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

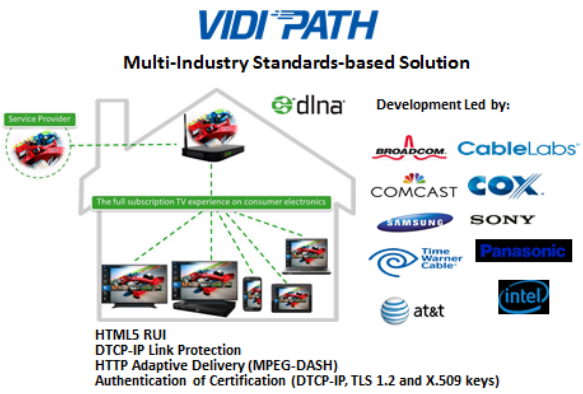
Source: http://xyo.net (accessed 2/6/15)

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.

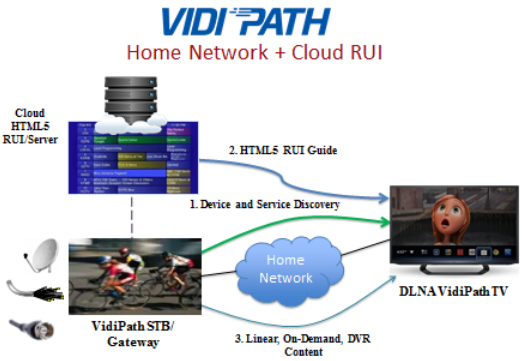
Some members did not agree with the MVPD's conclusions that these are the best examples of getting MVPD service on to consumer devices. The working group was also shown presentations on current retail CableCARD devices from TiVo and Hauppauge that offer consumers another alternative. In the CableCARD 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]

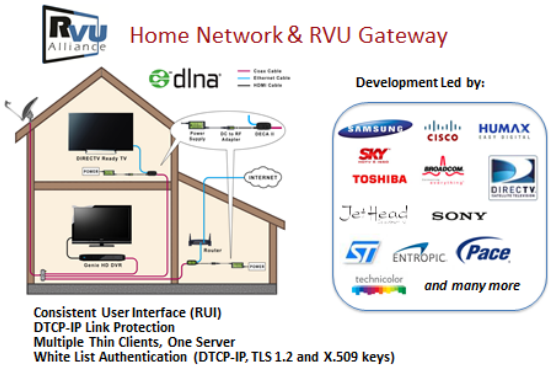


(1B) Example: Technology Survey – DLNA VidiPath

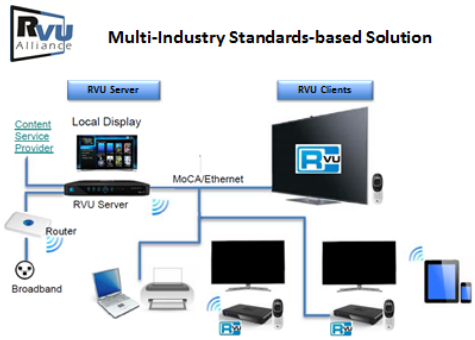


(1B) Example: Technology Survey – DLNA VidiPath

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.

