10 MVPDs undertook in response to demonstrable consumer demand. It removes APIs from devices and strips out applications that make service work. It instead calls for multiple new inventions, and the development of protocols, prosthetics, auxiliary devices, transcription and virtual headends in order to cover all architectures. Then comes the cost of implementing them, mapping them to existing systems, and transitioning to them over time.

The Device Proposal fails to offer essential procedures for testing and certification. Even after this was pointed out, the Device Proponents leave the matter "to be determined." Based on past experience, the effort necessary to create a functional and operating testing regime is a multi-year process. In the apps-based approach, extensive testing is performed on proprietary devices (e.g., iOS and Android), while DLNA has stood up multiple commercial test houses around the world to test VidiPath and RVU products to ensure conformance and interoperability for CE device consumers.

The Device Proponents have shifted massive burdens, costs, and losses onto service providers (and their customers). It would take years to develop the hundreds of protocols for use across all MVPDs,[64] and even then the protocols may not anticipate new services, features, or technologies for MVPD distribution. The claim is that this is needed to "keep the burden of implementation and licensing concerns minimal to a third party." But in fact, none of this is needed: an application-based system also keeps the burden of implementation and licensing concerns minimal to a third party, and does so while preserving innovation and competition.

Service Provider

The Device Proposal proposes limited interfaces that strip out key features of the MVPD service. Current or future features that are not carried across these interfaces cannot appear on the device. Service providers cannot present the service, and consumers cannot receive it, as they could with an updated app. The User Interface – which makes everything from promotional messages to StartOver to parental controls work – has been reduced to discrete *optional* popup widgets lacking any application support. Messaging and functions that cannot pass over a non-existent MMI must be abandoned. For example, under the Device Proposal, an MVPD could no longer offer a consumer the ability to instantly upgrade to add a channel through the guide, one of the most convenient and effective means for managing subscriptions.

The Device Proposal provides for no presentation of the brand identity of the MVPD's service.

Nor can MVPDs invent around the interfaces. The protocols are fixed, but business models and entitlements change rapidly. The proposal makes vague references to later "extensions of the interface protocols." Protocols freeze business models until you agree on exactly what rights are allowed and how to express them.

The Device Proposal also stymies innovation in content protection. It appears to require one single DRM (recommending PlayReady) for cloud to ground, rather than allowing competition and resulting improvement.[65] It also appears to require one link protection for the home (DTCP-IP), but DTCP-IP lacks the rich rights expression language expression featured in (ever evolving) DRMs. The Device Proposal offers no ability to support those models other than the ill-defined MMI, which does not enforce rights like expiration. Fixed protocols require long timeframes for standardization of each new feature, which

[64] 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.
[65] Major device makers, like Apple, do not support PlayReady.

is difficult given the variety and pace of change among video providers, technologies, platforms, services and features.

The Device Proposal also threatens to undermine the very security that is central to MVPD distribution systems by creating a single national point of attack at the interface.[66] There would be no choice in DRMs from the cloud, and no choice beyond a single link protection in the home. The proponents claim that an in-home gateway advertises services only on the managed IP network. But they refute that claim by calling for an SDV client that operates only over the open Internet.

The Device Proposal also proposes to define an entirely new Public Key Infrastructure (PKI) from scratch. This is a non-trivial exercise. The proposal mentions X.509 certificates, yet stops short of providing the critical and necessary details about how these certificates are managed, the required trust infrastructure (issuance, injection, protection, propagating revocation lists and requirements to query CRLs), and any policies necessary to make the certificates useful (profile, fields and information).[67] The amended proposal gives only a gesture to these many deficiencies, noting that revocation will need to be developed. Certificate revocation is one of the most challenging aspects of any public key infrastructure. It took DTLA, DOCSIS, and even CableCARD years to establish an appropriate PKI. Further, these PKIs are not static; it is necessary to continue to enhance these PKIs over time to address new and growing threat models.[68]

All significant burdens are asymmetrically imposed on service providers. The consumer devices do not need to implement any network-specific technology such as physical tuners, however non-IP MVPD operators must provide gateway devices that encapsulate their content into IP for transport within the home.

The Virtual Headend proposal also does not propose any method by which copy control information (CCI) or any other content usage rights are transmitted or implemented by or carried through to the downstream outputs of the retail device. And, as noted above, when using the CCI method, MVPDs would be frozen to very limited business models; EST, expiration date, or license restrictions on in-home or out-of-home distribution are not communicated with CCI.

---

[66] The section "Practical System Design Concerns" starting on page 193 of the amended proposal presents a new theoretical system proposal, not previously presented or discussed, rather than an analysis of the Device Proposal. The casual invocation of textbooks and a NIST reference is a far cry from designing and implementing a content protection system that protects content providers or their distributors.

[67] Nor has the Device Proposal included a functional approach to device authentication. It assumes the availability of an HTML-page for authentication in unidirectional systems, and a monthly renewal of temporary device certificates that would entail nontrivial engineering, operations, and bandwidth resources on DBS. Even after this was pointed out, the Device Proponents leave unidirectional systems to develop an undefined "offline" method to provide certificates by sideloading. It agrees that each MVPD will have unique operational requirements and needs, but offers no practical provision for how those needs would be met.

[68] The amended proposal compares its suggested PKI system as superior to "proprietary ones like in the MVPD UI proposal." The apps-based proposal does not specify a PKI.

The Device Proposal does not permit MVPDs to fulfill the many consumer protections (like statutory privacy requirements), "must carry" rules (like channel position and channel neighborhood), and other requirements built into regulated MVPD service.

The Device Proposal does not permit MVPDs to offer their services consistent with the content licenses and retransmission consent requirements under which they acquire distribution rights. For example, using native architectures or apps, MVPDs 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. They may assure that search returns do not place a programmer next to an X-rated offering. Under the Device Proposal, the MVPD cannot fulfill these requirements. The Device Proposal now acknowledges this lack of protection, but declines to advance a proposal that respects these licensing conditions. Instead, the proposal now suggests that all aspects of the numbering, grouping and presentation of channels be defined by FCC regulation rather than marketplace arrangements that reflect copyright license conditions, retransmission agreements, local laws and expectations, and an MVPD's own decisions about how to present services—decisions that are protected by the First Amendment.

Customer support is a necessary and large expense borne by an MVPD and passed along in its subscription costs to its customers. Consistency is a massively useful tool to control these costs and keep subscription fees low. The Device Proposal does not permit MVPDs to operate with such consistency.

The Device Proposal calls upon MVPDs to serve as delivery vehicles for raw video programming (and program guide metadata) from which Device Proponents may build their own services. MVPDs are not licensed by the content providers who own and license that copyrighted content to serve that role.

The same problem arises with the Device Proposal's requirement that program guide data be disassembled and delivered. MVPDs do not own guide data—they license it for limited uses from third parties. The Device Proponents agree that CableCARD only supplied minimal data and left it to the device manufacturers to license metadata from third party sources (e.g., Rovi and Tribune Media Service) and build their own guides. Under the applicable MOU, license and FCC rules, UDCPs only receive a virtual channel map and channel name, and only from cable operators. TiVo licenses data from third parties at its own expense for its guide. OCUR manufacturers like Hauppauge rely on Microsoft to do the same. Other vendors who license guide data to MVPDs do not even include the information sought in the Device Proposal.[69] Even VOD data comes with restrictions from rights holders, such as business and branding rules on search and search returns. The proponents offer no basis for ignoring these restrictions, only a vague claim to "assure the accuracy" in ways that have been unnecessary in the market. By contrast, apps that present MVPDs UI delivers all of this as the guide with the channels in their rightful location with all licensed material.

Content Providers

The Device Proposal does not assure that commercial channels appear in appropriate channel neighborhoods, that the Content Providers' brands are displayed in agreed upon locations, that programs are not overlaid with inappropriate ads, and that distributors respect license conditions that define permissible and impermissible uses and distribution. Content Providers' substantial investments

[69] For example, Gracenote, DISH's vendor for rich metadata, "has no plans to implement EIDR."

have built valuable and recognizable brands, which they license under carefully crafted arrangements to preserve their value and provide uniform nationwide presentation through licensed distributors. 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 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. 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 hardware 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.

The Device Proposal would also fail to support the interactive features used to enhance programming, or the advertising models that rely upon audience measurement and audit reports from the devices on which programming appears.

The Device Proposal fails to support the intellectual property rights underlying copyright licenses and that 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.

In addition, by failing to even support rich expression rights that are not enforced through CCI bits or link protection, the Device Proposal limits deployment of new business models under new rights models.

Such a system is unnecessary since content is readily available in the marketplace over a wide and growing array of devices and services, including over the Internet. Had such a system been imposed in 2010, it would have harmed consumers, content creators and service providers by mandating a one-size-fits all approach; ignoring the economic, technological, and competitive realities of the marketplace; and hindering the development of the myriad content, devices and services consumers enjoy today. Attempting to impose it again today would have the same result. It would also violate copyright and contract law, and potentially the First Amendment. Moreover, imposing such a system would impose costs and obligations on content and service providers that contradict the explicit statutory requirement that any solution not be "unduly burdensome."

Device Manufacturer

The Device Proposal is designed to “keep the burden of implementation and licensing concerns minimal to a third party.” It does so in three ways:

First, it assigns the burdens, costs, and losses to service providers, consumers, and content owners.

Second, it offers no commitment to operate within the actual trust infrastructure. In today's market, retail device makers negotiate with the content community over robustness and compliance, and operate under licenses and business-to-business agreements that assign additional responsibilities and liabilities. The Device Proposal would abandon this.

Third, it removes third parties from ordinary market dynamics: In today's market, Google (and others) pay content providers to include those providers' content in, for example, YouTube. This has created a great diversity of video options and experimentation in business models with compensation to content providers. Program networks and other content providers also enter into direct distribution contracts with CE device manufacturers (e.g., Apple and Sony), new video distributors (e.g., Netflix, Hulu and Amazon), non-traditional online packages (e.g., Sling TV), and offer 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. The Device Proposal would bypass this market by allowing the device manufacture to create a new retail service from the MVPD retail service, with no compensation to content owners or to the MVPDs that would be forced to design their networks and invent new support structures.

The amended proposal suggests that MVPD applications are at risk of being withdrawn, citing AT&T's sunset of an earlier X-Box app. AT&T continues to provide apps to X-Box.[70] Apps do evolve in response to changes in the market, as is evident from Google's sunset of YouTube apps on older devices.[71] However, the evidence demonstrates the continued expansion of MVPD apps in response to consumer and competitive demands.

Innovation

The FCC has previously acknowledged that regulation in this space "is perilous because regulations have the potential to stifle growth, innovation, and technical developments at a time when consumer demands, business plans, and technologies remain unknown, unformed or incomplete," and that it must therefore be wary of "fixing into law the current state of technology." [72]

The Device Proposal would do just that. The demands that the proposal would make on MVPDs would force MVPDs not only to lose the ability to deliver new and improved services to the customers who use retail devices, but would also force MVPDs to make changes to their overall networks that would impair their ability to innovate for all customers. Any changes made to any of the three interfaces described by the Device Proposal have to be coordinated across all MVPDs and retail device manufacturers, and presumably through regulatory processes. No mechanism has been included for updating supported codecs.[73] This necessarily slows innovation and advancements in service quality and/or features.

The Device Proposal further states that "Such [protocol based] architectures avoid the necessity to mandate and test detailed, internal operations of systems." Although well-written protocols can usually

[70] https://support.xbox.com/en-US/xbox-one/apps/att-uverse
[71] Google: Certain older YouTube apps will no longer be supported after April 2015, https://support.google.com/youtube/answer/6098135?p=yt_devicesupport&hl=en&rd=1
[72] *Commercial Availability of Navigation Devices,* CS Docket 97-80, First Report and Order, ¶¶ 15-16 (1998).
[73] The amended proposal states that the yet unspecified protocols will be extensible and new features can be added easily. The decade long transition from IPv4 to IPv6 demonstrates that specifying a protocol does not make it necessarily readily extensible.

hide the internal operations of systems, this simplification of real-world experiences has three major problems, all affecting the means by which interoperability would be maintained and the impact on innovation.

First, protocol validation and tests for correct implementation of protocols across multiple classes of devices (servers and clients) has historically proven to be a significant effort involving either massive coordination and co-location of many companies in an interoperability "plugfest" (e.g. UPnP), or purpose-built validation test suites that lead to certification (e.g. CableCARD and DLNA validation and certification). Given the geographic restrictions on many MVPD services, simple independent plugfests that invite all MVPDs and all likely device manufacturers seem to be impossible. The cost and complexity of developing and administering test suites for particular protocols is typically managed and paid for by an organization such as CableLabs or DLNA. The Device Proposal neither identifies nor proposes formation of such an organization.