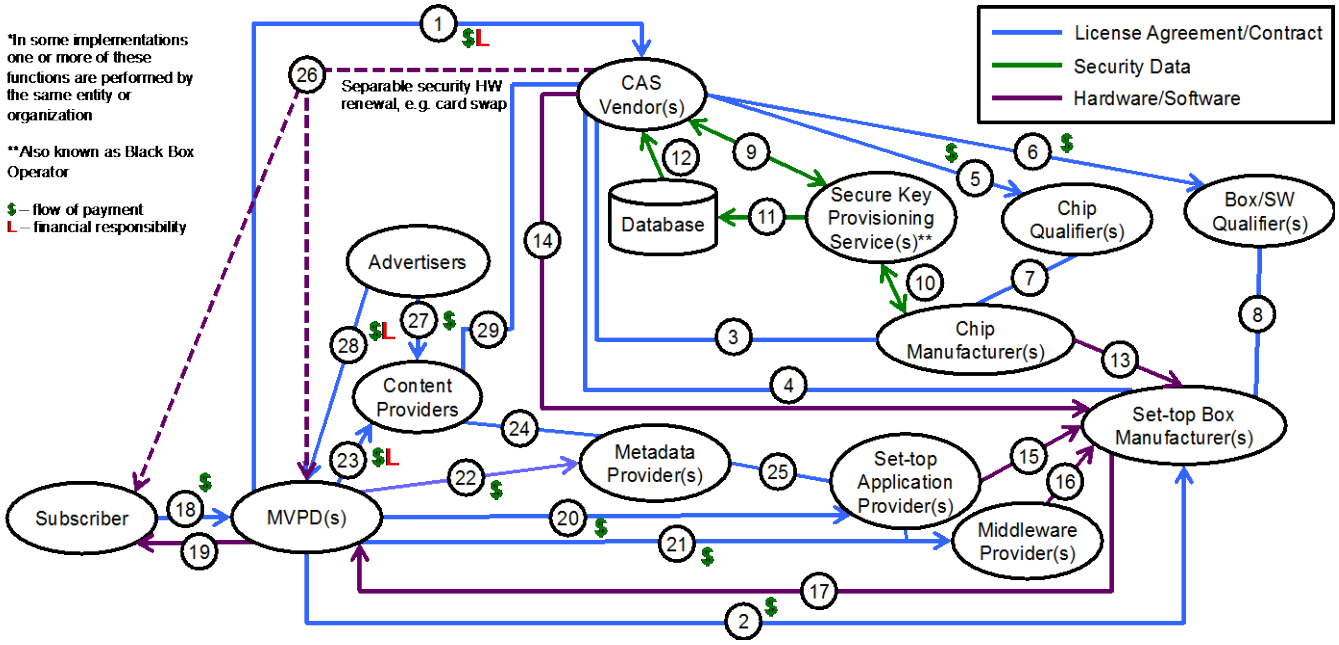


Figure 1 - Example MVPD Trust Infrastructure

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.