Second, when problems are found in either protocols or in specific implementations of protocols, changes to existing devices and systems are required. Coordination of changes to deployed devices is a significant task for each MVPD working within its own, entirely managed system. Coordination of changes across multiple MVPDs with asynchronous update practices, plus across fielded and still-on-the-shelf devices, plus next-year-model devices is a necessary function where the Device Proposal is silent.

Third, the retail device marketplace is a highly competitive environment. Some devices may be released with a focus on particular MVPD systems or architectures. If problems are found in a particular retail device's protocol implementation after that device is present in significant quantities in the market, the Device Proposal is silent on how any particular manufacturer should be expected (or required) to support necessary changes to already-sold and revenue-neutral devices. For example, a retail device that works across all cable systems but fails to interoperate with the particular features of a DBS transport stream or IPTV system may be a commercial success, but would not be interoperable or portable.

Recent history confirms the risk that technology mandates like those in the Device Proposal will rapidly become obsolete. In 2003, the FCC tried to create a uniform national digital video technology with CableCARD, but instead the market expanded well beyond cable, then embraced apps and other diverse solutions. One percent (1%) of today's 52 million CableCARDs are used in the retail devices for which they were originally intended. Over its entire 15 year lifespan, there have been only two major changes in CableCARD—multistream and support for SDV Tuning Adapters. And, even these came with time-consuming, significant re-engineering and high cost. In 2010, some consumer electronics interests proposed that the FCC adopt rules for a uniform "AllVid" successor to CableCARD. Had the FCC adopted the "AllVid" rules, the distributor and programming industries could not have developed today's amazing market that provides MVPD programming to smartphones, tablets and other devices embraced by consumers.

Interposing standards of the sort contemplated by the Device Proposal imposes a significant cost in lost innovation. There is considerable economic and academic literature documenting that the risks of non-market failure and the costs to innovation are particular high when the government intervenes in new markets that are rapidly evolving—such as we have in the converging communications, media, and IT industries today. Besen and Johnson's seminal 1986 study concludes: "[T]he government should refrain

from attempting to mandate or evaluate standards when the technologies themselves are subject to rapid change."[74]

Premature government standardization reduces competition, experimentation, and creativity, thereby limiting options for consumers. The need to adhere to a standard limits firms' product design choices and ability to invest in new technological approaches. The loss of innovation and variety that can be the result of standardization is a loss to consumers. If such a government-mandated standard is imposed, it risks locking consumers into obsolete and/or inferior products. NCTA has previously provided the FCC with a detailed study of the video devices market by respected economists which explains this very phenomenon in the video space.[75]

MVPDs need flexibility to use diverse solutions that can adapt their particular networks to rapid changes in technology, competition, cybersecurity needs, energy efficiency, and consumer demand. Effective service delivery would be paralyzed if FCC waivers were needed every time an MVPD or manufacturer sought to innovate.

Competition

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%. AT&T/DirecTV, Dish, and Verizon are the first, third, and fourth 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). 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.

Video distributors operate as differentiated retailers who implement a variety of technologies, compile bundles of programming, guides, navigation features, applications and other inputs into distinctive, branded offerings. Video distributors compete with each other by using different technologies. Verizon devoted an entire fiber wavelength to its linear video offering and transitioned to all-digital. AT&T launched its U-verse service designed 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. Features like instant channel change and multi-room DVR enabled AT&T to better compete against incumbent cable operators, despite limitations of VDSL networks. Remote Storage DVR enabled Cablevision to compete against multi-room DVR features. Video providers further 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

[74] "Compatibility Standards, Competition, and Innovation in the Broadcasting Industry," Stanley Besen and Leland Johnson, Rand, Prepared for the National Science Foundation, November 1986, at 135.

[75] Ex Parte Submission of Economic Analysis of the Regulation of MVPD Navigation Devices in Video Device Competition Notice of Inquiry (MB Docket No. 10-91, CS Docket No. 97-80, PP Docket No. 00-67), July 19, 2010, http://apps.fcc.gov/ecfs/document/view?id=7020549667

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. Each innovation by one provider spurs competitive responses by others in the market. The Device Proposal would strip away the very features and innovations with which MVPDs compete. Consumers would not even be aware of the enhancements—because the devices will not pass them through in apps. The Device Proposal would sacrifice the competition that has driven enhanced services to the benefit of consumers.

The Device Proposal would deny MVPDs the flexibility to innovate while over-the-top video providers would remain unconstrained in the services they provide. Such an approach is contrary to the Commission's well-established policy to favor a "regulatory regime that is technology and competitively neutral" and would create a competitive burden on MVPDs contrary to the technology- and platform-neutrality required by STELAR. Singling out only MVPDs with a different mandate would also create the same competitive disparities that undermined the cable-centric CableCARD regime.

Conclusion

The Device Proposal concludes that it retains the intended functionality of MVPD service and provides the same service as MVPD apps. As demonstrated above, it fails on both counts. Instead, it discards those services and features that do not fit through the stripped-down interfaces and the proposed architecture of the Device Proposal.

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.

Passage to Facilitate Transition to All DRM Approach

Sony's Passage™ technology is a simple, elegant solution that allows multiple security systems to co-exist on legacy digital CATV networks. It is suitable for broadcast linear streams where a service provider supports simultaneous distribution to receivers with legacy Conditional Access (CA) and new security such as Digital Rights Management (DRM).

Passage technology use of selective multiple encryption (SME) is based on a fundamental understanding of MPEG compression and how compression may be used as a form of encryption. Not all of the content needs to be scrambled by the security system – only that which is needed to decompress the rest of the content. Most of the compressed, hard-to-recover, content can be sent in-the-clear!

Passage facilitates a transition to an all DRM system where a DRM may be loaded into client devices and use the standardized HTML 5 Encrypted Media Extension (EME) abstraction layer. Use of DRM can also be compatible with the RVU and VidiPath proposals. The same DRM system used to encrypt the MVPD's web services may be used to encrypt linear content. And this can facilitate delivery of entitlements to client devices that comprehensively covers both linear and web content, instead of supporting parallel security systems - legacy CAS, for linear content, and DRM, for web services. All of the content could be delivered and managed using DRM (with support for legacy CAS with linear content).

Passage is efficient. With Passage technology, the customer experiences no degradation of existing services. A typical Passage system requires between .2-2% additional bandwidth to deliver the same content and services including the new, second security system. This means that Passage can be introduced in a system without changes to the existing channel line-up.

As shown in Figure 41, End-to-End DRM can facilitate the reception of linear content either through direct-attach or network attach means. It enables a larger number of devices, especially smaller form-factor mobile ones, to receive content that would otherwise be reserved for set-top boxes. If a gateway is assumed, content may be transcripted from DRM to DTCP link protection or pass-through AS IS with DRM encryption to home network devices. Persistent DRM control may allow for a wider variety of use cases that could be otherwise permitted using Copy Control Information (CCI) bits delivered with DTCP or across the CableCARD interface using DFAST.

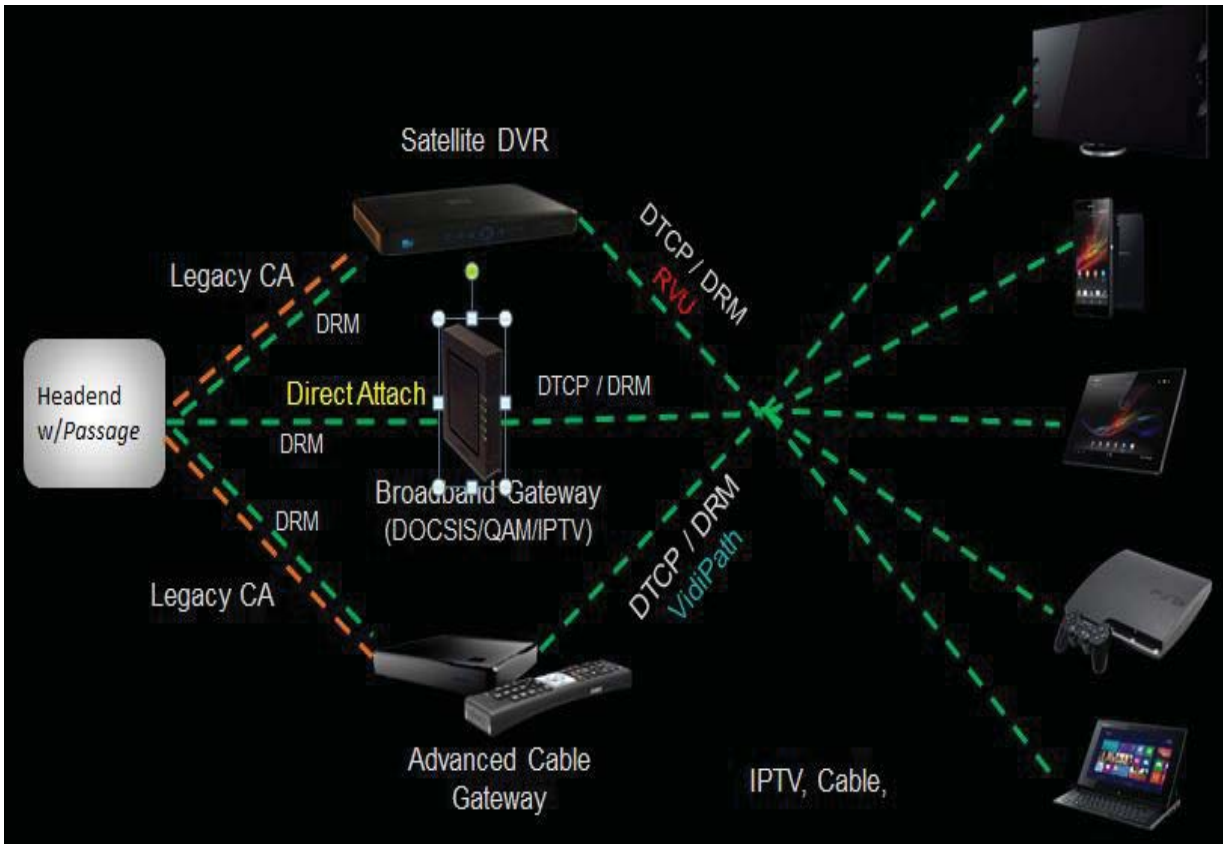


Figure 41- Use of Passage to Enable End-to-End DRM

Implementation

Passage is proven technology. There have been a number of field and lab trials as well as deployments with the Cisco CA Overlay system. A description of the steps needed to Passage encode a stream is described in Part II of this document.

The best way to deploy Passage is at the point of commercial distribution. All the MVPD receive their content one of 3 ways – Broadband/Satellite delivery, Programmer delivery, or locally. If the companies, offering Broadband/Satellite delivery or Programmer delivery, Passage encoded their commercial streams, MVPDs downstream would not require any new equipment. A stream would be processed in one place, and then distributed throughout the US. There are 4 or 5 different headend configurations and they all can be accommodated by reconfiguring their existing equipment. And non-participating headends, perhaps exempted from any FCC regulation, won't need to opt-out - they won't need to do anything. Participating headends will only require normal functions of existing equipment – stream groomers and multiplexers - with normal features such PID filtering, PID remapping, and descrambling and re-scrambling. Local content is the only content that would require local Passage encoding.

Passage hardware components are implemented in both the headend and in every Passage-enabled set-top box, with the latter available from a variety of participating manufacturers. The following components are implemented as part of the Passage-enabled system.

- Headend encoder

- Device (decoder)
- Alternate security system encryption

Contact Information

E-mail: Brant.Candelore@am.sony.com

Policy Analysis by Content Providers

Many members of the DSTAC continue to object to the scope of certain aspects of this report. Congress created the DSTAC to examine downloadable security systems. Indeed, as highlighted in a June 18 letter from Reps. Latta and Green to Chairman Wheeler, section 106(d) of STELAR gave the working group nine months from enactment "to identify, report, and recommend performance objectives, technical capabilities, and technical standards of a not unduly burdensome, uniform, and technology- and platform-neutral software-based downloadable security system designed to promote the competitive availability of navigation devices in furtherance of section 629 of the Communications Act of 1934." Some parties would like the DSTAC to go beyond its statutory mandate and design a system that forces video providers to allow third-parties to disassemble the programming, features, and functions of the video service so that the third-parties can selectively reassemble parts of them for their own commercial exploitation.

This is similar to the 2010 "AllVid" proposal the FCC abandoned in the face of widespread opposition by content creators; cable, satellite, and IPTV distributors; and others. Such a system is unnecessary since content is readily available in the marketplace over a wide and growing array of devices and services, including over the Internet. Had such a system been imposed in 2010, it would have harmed consumers, content creators and service providers by mandating a one-size-fits all approach; ignoring the economic, technological, and competitive realities of the marketplace; and hindering the development of the myriad content, devices and services consumers enjoy today. Attempting to impose it again today would have the same result. It would also violate copyright and contract law, and potentially the First Amendment. Moreover, imposing such a system would impose costs and obligations on content and service providers that contradict the explicit statutory requirement that any solution not be "unduly burdensome."

We participate, nonetheless, in the hopes of fulfilling the DSTAC's actual mission of promoting a downloadable security system; to protect the interests of consumers, content creators, and service providers from those who wish to disaggregate content, features, and functions for their own pecuniary gain; to ensure the report reflects our statutory, policy, and legal concerns over the AllVid-type proposals; and to make sure that any such proposals at least provide consumers access to all the features and functions currently available. If parties wish to offer a narrow or specialized subset of features and functions, they should do so through individualized negotiations in the marketplace, not through regulatory fiat.

Summary of Objections Stated Within the Policy Analysis

Our overall objections are that: 1) the working group assignment goes beyond the DSTAC statutory mandate, 2) that the marketplace for MVPD and OTT services is flourishing, calling into question the need to impose an AllVid like mandate, 3) that doing so will harm consumers, content creators, and service providers, and 4) that some of the proposals would violate copyright and contract law.

Evaluation of Both Proposals by Proponents of "Competitive Navigation" Proposal

Fundamentally, the "MVPD" App proposal does not allow for a competitive user interface and, instead, seeks to lock consumers into having an operator-*mandated* user interface as the only way to discover, browse, select, record and view content. No resource is made available to a third party device to perform such functions. Hence no competitor can field a device that is comparable to the operator's own. This is anathema to the entire purpose of Section 629 of the Communications Act, which is to assure that there is a market for competitive navigation devices.[78]

As described in the Response to Evaluation of CE Device Competitive Navigation System Proposal by Proponents of Application-Based Service, the "MVPD" app approach not only forecloses use of a competitive interface; it also locks in the *status quo* of operator control by eliminating the degree of interoperability and choice assured by the CableCARD interface, impaired as it has been by existing licenses, contractual restrictions, and failures to update the technology. Unlike CableCARD, the interfaces required by the MVPD App proposal offer to consumers none of these assurances:

- An assurance that her device will be authorized by the operator for their mandated user interface. The MVPD can withdraw support for the app for any reason at any time.[79]
- An assurance that her device will operate portably across similar systems.
- An assurance that her personal recordings, viewing preferences, account associations, parental control settings and other components of the user experience will be portable across operators. Because the MVPD owns the entire experience, all of these preferences remain in the control of the MVPD.
- An assurance that recommendations are according to her personal preferences rather than the MVPD's economic interest. Only an competitive third party user experience has the ability to work independently of the economic interests that content owners can enforce on MVPDs with respect to promotions through "recommendations."
- An assurance that there will *ever* be an "app" that will work interoperably across systems. Rather, operators will be assured that devices do *not* become an instrument to empower consumers to choose among MVPD offers on a competitive basis.

---

[78] Consumers' desire for better alternatives to MVPD supplied interfaces is well established. *See, e.g.*, John Patrick Pullen, *America's Most Hated Device: The Cable Box*, Aug. 27, 2013, *at* **http://tech.fortune.cnn.com/2013/08/27/americas-most-hated-device-cable-box/.** The limitations on competition inherent in the MVPD App proposal can only enlarge and entrench this circumstance.

[79] AT&T U-verse had advertised its app on X-Box as an inducement for customers to sign-up for its service and later abruptly announced that it would terminate support for its app on the Xbox 360 service. *See* Jeff Baumgartner, *AT&T U-verse TV To Drop Support For Xbox 360 on December 31*, Nov. 26, 2013, *at* **http://www.multichannel.com/distribution/att-u-verse-tv-drop-support-xbox-360-december-31/146904.**

A Comparison of WG4 Proposed Systems

Two systems have been proposed in Part III of this document, each highlighting issues that should be addressed and appropriately balanced in the distribution of paid video programming with and without competitive retail navigation devices.

These system proposals emphasize, and are consistent on, several key points:

- Content should be protected against piracy and other illegal uses.
    - As such, detailed content usage restrictions (e.g. CCI) should be appropriately addressed or addressable via given systems without unduly restricting end-user consumption capabilities.
- Various operator network technologies must be abstracted and uniformly addressable via these systems, including unidirectional distribution networks (e.g. Satellite).
- Because formats and network architectures are evolving, systems and protocols should be tolerant to changes in delivery networks to provide service continuity and consumer confidence in retail device compatibility.
- Basic metadata for navigation is fundamental to network-based experiments
- Rich metadata, either from the MVPD or at least with the ability to align with independently-sourced rich metadata is critical to enabling modern content consumption experiences.
- Regulatory concerns (e.g. EAS) must be considered.
- Commercial considerations (e.g. billing notification) should be addressed, where possible.

Though the two proposals differ on elements such as enabling choice in competitive user interfaces, large elements of the proposed systems align architecturally. As described below however, where the systems differ manifests in the user experiences allowed due to design elements controlling capabilities independent of downloadable content security.

Description of Part III Section I proposal

Part III: Section I describes a “Competitive Navigation” System enabling competitive navigation devices with access to MVPD content. This system emphasizes necessary structural elements within a “Provider Interface”, and it focuses on description of the elements necessary for an Internet-Protocol-backed protocol-based interoperable mechanism.

In particular it describes three extensible interfaces, based on Internet standards, called the Service Discovery Interface, the Content Delivery Interface, and the Entitlement Information Interface. These Provider Interfaces could be offered by each MVPD alongside their own application based solution. The interfaces provide the following to competitive navigation devices over the user’s home network:

- information on video services available to the consumer and devices
- access to content over a common network interface
- entitlement and usage rights information of the available services

Description of Part III Section II proposal

Part III: Section II. describes an "Application-Based Service with Operator Provided User-Interface" System. This proposal suggests the implementation of six sub-proposals consisting of existing technology. The most obvious common feature of these sub-proposals is the requirement of control of the navigation user interface by MVPDs, even on competitive devices.

The sub-proposals highlighted in the Part III Section II proposal are:

- An application framework for Device Specific Apps (e.g. iOS, Android, Samsung Smart TV, LG WebOS, Xbox, PlayStation, Roku)
- HTML5 Web Browser that may support MVPD Apps
- DLNA VidiPath Client platform (but not allowed to be server with independent UI for MVPD services)
- RVU Client platform
- DISH Virtual Joey
- Sling Media Technology Clients

The first, use of *Device Specific Apps*, is naturally open-ended, but will be discussed below.

Two more of these, *DISH Virtual Joey* and *Sling Media Technology Clients*, are closed and proprietary, providing difficulty in technical analysis and, by definition, competitive interoperability. Nonetheless, elements of their design will be discussed

The remaining three sub-proposals (*HTML5 Web Browser*, *DLNA VidiPath*, and *RVU Client*) are similar in their approaches to user-interface presentation (i.e. operator controlled HTML) but vary in downstream link protection and network topology.

Evaluation of CE Device "Competitive Navigation" System Proposal

Unlike the MVPD UI Application-Based Service proposal, the CE Device "Competitive Navigation" System Proposal (henceforth the "Competitive" proposal) offers consumers choice in competitive user navigation experiences. It enables a competitive landscape by allowing both an MVPD UI Application, and a competitive alternative UI option to consumers. Without this choice, consumers would have nothing more than the current status quo of a fragmented MVPD application space, where some MVPDs offer applications on some devices, without the advantage of a competitive UI option that CableCARD provides. If a reduction in the status quo were sufficient, Congress would not have directed the FCC to establish the DSTAC and would have repealed Section 629.

While the MVPD UI proposal mandates only the MVPD's UI via their proprietary application, the competitive proposal provides an alternative option, which meets the requirements for competitive navigation devices. The Competitive proposal does not prohibit competitive app-based solutions from the MVPD directly, thus giving consumers both options.

The Competitive proposal identifies a system comprising minimum standards, protocols, and information to enable competitive availability of devices that receive MVPD services in accordance with

Section 629 of the Communications Act. The "MVPD" app proposal, by contrast, does not afford competitive availability of devices as that goal has been understood to date, and would lock consumers into having their video consumption experience framed and controlled entirely by the MVPD. That proposal provides for an operator-*mandated* user interface as the only way to discover, browse, select, record and view content. The navigation device is given no resource to perform those functions on its own, and therefore by definition is not a competitive navigation device compared to one provided by the MVPD themselves.

The premises upon which a competitive environment for navigation devices and user interfaces can and should rest are:

- A recommendation for the identification and development of standards to further the objectives of Section 629 need neither limit nor rely upon the existence and development of any MVPD-provided UI. Hence, the Competitive proposal, *while not conceding that an MVPD's UI is "integral to the service," does not rule out its availability to a user in a device with a competitive UI.*
- Nothing in legislation, FCC regulation, or market practice today refers to an MVPD's suite of programming and services as an *indivisible bundle, aggregate, or "service."* The "MVPD" analysis recognizes this in portions in which it refers to MVPD support for "apps" that provide partial or limited access to MVPD offerings.
- Nothing in the Competitive proposal addresses whether *FCC regulations* would or would not require, e.g., the numbering, grouping or presentation of channels, or other matters of concern to an MVPD and / or content provider. The proposal is made in the context of a TAC process and DSTAC recommendation of "performance objectives, technical capabilities, and technical standards … to promote the competitive availability of navigation devices …."
- That the ability of a consumer to choose among MVPDs, geographically or on a competitive basis, will be a consideration for the Commission in evaluating DSTAC recommendations.

The history of innovation in this space, however, shows the advantage of a competitive enabler like CableCARD: The significant innovations in empowering consumers with abilities to control access to content have come from third parties. The success of these third party innovations has been constrained only, and significantly, by an ongoing inability to effectively integrate them with MVPD programming and services on any competitive basis. Innovation thus has occurred despite, rather than because of, MVPD initiative. Consumers will gain, not lose, from an environment in which such innovation is enabled rather than frustrated. Examples:

DVR – Pioneered by ReplayTV and Tivo with products launched in 1999, this is one of the most widely loved technologies by consumers and was truly innovative. This was a technology developed by third parties, with no involvement from MVPDs. This third party innovation became fundamental to every MVPD's conception of its "service," yet owes nothing to any concept or application of service "aggregation." The only "disaggregation" that occurred was when MVPDs moved to HDTV transmission without providing for competitive access to the digital program stream, until obliged by legislation and regulation to offer the CableCARD interface.

Whole Home Media w/ DVR – Pioneered by SageTV and integrated into its products in 2003; this was the first product that afforded user access to all household media content, including DVR recordings from any TV. This technology was built on top of a PC platform without any involvement from MVPDs. Similar technologies are now standard in most MVPDs systems, as many have evolved to a client/server model with DVR storage all occurring on a central device in the home and client devices existing at the TVs. This third party innovation is a parent of VidiPath, RVU and other 'gateway' approaches now purportedly "integral" to MVPD "services." VidiPath employs a technology similar to the SageTV Client solution released in 2003; RVU employs a technology similar to the SageTV Media Extender technology released in 2005.

Remote Viewing – Pioneered by Slingbox in 2005; the first to allow users to view live TV and DVR content from anywhere they choose. It freed viewers from having to be at home to see their content, and allowed them to stream it to parts of the home away from the main set top box (before MVPDs starting offering whole home media solutions). This technology was extended to support smart phone and tablets once those became available in the consumer market. This third party innovation is now also said to be "integral" to an MVPD's "service" *if* (and only if) provided via the MVPD's UI or a licensed app.

Remote DVR Management – Released by SageTV in 2005 as a webserver plugin for SageTV Media Center; this innovation allowed consumers to schedule recordings from anywhere at any time, through the use of a web browser (which became even more accessible with the advent of smart phones & tablets). Again, this was built on top of a 3rd party system that integrated on top of the essential MVPD video services with no assistance from MVPDs. This innovation is now a standard feature in many of the MVPD 'apps'.

Not every third party innovation is successful or available to consumers, because they cannot be integrated into an MVPD service on a competitive basis. A vast number of innovations remain unavailable to most consumers (e.g., plugins for products like MythTV, SageTV, MediaPortal, XBMC, etc.). The main reason for this is the lack of the ability to make a product that can actually do well in the retail market. Currently, it is impossible to make any kind of cost effective retail device that interoperates in an HDTV environment with all the different MVPD service offerings. Implementation of the Competitive Navigation Device proposal would allow such innovations to reach a competitive market. Shutting the door on such innovation would put an end to it.