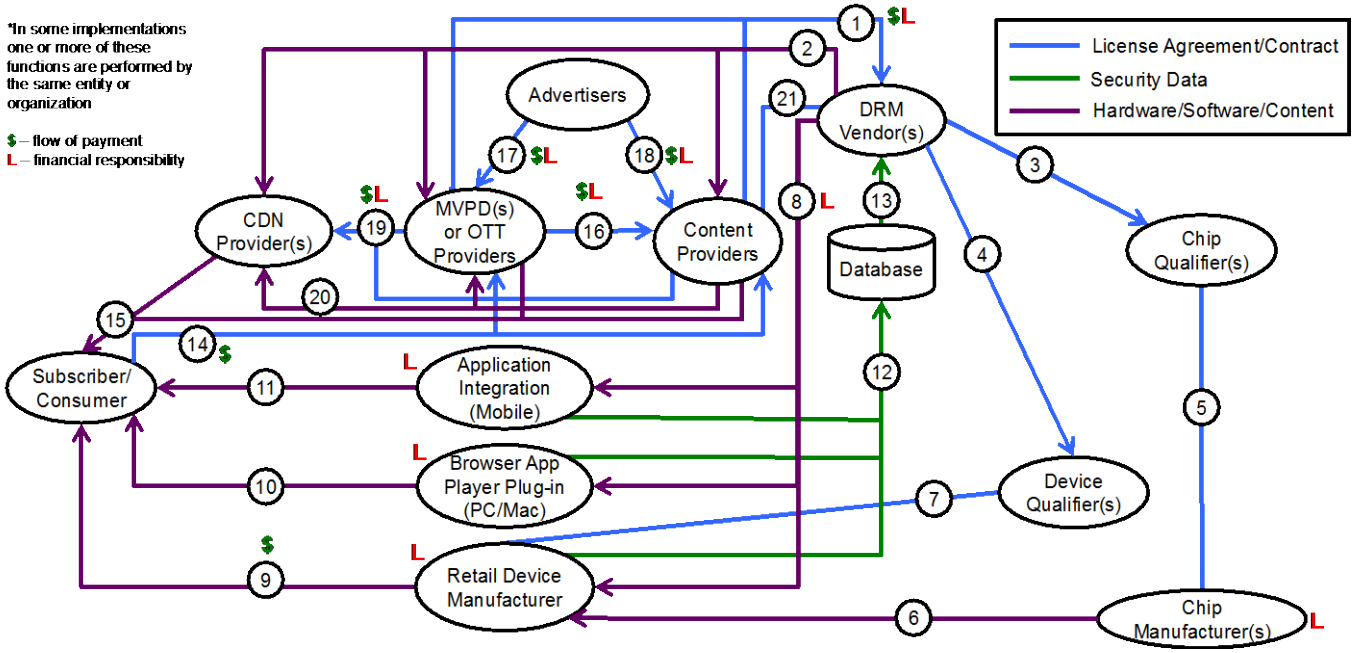


Figure 2 - Example DRM Trust Infrastructure

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)

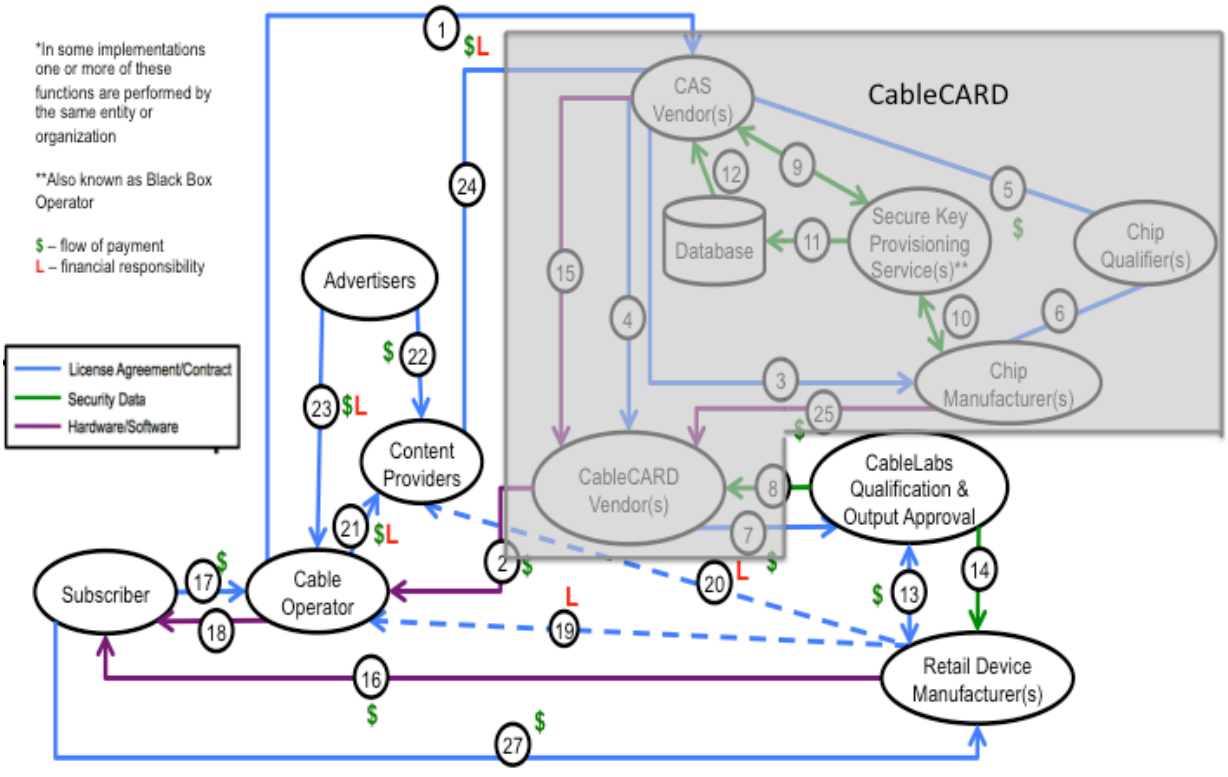


Figure 3 - Example CableCARD CAS Trust Infrastructure

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.