While CableCARDs were limited to one-way function by MVPDs as a license condition[80] rather than a technical requirement, and were hampered by poor support from Cable operators[81], the competitive

[80] The cable industry itself promoted and licensed a "tru2-way" implementation relying on the same CableCARDs, purportedly to support competitive devices but saddled with additional license restrictions

[81] Criticism of the extent and quality of cable industry support for CableCARD-reliant retail devices has been repeatedly acknowledged in FCC and judicial records, including by the FCC itself and the Court of Appeals. *See, e.g., In the Matter of Implementation of Section 304 of the Telecommunications Act of 1996, Commercial Availability of Navigation Devices*, CS Dkt. No. 97-80, Second Report and Order ¶ 39 & n.162 (Mar. 17, 2005); Federal

proposal would enable third party devices and unique user interfaces to present two-way services. Despite baseless assertions that competitive guides were always meant to be "transitional" features or that CableCards (hence *all* competitive devices) were designed as inherently "one way," the Competitive proposal enables the intent to create a competitive market for two-way navigation devices. Such devices will have access to the services the customer has paid for, including traditional services such as linear television, Video On Demand, and Pay Per View, and new services such as "cloud" DVR and out-of-home viewing. Separating the MVPD user interface from these services will foster innovation in their usage, just as CableCARD devices brought several new innovations to Cable.

The MVPD UI proposal also appears to be limited to existing standards and tries to define application environments which do not meet all of the requirements of a future looking solution. Being limited to existing standards could freeze innovation into those existing standards. There is no reason to cabin DSTAC recommendations so as to reflect only the status quo. The references to technical standards in FCC regulations have accounted for progress as reflected in standards, and can so account when recommendations are reflected in references. The Competitive proposal includes extensible protocols that allow both MVPDs and Competitive device manufactures to add new features without having to do the difficult task of changing the application environment. There is no requirement or even recommendation for an application execution environment. On the contrary, the competitive proposal points out that previous application execution environments for pay television such as OCAP [23] and DVB-MHP [22] were failures because of both the technical complexity and competitive restrictions they placed on navigation devices.

Additionally, the Competitive proposal gives the consumer the ability to (1) move a purchased device to a territory served by another cable operator, or (2) choose to change MVPD providers, or to access video programming and services from more than one provider. The MVPD UI proposal, by contrast, could remove this consumer benefit as enjoyed by CableCARD device purchasers today. Unlike with CableCARD, under the MVPD proposal the consumer gets none of the following assurances in her decision to purchase a navigation device instead of obtaining one directly from the MVPD:

- An assurance that her device will be authorized by the operator for their mandated user interface. The MVPD can withdraw support for the app for any reason at any time.
- An assurance that her device will be portable across operators.
- An assurance that her personal recordings, viewing preferences, account associations, parental control settings and other components of the user experience on the device will be portable across operators. Because the MVPD owns the entire experience, all of these preferences remain in the control of the MVPD.

Communications Commission, Connecting America: The National Broadband Plan § 4.2 at 52" ([C]onsumers who buy retail set-top boxes can encounter more installation and support costs and hassles than those who lease set-top boxes from their cable operators."); *Charter Communications v. FCC,* 460 F.3d 31, 40-44 & n.10 (D.C. Cir. 2006).

- An assurance that recommendations are in her personal preferences rather than the MVPD's economic interest. Only an independent, third party user experience has the ability to work independently of the economic interests that content owners can enforce on MVPDs with respect to promotions through "recommendations."

The Competitive proposal leverages the existing dominant usage of HTTP as the modern method for delivering uni-cast video content. YouTube, Apple TV, Netflix, Sling.tv and millions of other content platforms on the Internet use HTTP as transport of video and metadata and not web pages and web apps. It does not relay on outdated technology such as silicon key ladders, DOSCIS cable modems, low-noise block downconverters (LNB), etc.

Like the CableCARD specification, the Competitive proposal defines protocols but intentionally leaves implementation details of navigation up to the implementer. This is consistent with many layer protocols that define Internet web services. For example Hypertext and hyperlinks, the basis for modern web browsing, are intentionally defined separately from the browser or other technology that navigates them to allow both sides of the interface to be flexible. Defining implementation like in an App-only approach would limit both the cable operator and the device manufacturer.

The competitive model describes a Man Machine Interface (MMI) that does offer a predictive execution environment for the MVPD to create "widgets" that may be needed for implementation of certain features (such as PPV/VOD purchasing, VOD playback including LookBack and StartOver, service upgrades, billing, support relating to the MVPDs service, caller ID, sports scores, etc.) without requiring the added complexity of requiring an execution environment for content delivery. HTML5 with various extensions is clearly a choice many parties are agreeing on for user interaction (as opposed to the prevalent use of HTTP and not HTML5 for content delivery). While the consumer could choose to use a MVPD provided app that reflects the entire MVPD UI (similar to VidiPath), in order to enable competitive navigation UIs they would simply also need to offer subsets of that same UI that reflect the various widget components mentioned above.

The competitive proposal strikes the proper balance of implementing an execution environment for what it is good at, without requiring it for access to content, and therefore restricting or preventing a competitive UI. Through this correct balanced use of an execution environment, competitive devices would have the freedom to innovate on the UI and then utilize the widgets in the contexts where they are needed to interface with the particulars of a given MVPDs service. Mandating an execution environment for the MVPD application as the only platform for access to service would only limit innovation and the marketplace.

The basis of competition is differentiation and choice. Not every feature available from one product would be available in every competitor. The market will decide which set of features it prefers. The MVPD UI proposal does not give the user a choice in the feature set. The Competitive model allows the MVPD to enable features in both their own application and in the competitive interface if they choose. For example in their presentations operators listed several features that are part of their user interface application. U-Verse noted it has implemented fast channel change within its application. In the

competitive proposal U-Verse can also offer that service in its implementation of the Content Delivery Interface; U-Verse would implement fast channel change in the interface itself. The competitive device would request a channel, and the U-Verse interface implementation would perform whatever proprietary protocol is required for fast channel change. U-Verse would do the same in a VidiPath or App-model approach. In both proposals the receiving device does not implement fast channel change, but it is still available to all navigation devices. The same applies to features such as advertising insertion, telescoped ads, switched digital channels, and many more that are network or system specific features. In addition, the abstraction (not stripping as claimed) from network specific technologies that both proposals use gives MVPDs more freedom to make changes to their network technologies. Vidipath clients, for example, would make the same request for a channel change regardless of how U-Verse implements fast channel change. If they change that technology, the clients would not need to change.

Additional features maybe not thought of yet could be covered by the HTML5 widget model in the MMI explained above. The competitive proposal included interactive enhancements and MVPD-unique elements via the MMI. Interactive enhancements from the MVPD can easily be achieved by the MMI widget model. Beyond that, the implementer's competitive navigation devices will be able to create their own interactive enhancements that to date have lacked any vehicle for delivery to consumers. Final specifications may include methodologies for phasing out obsolete technologies over time and use extensible technologies for expansion of future capabilities.

As noted, the Competitive proposal describes interfaces based on extensible web protocols, the basis for most Internet services which have proven they support rapid innovation. In the competitive proposal services can be enhanced and new ones added without constraining the client device into running a complete MVPD UI. Extensible protocols such as XML allow client devices to ignore elements they don't support (or choose not to support) and thus new features can be added easily. The Internet has been built on such extensible technologies. The standards, protocols, APIs, and interfaces that will eventually be finalized for allowing creation of a competitive navigation device should also include extensible technologies as well where relevant.

While the MVPD UI proposal lists many different DRM and copy protection systems, without indicating which would guarantee access to content, the Competitive proposal recommends DTCP-2 which is in development and would satisfy both the CCI and format requirements of modern business models. Consumer device manufactures that implement and meet the licensing requirements of DTLA would have assurance that their devices would be able to receive encrypted content.

The competitive proposal includes content protection models similar to the content distribution and DRM/CAS solutions presented in the MVPDs App model proposal. They both focus on IP delivery of content, either from 'cloud to ground' or from an in home gateway device. The competitive proposal is an extension of technologies the MVPDs have already deployed and/or have presented to the FCC. None of this requires any radical re-architecting of networks because it involves software protocols from either the Cloud or in-home gateways, and not network hardware.

Network-sourced ad insertion is the norm for both traditional MVPDs and OVDs. YouTube for example uses network-sourced ad insertion exclusively and not local insertion. Local insertion by the client is extremely rare, primarily in limited one-way systems as noted in the DBS section. Ad insertion for VOD (or any other content played back from an MVPD source directly, such as live linear TV, LookBack, StartOver, cloud recorded DVR) is almost entirely network-sourced today. In the competitive proposal MVPDs can implement novel interactive advertising models such as telescoping ads using an HTML 5 playback widget that would have full control over ad insertion and audience measurement. This does not need to apply to recorded DVR content because for a retail DVR device built on this kind of system, if the content is played back after being recorded, it is then under the user's full control and should not be subject to any service management by the MVPD. The competitive proposal supports delivery of content over IP in the same manner of most OVD solutions, which means advertising (pre, post and interstitial) is inserted in the network by manipulating the playlist of adaptive bitrate technologies such as HLS. This is how the vast majority of content is delivered and multiple advertising models are supported today on the Internet.

Both MVPD user interfaces and Competitive navigation devices based on CableCARD provide tools to customers to block potentially objectionable content in a variety of ways by using the parental control information delivered on the Cable plant and abstracted by the CableCARD. In the competitive proposal, navigation devices can continue to innovate on such features in the user interface to give consumers more choice in managing potentially offensive content. Users would not benefit from this innovation under the MVPD-app only proposal.

The Competitive Proposal proposes the use of Public Key Infrastructure (PKI) certificates. As was noted in the presentation to WG3 by NDS (Cisco), legacy conditional access systems used symmetric security keys which made it very important that keys be kept secret and thus a non-trivial exercise to set-up and share keys between vendors. PKI systems are based on asymmetric keys which are designed to allow keys to be shared and even openly published without compromising security. PKI systems are also pervasive in secure web services from electronic banking to secure email. Public source code exists and is believed to increase security by allowing both hackers and defenders to continuous test the code against threats. Using a PKI system over proprietary ones like in the MVPD UI proposal may be significantly simpler for device manufactures to implement.

Practical System Design Concerns

To frame a comparison of these proposals, it is worth examining common architectural elements and features of video distribution networks. In order to manage service entitlements, MVPD networks have evolved from mere filtering and scrambling to cryptographic protection mechanisms leveraging management facilities enabled by chains of cryptographic trust. Examination of system architectures and design elements in furtherance of the DSTAC's mission to "…promote the competitive availability of navigation devices…" follows.

47 USC 629 (b) states "***Protection of System Security**: The Commission shall not prescribe regulations under subsection (a) which would jeopardize security of multichannel video programming and other services offered over multichannel video programming systems, or impede the legal rights of a provider of such services to prevent theft of service."*

From this, the DSTAC can take assurance that any proposed system must fundamentally protect multichannel video programming against theft of service and may not jeopardize security. Adherence to best practices is fundamental to the design of secure systems. Listings of accepted industry-standard guidelines can be found at owasp.org[82], in *Writing Secure Code* by David LeBlanc and Michael Howard[83], or in *Engineering Principles for Information Technology Security (A Baseline for Achieving Security), Revision A*[84], published by the *National Institute of Standards and Technology*. For clarity, secure engineering principles in this writing will reference NIST documentation.

Additionally, content distribution networks can be readily mapped to the Open Systems Interconnection (OSI) model[85] (ISO/IEC 7498-1). The following analysis leverages this conceptual model for description of underlying communications technologies, and readers unfamiliar with the OSI model are encouraged to read either the standard or a summary (e.g. https://en.wikipedia.org/wiki/OSI_model).

In addition to consideration of fundamental secure system design principles, any system designed to facilitate MVPD service integration per the DSTAC's mission must remain "…uniform and technology- and platform-neutral…" Due to this guidance, any system or protocol design calling for integration of proprietary or service-specific technology is, necessarily, outside of the scope of the DSTAC. Such service-specific technologies are typically coupled to OSI Layer 1 and/or Layer 2. For connectivity, normalization at Layer 3-7 (e.g. IP, TCP, UDP, and above) provides the greatest potential for uniformity, as even connector types, wire performance standards, and conductor count are not uniform among various MVPD network technologies.

Though several key security principles are outlined by NIST in their guidelines, most critical in the design of an interoperable and secure system are the following:

- Principle 2. Treat security as an integral part of the overall system design.
- Principle 3. Clearly delineate the physical and logical security boundaries governed by associated security policies.
- Principle 6. Assume that external systems are insecure.
- Principle 9. Protect information while being processed, in transit, and in storage.
- Principle 12. Where possible, base security on open standards for portability and interoperability.
- Principle 14. Design security to allow for regular adoption of new technology, including a secure and logical technology upgrade process.

---

[82] (https://www.owasp.org/index.php/Secure_Coding_Principles)

[83] Writing Secure Code (2nd Edition) - David LeBlanc and Michael Howard ISBN-13: 978-0735617223 ISBN-10: 0735617228

[84] *Engineering Principles for Information Technology Security (A Baseline for Achieving Security), Revision A#*, written by Gary Stoneburner, Clark Hayden, and Alexis Feringa http://csrc.nist.gov/publications/nistpubs/800-27A/SP800-27-RevA.pdf

[85] ISO/IEC 7498-1, http://standards.iso.org/ittf/PubliclyAvailableStandards/s020269_ISO_IEC_7498-1_1994(E).zip

- Principle 24. Strive for simplicity.
- Principle 25. Minimize the system elements to be trusted.

Systems provided by third parties are fundamentally outside of the control of MVPDs, and, barring significant advancements in cryptography beyond the current state of the art, no mechanism is available to avoid adherence to Principle 6 (external systems are insecure) without coordination. Such secure coordination can be assured via cryptographic signature chaining of executed functionality on specific systems, further facilitated by roots of trust and secure protocols (e.g. Playready, Widevine, Fairplay). In order to adhere to Principle 3 (clear delineation), Principle 24 (strive for simplicity), and Principle 25 (Minimize the system elements to be trusted), trusted code execution on devices under customer control must be restricted to narrow components of device functionality. Ideally, such functionality is of the minimal size as to be sufficient to implement necessary security protocols. This provides a manageable minimal functional surface area, in order to reduce possible mechanisms of malicious compromise. Engineers commonly refer to this principle as keeping a "small surface area" for attack, denoting that large hardware/software interfaces are more difficult to secure against compromise.

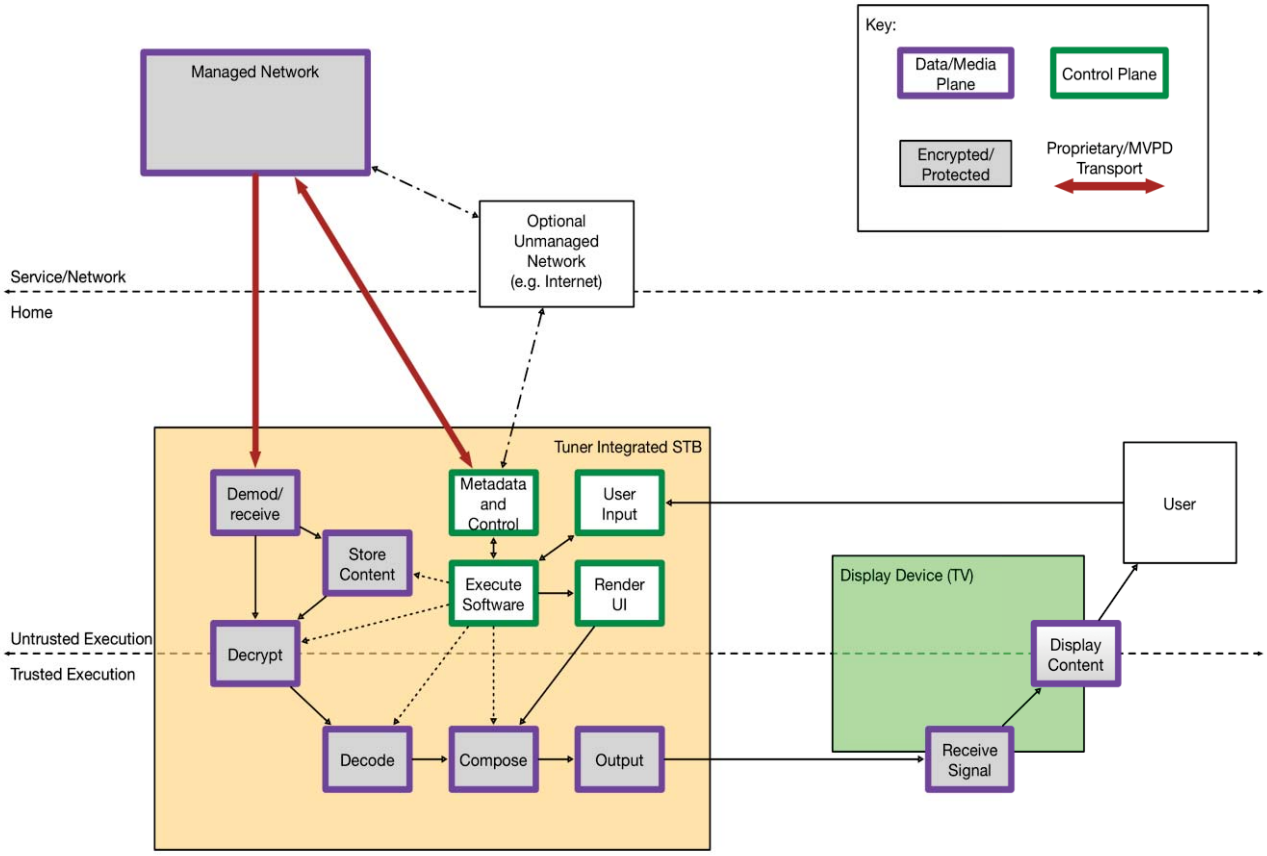


Figure 42 - A canonical MVPD system encompassing a MVPD-provided tuner/DVR and a user-provided TV

In the case of a MVPD-provided set-top-box (STB) used with a MVPD distribution network, care must be taken in the design of the system and STB to resist compromise by malicious modification of, or intrusion into, the provided STB and/or the connection to the network. Such management is handled by embedding critical functions into limited trusted secure elements of the system, further enabled by cryptographic protection of the underlying content. Such a split between the "data plane" and "control plane" of the system allows for rapid and unburdened development of the bulk of the hardware and software of the system while maintaining robustness standards necessary to protect the underlying content. Of note in Figure 42 is the fundamental directionality of media and input in the system. Though secure-mode modules residing in the "data plane" may return narrow results and confirmation to the "control plane", the means of communication are necessarily narrow. Such a system design provides for a limited attack surface area, enabling an elevated degree of trust.

The data plane vs. control plane separation is a semantic, physical, and functional separation in the design of secure content systems. It is critical to understand that such a separation is fundamental to the design and implementation of systems enabling content security.

Critically, the secure elements of these hardware platforms are designed to elevate the degree of sophistication necessary to compromise the underlying content security. Debuggers, arbitrary code execution, and software modification are all tools typically left available in untrusted execution hardware, allowing for quick and effective software/hardware development. Control plane operations are typically segregated to untrusted hardware or untrusted modes of execution on secure hardware. Conversely, trusted execution environments, modes, and hardware disable these "software" or "external" inspection mechanisms, forcing attackers to resort to more exotic means for intrusion (e.g. hardware probing, chip shaving, electron microscopy). As such, critical content protection mechanisms such as key storage, decryption, decode, and presentation are typically reserved for these functional regions.

In Figure 43, all boxes outlined in purple are members of the data plane. In this case, it means that their underlying hardware is either confirmably trusted (by means of cryptographic handshake, or, in literally the case of some MVPD legacy CAS systems, armed guard) or content transiting this component is encrypted. This allows for insecure hardware to participate in the facilitation of the secure data plane through the use of a trusted decryption engine. Decryption modules for high-value data (e.g high definition video content) are typically implemented in separate hardware or in protected hardware operation modes (e.g. Trusted Execution Environment) that prohibit the unintended copying of decrypted content, either through accident or abuse.

In essence, the data plane runs in secure software/hardware environments, and the control plane can then run in insecure software/hardware environments. Furthermore, to protect the integrity and security of the data plane, control plane functions **must** remain separated. These functions (e.g. User interface, media transport control, network interface) are kept out of trusted environments, and communication with, and operation of, data plane components is handled through small, manageable, auditable functional interfaces. Security Principles 24 and 25 (*Strive for simplicity* and *Minimize the system elements to be trusted*) address the necessity of this functional separation. Adherence to these principles is critical to the design of effective content protection mechanisms.

Fortunately, this secure separation is exhibited in all of the proposed and sub-proposed systems, and it is maintained by designing systems such that operations executed in insecure environments (e.g. a Hard Disk Drive used to store programming, or an HDMI connector) are protected by cryptographic authentication/keying protocol (e.g. Widevine, HDCP, DTCP/IP).

In the case of our proposals, systems broadly fall into two categories:

1. Link-protected *local* network systems
2. *End-to-end* systems

In the case of *Device Specific Apps*, content protection methodologies vary greatly, but methodologies can fundamentally be broken into "software" and "hardware" systems, presumably to be covered by WG3. Nonetheless, these systems generally fall into the *End-to-end* category of systems, as the content is decrypted on the same physical device that will decode/deliver it, having previously been encrypted once from operator. *Device Specific Apps* may, however, participate in a *local* system via *Device Specific Apps*.

HTML5 Web Browser systems leveraging EME or other specific plugins for content protection also fall into this *End-to-end* category, as, presumably, do *Sling TV* clients. In each of these cases, underlying content remains in the same cryptographic domain until it is decrypted and decoded on a given device. That device may then use cryptographic link protection (e.g. HDCP) to present still-protected content that has never left the secure data plane. Such an approach *could* be used in a local system with appropriate local key generation.

DLNA VidiPath and RVU represent architectures specifically designed to serve as Link-protected *local* systems for redistribution of MVPD services. These systems both leverage DTCP/IP for local network content protection, effectively abstracting content protection protocols down to local link protection.

The *Competitive Navigation* system proposal could serve as both an *End-to-end* system and a *local* system. It specifically calls for a "*Content Delivery Interface"* that affords for a "*Provider Interface*". A provider interface effectively serves as a Virtual Headend device, allowing MVPDs to alter underlying network delivery mechanisms without disturbing customer service. DLNA VidiPath devices, RVU devices (such as DirecTV's Genie), and the DISH Hopper are all examples, fundamentally, of Provider Interfaces.

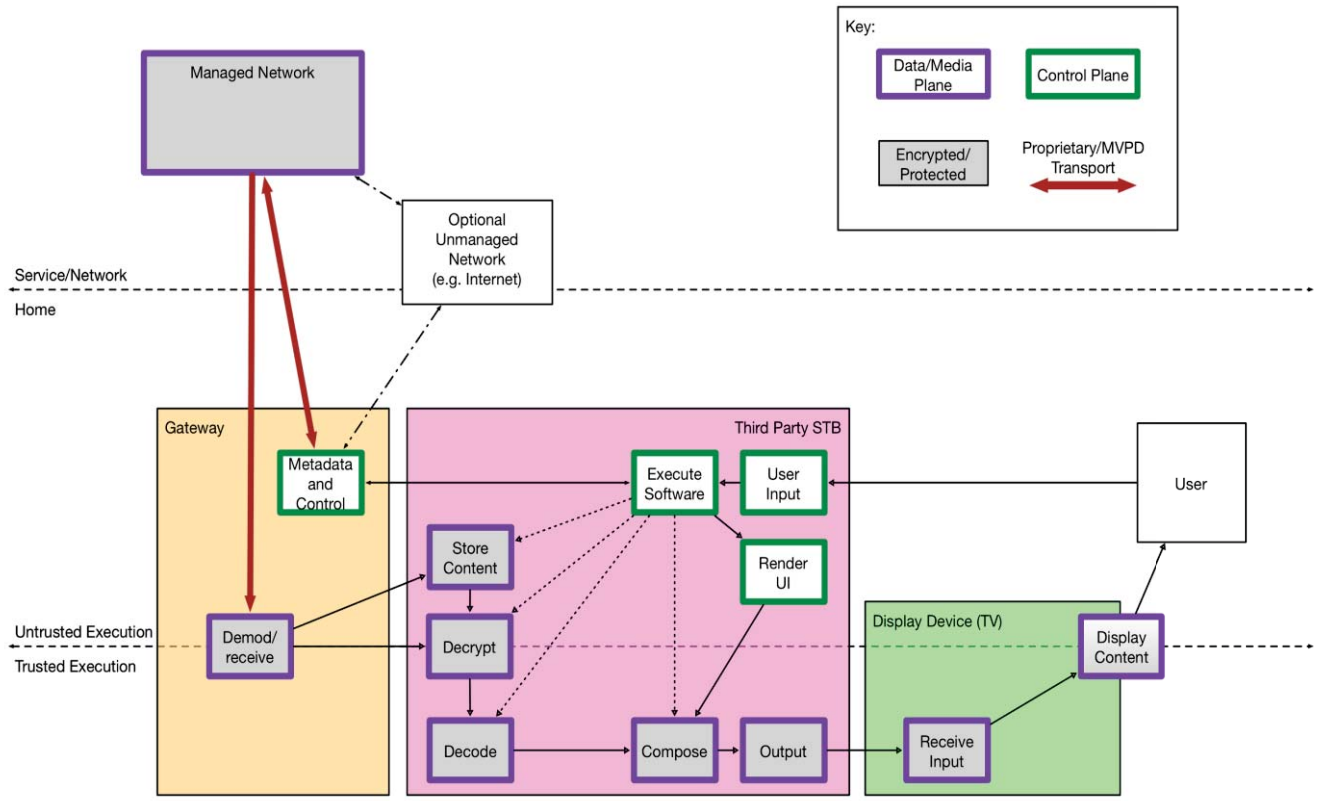


Figure 43 - A "local", "gateway", or "Provider Interface" example system encompassing a MVPD-provided interface, a third-party/user-provided STB, and a user-provided TV

Note that certain elements, such as "Store Content" can be functionally relocated without adversely impacting content security.

To afford for scalability requirements, video distribution systems do not generally provide content streams cryptographically keyed to individually provisioned devices (as this would not scale at OSI Layer 1/Layer 2 effectively). Instead, content streams are uniformly encrypted using symmetric ciphers leveraging keys propagated to trusted execution environments via challenge-response and public/private key protocols. These challenge/response protocols call for bidirectional communication not available end-to-end in broadcast and unidirectional systems (e.g. DBS). Such systems necessarily resort to trusted (or partially trusted) *Provider Interface* devices able to securely manage extended service functionality for non-integrated devices. Such functionality may include, but is not limited to, entitlement management, purchase recording/reporting, and usage auditing. Current examples of such systems include, but are not limited to, Dish Network's Hopper, DirectTV's Genie, and SiliconDust's HDHomeRun Prime, a third-party device interoperating via CableCARD with US domestic cable networks.

Provider interfaces may also be used in bidirectional networks to terminate protocol or media variations to interoperable interfaces. For example, ADSL modems serve as *Provider Interfaces* in AT&T UVerse video distribution networks. In essence, a device that adapts a video distribution network to a different, local distribution, network in the home may be thought of as a *Provider Interface*. Such canonicalization is fundamental to affording for the evolution of MVPD networks while also stabilizing the means by which third party devices may be integrated with MVPD services, and any mechanism affording for third

party device integration should, at the very least, facilitate the use of this category of device in provider-to-user networks.

The *Competitive Navigation* system proposal addresses provider interfaces for *local* networks, necessary to account for unidirectional network peculiarities and evolving MVPD technologies. The *Operator Provided User-Interface* alternative system addresses this design constraint, though it is unclear in the proposal which elements may be necessary to enable competitive navigation devices in possible provider network configurations.

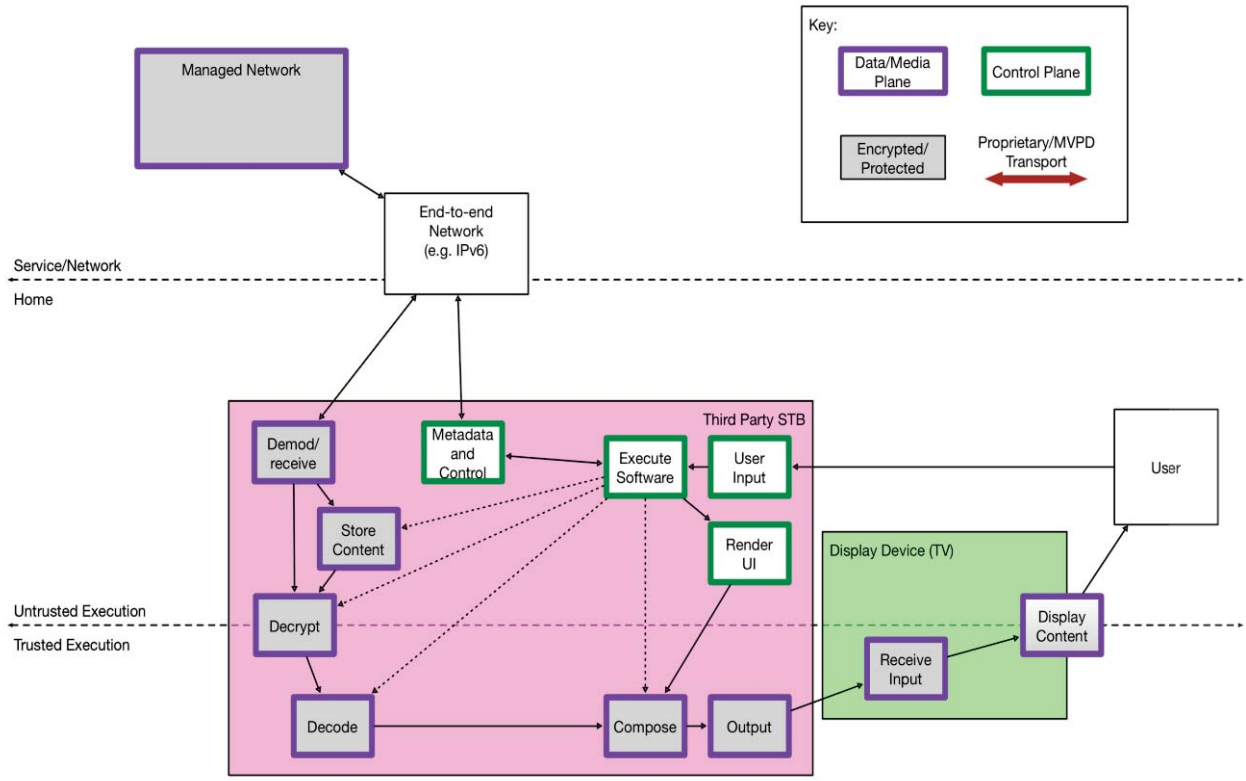


Figure 44 - An end-to-end network encompassing an MVPD system connected via a standardized transport to a third-party-provided STB and a user-provided TV

MVPD networks are increasingly evolving to be end-to-end IP networks, possibly leveraging multicast topologies for distribution efficiency. Such video distribution networks can leverage the same underlying protocols used for Provider-Interface-based service distribution without incurring the added costs of building, deploying, and maintaining Provider Interfaces.

Whether end-to-end IP systems involve OSI Layer 1 and Layer 2 functionality to the subscriber's premises, the [sic]

An appropriately established protocol or family of protocols can facilitate these and many other modalities as various MVPD networks evolve in the face of wildly disparate underlying delivery technologies. Properly designed and abstracted, such systems also allow for reliable competitive retail navigation interface integration without encumbering MVPD service provider innovation. All of this can further be done while maintaining content and service security by leveraging cryptographic roots of trust, security-centric protocol design, and mindful segmentation of critical content-security functions from other functional elements of MVPD networks and downstream distribution devices.

Similarities and Differences

Despite many differences in terminology, protocol selection, and problem set description, significant similarities exist between these proposals.

Two critical conclusions should be drawn from this:

1. Both proposals indicate that it is clearly possible to implement sufficient content security mechanisms to provide MVPD content services to third party devices.
2. By design, in both proposals (and sub-proposals of Part III: Section II.), content security enforcement is independent of user-interface requirements. For any given capable security mechanism provided, content security must fundamentally be orthogonal to the presentation of user interface in order to capably maintain content security.

Both proposals address variations in MVPD network technologies and topologies, affording for functional *Provider Interface* or local network distribution devices to be included where necessary. Additionally, both proposals structurally lay out system designs incorporating secure elements that, with varying degrees of modification, could include security systems proposed by WG3.

To provide an example of how one proposal may be adapted, let us start with a DLNA VidiPath example. The VidiPath specification leverages HTML5 + EME + MSE to drive video playback via operator-controlled user interfaces. In this scheme, only operators are able to provide navigation interfaces to customers, leaving downstream devices to serve as undifferentiated dumb terminals. Though this is a significant and material difference between these system proposals, a system such as DLNA VidiPath could be adapted to provide catalog metadata relatively simply.

For example, a given VidiPath system could conceivably provide a lineup or manifest via XML, in its most basic manifestation, such a presentation could look like:

```
<lineup provider="Comcast" zipcode="90210">
  <channel>
     <callsign>KTTVDT</callsign>
     <network>FOX</network>
     <number>4</number>
     <package>Basic</package> <!-- for easier assocation with entitlement packages, alternatively the provider could assign IDs to channels which associate with entitlements, or link entitlements directly to callsign -->
  </channel>
  <channel>
     <callsign>HBOHD</callsign>
     <number>605</number>
     <package>HBO</package>
     <package>PremiumMovies</package>
  </channel>
</lineup>
```

Such a system could be used, for example, to provide indexed access to a playback system using HTML5 + EME + MSE with a canonicalized resource description mapping (e.g. predetermined http:// directory structure). A more fully-functional example of a content catalog XML schema can be found in the SD&S Schema in Annex C of ETSI TS 102 034 V1.5.1[86]. In essence the functional technical similarity between Part III Section I and several sub-proposals (VidiPath, RVU, HTML5 + EME) of Part III Section II points to the feasibility of a spectrum of capabilities that, if properly applied, could meet multiple important goals:

1. Exposure of catalog and content metadata via protocols affords for the creation of competitive navigation systems and innovative interfaces not yet conceived.
    a. Such canonicalization also strongly facilitates essential accessibility capabilities (e.g. for vision-impaired users) and limited-audience interface accommodations (e.g. for users with severe physical, cognitive, mental, or sensory impairment).
    b. Careful restriction of elements embodied in such a protocol could significantly reduce the cost of implementation of competitive navigation devices, allowing for greater adoption of cost-saving competitive navigation devices in low-income markets.
2. Optional affordance for MVPD-controlled remote user interfaces in such a system could provide ample space for MVPDs to craft competitive and innovative user experiences independently of navigation hardware. Such an accommodation coupled with protocol-based metadata and management facilities could allow for MVPD-supplied innovation without leaving innovation solely at the hands of MVPDs. Competitive navigation devices facilitating these optional features could provide best-in-breed experiences driven by market responses to innovation and competition.

[86] ETSI TS 203 034 V1.5.1
http://www.etsi.org/deliver/etsi_ts/102000_102099/102034/01.05.01_60/ts_102034v010501p.pdf

References

[1] Louis D. Williamson, "FSN Technology," Proceedings: Society of Cable Television Engineers 1995 Conference on Emerging Technologies, Jan. 4-6, 1995, Orlando, FL, pp. 27-35.
[2] Michael B. Adams, "MPEG and ATM in the Full Service Network," Proceedings: Society of Cable Television Engineers 1995 Conference on Emerging Technologies, Jan. 4-6, 1995, Orlando, FL, pp. 13-26.
[3] Ralph Brown and John Callahan, “Software Architecture for Broadband CATV Interactive Systems,” NCTA Cable ’95 Proceedings, Dallas, TX, May 1995.
[4] PEGASUS PROGRAM, Request For Proposal and Functional Requirements Specification, V1.0, Time Warner Cable - Engineering & Technology, March 6, 1996.
[5] ISO/IEC 13818-6:1998 - Information technology -- Generic coding of moving pictures and associated audio information - Part 6: Extensions for DSM-CC.
[6] ISO/IEC 13818-2, 2000: Information technology—Generic coding of moving pictures and associated audio (MPEG): Video.
[7] ATSC Digital Audio Compression Standard (AC-3, E-AC-3), Revision B.
[8] ISO/IEC 14496-10:2005: Information technology - Coding of audio-visual objects - Part 10: Advanced Video Coding.
[9] ISO/IEC 13818-1, 2000: Information technology—Generic coding of moving pictures and associated audio (MPEG): Systems.
[10] Federal Information Processing Standards Publication (FIPS PUB) 46-3, Data Encryption Standard.
[11] ANSI/SCTE 52 2008, Data Encryption Standard – Cipher Block Chaining Packet Encryption Specification.
[12] ANSI/SCTE 65 2008, Service Information Delivered Out-Of-Band For Digital Cable Television.
[13] ANSI/SCTE 55-1 2002, Digital Broadband Delivery System: Out Of Band Transport Part 1: Mode A.
[14] ANSI/SCTE 55-2 2002, Digital Broadband Delivery System: Out Of Band Transport Part 2: Mode B.
[15] CableLabs Press Release, “Cable Industry Creates 'OpenCable™' Goal is Interoperable Set-top Boxes”, September 4, 1997.
[16] OpenCable Host Device 2.1 Core Functional Requirements, OC-SP-HOST2.1-CFR-I15-120112, January 12, 2012, Cable Television Laboratories, Inc.
[17] CEA-679-C Part B, National Renewable Security Standard (July 2005). A joint work of NCTA and CEMA Technology and Standards.
[18] EN 50221-1997, EN 50221: "Common interface specification for conditional access and other digital video broadcasting decoder applications".
[19] DOCSIS Set-top Gateway (DSG) Interface Specification, CM-SP-DSG-I20-120329, March 29, 2012, Cable Television Laboratories, Inc.
[20] ANSI/SCTE 28 2007, HOST-POD Interface Standard
[21] OpenCable™ Software Request For Proposals, OC-RFP-990914, September 14, 1999, Cable Television Laboratories, Inc.
[22] DVB Multimedia Home Platform 1.1.3, DVB-MHP 1.1.3, ETSI TS 102 812 V1.3.1 (2007-03), Blue book A068r3.
[23] OpenCable Application Platform Specifications, OC-SP-OCAP1.2.2-120224, February 24, 2012, Cable Television Laboratories, Inc.
[24] DVB Globally Executable MHP version 1.0.2, (GEM 1.0.2), ETSI TS 102 819 V1.3.1 (2005-10).
[25] Advanced Common Application Platform (ACAP), ATSC Document A/101A, February 12, 2009.
[26] Application Execution Engine Platform For Digital Broad Casting, ARIB STD-B23, Version 1.1, Association of Radio Industries and Businesses, February 5, 2004.

[27] System Description, Blu-ray Disc Read-Only Format, Part 3-2: BD-J Specifications, version 2.4. Blu-ray Disc Association, 2009.
[28] Host 2.0 DVR Extension, OC-SP-HOST2-DVREXT-I03-110512, May 12, 2011, Cable Television Laboratories, Inc.
[29] OCAP Digital Video Recorder (DVR), OC-SP-OCAP-DVR-I08-120112, January 12, 2012, Cable Television Laboratories, Inc.
[30] OpenCable Host Home Networking Extension 2.0, OC-SP-HOST-HN2.0-I06-120112, January 12, 2012, Cable Television Laboratories, Inc.
[31] Home Networking Protocol 2.0, OC-SP-HNP2.0-I07-120224, February 24, 2012, Cable Television Laboratories, Inc.
[32] Reserved Services Domain Protocols Specification, OC-SP-RSD-PROT-I01-080828, August 28, 2008, Cable Television Laboratories, Inc.
[33] Reserved Services Domain Technology Specification, OC-SP-RSD-TECH-I01-080630, June 30, 2008, Cable Television Laboratories, Inc.
[34] OCAP Home Networking Extension, OC-SP-OCAP-HNEXT-I08-120112, January 12, 2012, Cable Television Laboratories, Inc.
[35] Home Networking Security Specification, OC-SP-HN-SEC-I03-120112, January 12, 2012, Cable Television Laboratories, Inc.
[36] Enhanced TV Application Messaging Protocol 1.0, OC-SP-ETV-AM1.0-I06-110128, January 28, 2011, Cable Television Laboratories, Inc.
[37] Enhanced TV Binary Interchange Format 1.0, OC-SP-ETV-BIF1.0-I06-110128, January 28, 2011, Cable Television Laboratories, Inc.
[38] HTTP Live Streaming, Internet Draft, http://tools.ietf.org/html/draft-pantos-http-live-streaming-16
[39] HTML5 - A vocabulary and associated APIs for HTML and XHTML, W3C Recommendation, World Wide Web Consortium, http://www.w3.org/TR/html5/
[40] ISO/IEC 23009-1:2012: Information technology -- Dynamic adaptive streaming over HTTP (DASH) -- Part 1: Media presentation description and segment formats.
[41] *ISO/IEC 23001-7:2012, Information technology -- MPEG systems technologies -- Part 7: Common encryption in ISO base media file format files*. International Standard. URL: https://www.iso.org/obp/ui/#iso:std:iso-iec:23001:-7:ed-1:v1
[42] CAS / DRM Reality Check, Robin Wilson, Nagra, presented to DSTAC Working Group 2 (Technology and Preferred Architectures), March 19, 2015.
[43] AT&T IPTV Technologies and Architectures, Ahmad Ansari, AT&T, presented to DSTAC Working Group 2 (Technology and Preferred Architectures), March 12, 2015.
[44] Verizon Technologies and Architectures, Dan O'Callaghan, Verizon, presented to DSTAC Working Group 2 (Technology and Preferred Architectures), March 12, 2015.
[45] Downloadable Security Technology Advisory Committee (DSTAC) Working Group 2 Report #1, April 21, 2015, https://transition.fcc.gov/dstac/wg2-report-01-04212015.docx.
[46] Cable Technologies And Architectures Overview, Ralph Brown, CableLabs, presented to DSTAC Working Group 2 (Technology and Preferred Architectures), March 12, 2015.
[47] MPEG & IP Video Comparisons, Mark Vickers, Comcast, presented to DSTAC Working Group 2 (Technology and Preferred Architectures), March 12, 2015.
[48] DSTAC Presentation OMS and Optimum Services, Ken Silver, Cablevision, presented to DSTAC Working Group 2 (Technology and Preferred Architectures), March 12, 2015.
[49] Charter DCAS Environment, Jim Alexander, Charter, presented to DSTAC Working Group 2 (Technology and Preferred Architectures), March 12, 2015.

[50] TWC IP Video Architecture, George Sarosi, Time Warner Cable, presented to DSTAC Working Group 2 (Technology and Preferred Architectures), March 12, 2015.
[51] Bright House Overview, Jeff Chen, Bright House, presented to DSTAC Working Group 2 (Technology and Preferred Architectures), March 12, 2015.
[52] DBS Architecture Overview, John Card II, DISH & Steve Dulac, DirecTV, presented to DSTAC Working Group 2 (Technology and Preferred Architectures), March 12, 2015.
[53] Cable Risk and Threats, Ralph Brown, CableLabs, presented to DSTAC Working Group 2 (Technology and Preferred Architectures), March 19, 2015.
[54] MVPD CAS and DRM Trust Infrastructures, Ralph Brown, CableLabs, presented to DSTAC Working Group 2 (Technology and Preferred Architectures), April 14, 2015.
[55] Open Source Implementations of CVP-2 Server and Client, CableLabs, http://html5.cablelabs.com/dlna-cvp-2/index.html
[56] Reference Device Kit (RDK), http://rdkcentral.com
[57] W3C MSE, *Media Source Extensions*. http://www.w3.org/TR/media-source/
[58] W3C EME, *Encrypted Media Extensions*. http://www.w3.org/TR/encrypted-media/
[59] DLNA CVP-2 Press Release, March 18, 2014, http://www.dlna.org/docs/default-source/press-releases/the-digital-living-network-alliance-releases-cvp-2-guidelines-for-viewing-subscription-tv-content-on-multiple-home-devices.pdf?sfvrsn=4
[60] DLNA Guidelines, http://www.dlna.org/dlna-for-industry/technical-overview/guidelines
[61] W3C Crypto, *Web Cryptography API*. http://www.w3.org/TR/WebCryptoAPI/
[62] The Open SSL Project, https://www.openssl.org
[63] RemoteUIServer:1 Service Template Version 1.01, For UPnP™ Version 1.0, September, 2, 2004, http://upnp.org/specs/rui/UPnP-rui-RemoteUIServer-v1-Service.pdf
[64] Mapping from MPEG-2 Transport to HTML5, I03, CL-SP-HTML5-MAP-I03-140207, Cable Television Laboratories, Inc. Specifications, Web Technology, February, 7, 2014
[65] Server Sent Events, W3C Candidate Recommendation, 11 December 2012, http://www.w3.org/TR/eventsource/
[66] DTCP Volume 1 Supplement E, Mapping DTCP to IP, Revision 1.4 ED3, June 5, 2013, Digital Transmission License Administrator, http://www.dtcp.com/documents/dtcp/info-20130605-dtcp-v1se-ip-rev-1-4-ed3.pdf
[67] UPnP Device Management: 2, http://upnp.org/specs/dm/dm2/
[68] IEEE 1905.1, IEEE Standard for a Convergent Digital Home Network for Heterogeneous Technologies, 2013, http://standards.ieee.org/findstds/standard/1905.1-2013.html
[69] BasicManagement:2, Service Template Version 1.01, For UPnP™ Version 1.0, February 16th, 2012, http://upnp.org/specs/dm/UPnP-dm-BasicManagement-v2-Service.pdf
[70] ConfigurationManagement:2, Service Template Version 1.01, For UPnP™ Version 1.0, March 4th, 2013,http://upnp.org/specs/dm/UPnP-dm-ConfigurationManagement-v2-Service.pdf
[71] EnergyManagement:1, Service Template Version 1.01, For UPnP™ Version 1.0, August 30, 2013, http://upnp.org/specs/lp/UPnP-lp-EnergyManagement-v1-Service.pdf
[72] S. Santesson, TLS Handshake Message for Supplemental Data, IETF RFC 4680, September 2006, http://tools.ietf.org/html/rfc4680
[73] T. Dierks, et al, The Transport Layer Security (TLS) Protocol, Version 1.2, IETF RFC 5246, August 2008, http://tools.ietf.org/html/rfc5246
[74] The WebKit Open Source Project, http://www.webkit.org
[75] Downloadable Security Technology Advisory Committee (DSTAC) Working Group 1 Report #1, April 21, 2015, https://transition.fcc.gov/dstac/wg1-report-01-04212015.pdf

[76] Report of WG1, MVPD Requirements and Content Providers Requirements {reference to document goes here}

Tables in Document

Table 1 - Diversity of MVPD Customer Premise Equipment 7
Table 2 - Comparison 802.11n and 802.11ac features 30
Table 3 - Summary of MoCA 2.0 PHY and MAC Layer Parameters 34
Table 4 - MoCA 2.0 Power Mode Names and Description 36
Table 5 - Sample OTT Service ca. Summer 2015 43
Table 6 - Transport, Control, And Codec Support 47
Table 7 - Examples of Stream Management 50
Table 8- US Retail Device Numbers 73
Table 9 - MVPD Subscriber Count and Support for Personal Computers 128

Figures in Document

Figure 1 - Typical Cable System Network Architecture 9
Figure 2 - OpenCable/tru2way Interface Diagram 12
Figure 3 - DBS Architecture – Satellite to Home Distribution Path 14
Figure 4 - DIRECTV Uplink Facilities 15
Figure 5 - DISH Uplink Facilities 16
Figure 6 - DIRECTV Frequency Plan 17
Figure 7 - DISH Frequency Plan 18
Figure 8 - DIRECTV Server-Client Architecture 20
Figure 9 - DISH Server-Client Architecture 21
Figure 10 - AT&T U-verse Architecture 23
Figure 11 - ITU G.98x PON Optical Spectrum 24
Figure 12 - Verizon FiOS Access Network 25
Figure 13 - Verizon FiOS High-Level Architecture 26
Figure 14- Verizon FiOS Dual-Network Hybrid STB Architecture 26
Figure 15 - Example Home Network 28
Figure 16 - Current in Home Wireless Technologies 28
Figure 17- MoCA 2.0 Extended Band D Frequency Plan 34
Figure 18- Switched and Non Switched Video 50
Figure 19 - DLNA VidiPath Overview 80
Figure 20 - DLNA VidiPath Architecture 81
Figure 21 - VidiPath HTML5 RUI Usage Model 82
Figure 22 - Secure content transmission using DTCP-IP 84
Figure 23 - VidiPath Diagnostics Architecture 86
Figure 24 - DLNA Low Power Architecture 87
Figure 25 - HTTP-Adaptive Delivery Entities 88
Figure 26 - VidiPath Authentication Entities 89
Figure 27 - Hybrid In-home + Cloud Deployment 92
Figure 28 - In-home only Deployment 93

Figure 29- Media Source Extensions Architecture 96
Figure 30- Encrypted Media Extensions Architecture 97
Figure 31 - Detailed EME Architecture with APIs 98
Figure 32 - Creation of Passage Selective Multiple Encrypted Stream 102
Figure 33 – Typical Digital Cable System Architecture 103
Figure 34 – *Passage*-enabled Digital Cable System 104
Figure 35 – The Headend Encoding Process - 4 Steps - Selection, Duplication, Encryption and Reconstruction 105
Figure 36 – *Passage* Bandwidth Usage 106
Figure 37 - Interfaces 115
Figure 38 - Overview of App Approach 129
Figure 40 - Example App Interfaces ..... **Error! Bookmark not defined.**
Figure 41 - HTML5/EME Implementation 137
Figure 42- Use of Passage to Enable End-to-End DRM 175
Figure 43 - A canonical MVPD system encompassing a MVPD-provided tuner/DVR and a user-provided TV 188
Figure 44 - A "local", “gateway”, or "Provider Interface" example system encompassing a MVPD-provided interface, a third-party/user-provided STB, and a user-provided TV 191
Figure 45 - An end-to-end network encompassing an MVPD system connected via a standardized transport to a third-party-provided STB and a user-provided TV 192

Part IV: Appendix A: Survey of Existing Devices

Description	Supports Direct Attach to MVPD Distribution Network	Supports Direct Attach to IP Network Used for Content Distribution	Supports Direct Attach to OTT Network Over Internet	Supports Local Network Connectivity	Uses Custom Apps	Uses HTML 5 Apps	Uses Local MVPD Guide	Uses Remote UI	Allows User to Make Local Recordings	Provides Access to Cloud PVR from Competitive Navigation UI	Supports Navigation of MVPD Linear Service by 3rd Party UI App
MVPD provided Set-top Box	Yes	Some[87]	Yes	YES	Yes	(Some) YES	Yes, if PVR	No	Yes	No	No
High Definition and 4K Ultra HD TV – for IP and other delivery paths	No (assumes Clear QAM no longer possible)	No	Yes, smart TV	DLNA	Yes (OTT) No (Next Gen Android TV)	Yes	No for MVPD, creates one for over-the-air Broadcasts	No	No	N/A	No
RVU certified TV	Home Network	No	Yes, smart TV	DLNA	Yes, RVU	No	Remotely	Yes, with RVU application	See discussions in Section III system proposals	N/A	with DirecTV SHEF protocol

[87] Not for DBS and QAM distribution.

Description	Supports Direct Attach to MVPD Distribution Network	Supports Direct Attach to IP Network Used for Content Distribution	Supports Direct Attach to OTT Network Over Internet	Supports Local Network Connectivity	Uses Custom Apps	Uses HTML 5 Apps	Uses Local MVPD Guide	Uses Remote UI	Allows User to Make Local Recordings	Provides Access to Cloud PVR from Competitive Navigation UI	Supports Navigation of MVPD Linear Service by 3rd Party UI App
VidiPath certified TV	Home Network	Yes	Yes, smart TV	DLNA	Yes, VidiPath (DLNA)	Yes, VidiPath for RUI, VidiPath 2.0 will have cloud/ DRM capability	Remotely	Yes, DLNA + HTML 5	See discussions in Section III System proposals	No	No
MVPD Provided Home Media Server (Content Server on Home Network)	Yes	Yes	Yes	Yes	Yes	Yes	Yes, plus additional guide data provided via broadband	Yes, for serving client devices	Yes	Yes for various cable systems, No for current satellite delivered services	Yes (custom MVPD-provided custom API)
Home Video Gateway from MVPD, Residential Gateways (RG)[88]	Yes	Yes	Yes	Yes	No	Yes (Some)	Yes	Yes (Some)	Yes	No	No
Digital Transport Adapter (DTA)	Yes	No	Yes	Not currently	Yes	Not currently	No	No	Not currently	No	No

[88] AT&T DSL gateway includes wifi access.

Description	Supports Direct Attach to MVPD Distribution Network	Supports Direct Attach to IP Network Used for Content Distribution	Supports Direct Attach to OTT Network Over Internet	Supports Local Network Connectivity	Uses Custom Apps	Uses HTML 5 Apps	Uses Local MVPD Guide	Uses Remote UI	Allows User to Make Local Recordings	Provides Access to Cloud PVR from Competitive Navigation UI	Supports Navigation of MVPD Linear Service by 3rd Party UI App
Retail Whole Home DVR Ecosystem (TiVo)	Yes	No	Yes	Yes	Yes	Yes	No	Yes, for VOD and OTT	Yes	N/A	Yes
Media Player Box from Retail (Roku, Apple TV, Amazon, WD)	No	Yes	Yes	Yes	Yes	Yes	No	No	Some - This is software dependent and highly variable, but coming to more current-run devices via software.	No, access via MVPD /OTT app	No, access via MVPD /OTT app
Media Player Sticks (USB/HDMI)	No	Yes	Yes	Yes	Yes	Yes	No	No	Some - This is software dependent and highly variable, but coming to more current-run devices via software.	No, access via MVPD /OTT app	No, access via MVPD /OTT app
Connected Tablet or Smart Phone with Data Plan or Wi-Fi	No	Yes	Yes	Yes	Yes	Yes	No	No	Software dependent (rare)	No, access via MVPD /OTT app	No, access via MVPD /OTT app

Description	Supports Direct Attach to MVPD Distribution Network	Supports Direct Attach to IP Network Used for Content Distribution	Supports Direct Attach to OTT Network Over Internet	Supports Local Network Connectivity	Uses Custom Apps	Uses HTML 5 Apps	Uses Local MVPD Guide	Uses Remote UI	Allows User to Make Local Recordings	Provides Access to Cloud PVR from Competitive Navigation UI	Supports Navigation of MVPD Linear Service by 3rd Party UI App
Broadband Connected Blu-Ray Players	No	Yes	Some	Some	Some	Some	No	Yes	No	No, access via MVPD /OTT app	No, access via MVPD /OTT app
Notebook or Laptop Computer (Apple, Windows, Linux)	No	Yes	Yes	Yes	Yes, but less common usage	Yes	No	No	Yes	No, access via MVPD /OTT app	No, access via MVPD /OTT app, except w/Windows /OCUR
All-in-One or Desktop Computer (Apple, Windows, Linux)	No	Yes	Yes	Yes	Yes, but less common usage	Yes	No	No	Yes	No, access via MVPD /OTT app	No, access via MVPD /OTT app, except w/Windows /OCUR
Gaming Consoles (PS4, Xbox)	No	Yes	Yes	Yes	Yes	Yes	No	No	Yes (Some)	No, access via MVPD /OTT app	No, access via MVPD /OTT app
Connected AV Receivers	Yes, radio No, AV	Some	Some	Yes	Some	No	No	No	No	No	N/A

Description	Supports Direct Attach to MVPD Distribution Network	Supports Direct Attach to IP Network Used for Content Distribution	Supports Direct Attach to OTT Network Over Internet	Supports Local Network Connectivity	Uses Custom Apps	Uses HTML 5 Apps	Uses Local MVPD Guide	Uses Remote UI	Allows User to Make Local Recordings	Provides Access to Cloud PVR from Competitive Navigation UI	Supports Navigation of MVPD Linear Service by 3rd Party UI App
Internal/External Tuners (Hauppauge, Silicon Dust, Sat-IP)	Yes	No	No	Via 3rd party service[89]	Via 3rd party service[89]	Via 3rd party service[89]	Not from MVPD Guide, sourced externally via 3rd party service	Via 3rd party service[89]	Via 3rd party service[89]	No	Via 3rd party service[89]
External/External Tuners (Hauppauge, Silicon Dust, Sat-IP)	Yes	No	No	Yes; DLNA, DTCP-IP, OCUR/DRI, or custom protocols	3rd party client apps supported	Via 3rd party client	Not from MVPD Guide, sourced externally via 3rd party service	Via 3rd party client implementation	Via 3rd party client	No	Via 3rd party client using DLNA or OCUR/DRI

[89] 3rd party services for internal/external tuners can be protocol based servers or direct clients such as:
- VLC media player client
- DLNA Digital Media Servers, such as tv-now
- Windows Media Center
- Windows Media Player
- Command line tools
- Custom applications (Hauppauge WinTV, etc)

Description	Supports 3rd Party Apps	Supports 3rd Party Access from external device	Works across MVPD Network Technologies (Cable, IPTV, Satellite)	Portable across MVPDs (within Cable or within Satellite)	Supports ATSC Tuner and Guide Integration	Supports National EAS	Universal Remote Control Support	Supports Multiple Tuner Management and Conflict Resolution	Supports archiving customer-recorded content to external storage
MVPD provided Set-top Box	(Some) YES	(Some) YES	No, MVPD Network Technology specific	(Some) YES	(Some) YES	Yes	Yes	Yes, in whole home DVR	Some[90]
High Definition and 4K Ultra HD TV – for IP and other delivery paths	Yes, smart TV	Yes, smart TV based on Android	HDMI, VidiPath, RVU	HDMI, VidiPath, RVU	Yes, a guide can be generated by scanning channels and using event informatio n tables	Yes	Yes	Usually a single tuner now, PiP feature is gone	Japanese, European Models
RVU certified TV	Yes	TBD	if RVU used	if RVU	Not RVU Feature	Yes	Yes	Same	Not RVU Feature
VidiPath certified TV	Yes	TBD	if VidiPath used	if VidiPath	Not VidiPath feature	Yes	Yes	Same	Not VidiPath feature

[90] Some DISH STBs support use of customer-provided USB HDD for external archive (not export) and DVR functions.

Description	Supports 3rd Party Apps	Supports 3rd Party Access from external device	Works across MVPD Network Technologies (Cable, IPTV, Satellite)	Portable across MVPDs (within Cable or within Satellite)	Supports ATSC Tuner and Guide Integration	Supports National EAS	Universal Remote Control Support	Supports Multiple Tuner Management and Conflict Resolution	Supports archiving customer-recorded content to external storage
Home Media Server (Content Server on Home Network)	Yes (MVPD-provided custom API)	Some	No, except for certain OTT-provided services	No	Yes	Yes	Yes	Yes	Yes
Home Video Gateway from MVPD, Residential Gateways (RG) [88]	No	No	No	No	No	Some	No	No	No
Digital Transport Adapter (DTA)	No	No	No, cable specific technology	Yes	No	Yes	Yes	No	No
Retail Whole Home DVR Ecosystem (Tivo)	Yes	Yes	No	All Cable	Yes	Yes	Yes	Yes	Yes
Media Player Box from Retail (Roku, Apple TV, Amazon, WD)	Yes	Yes	HDMI, local or network gateway	HDMI, local or network gateway	With ATSC gateway	Software (and gateway) depende nt.	Yes. BT, WiFi, and IR support varies by device.	Tuner, gateway, software specific.	Variable (software and hardware specific)
Media Player Sticks (USB/HDMI)	Yes	Yes	HDMI, local or network gateway	HDMI, local or network gateway	With ATSC gateway	Software (and gateway) depende nt.	Yes. BT, WiFi, and IR support varies by device.	Tuner, gateway, software specific.	Variable (generally not local storage, but network storage)

Description	Supports 3rd Party Apps	Supports 3rd Party Access from external device	Works across MVPD Network Technologies (Cable, IPTV, Satellite)	Portable across MVPDs (within Cable or within Satellite)	Supports ATSC Tuner and Guide Integration	Supports National EAS	Universal Remote Control Support	Supports Multiple Tuner Management and Conflict Resolution	Supports archiving customer-recorded content to external storage
Connected Tablet or Smart Phone with Data Plan or Wi-Fi	Yes	Yes	HDMI, local or network gateway	HDMI, local or network gateway	With ATSC gateway	Software (and gateway) depende nt.[91]	Yes. BT, WiFi, and IR support varies by device.	Tuner, gateway, software specific.	Variable (local MMC/SD or network storage)
Broadband Connected Blu-Ray Players	Yes	Yes	HDMI, local or network gateway	HDMI, local or network gateway	With ATSC gateway	Software (and gateway) depende nt.	Yes. BT, WiFi, and IR support varies by device.	Tuner, gateway, software specific.	With computer/gate way assistance (e.g. Plex, Kodi)
Notebook or Laptop Computer (Apple, Windows, Linux)	Yes	Yes	HDMI, local or network gateway	HDMI, local or network gateway	With ATSC gateway or built-in/optional tuner (PCIe, USB, etc)	Software (and gateway) depende nt.	Yes. BT, WiFi, and IR support varies by device.	Tuner, gateway, software specific.	Yes
All-in-One or Desktop Computer (Apple, Windows, Linux)	Yes	Yes	HDMI, local or network gateway	HDMI, local or network gateway	With ATSC gateway or built-in/optional tuner (PCIe, USB, etc)	Software (and gateway) depende nt.	Yes. BT, WiFi, and IR support varies by device.	Tuner, gateway, software specific.	Yes

[91] Tablets with Data Plan may also support WEA; Connected Smartphone with Data Plan is generally required to support WEA; Connected Smart Phone with Wi-Fi may support WEA.

Description	Supports 3rd Party Apps	Supports 3rd Party Access from external device	Works across MVPD Network Technologies (Cable, IPTV, Satellite)	Portable across MVPDs (within Cable or within Satellite)	Supports ATSC Tuner and Guide Integration	Supports National EAS	Universal Remote Control Support	Supports Multiple Tuner Management and Conflict Resolution	Supports archiving customer-recorded content to external storage
Gaming Consoles (PS4, Xbox)	Yes	Yes	HDMI, local or network gateway, or HDMI passthrough	HDMI, local or network gateway	With ATSC gateway or USB tuner	Software (and gateway) depende nt.	Yes. BT, WiFi, and IR support varies by device.	Tuner, gateway, software specific.	Yes
Connected AV Receivers	N/A	N/A	HDMI	HDMI	N/A	N/A	N/A	N/A	N/A
Internal Tuners (Hauppauge, Silicon Dust, Sat-IP)	requires 3rd party app[89]	requires 3rd party app[89]	Some tuners support more than one DBS/terrestrial/Cable standard	Yes	N/A	N/A	N/A	N/A	N/A
External Tuners (Hauppauge, Silicon Dust, Sat-IP)	requires a client[89]	requires 3rd party app or OCCUR client[89]	Some tuners support more than one DBS/terrestrial/Cable standard???	OCUR on Cable	N/A	N/A	N/A	N/A	N/A