Premium Cable Content on Any Device, In Any Room Using DLNA CVP-2

Amol Bhagwat, CableLabs

Abstract

The paper first introduces key requirements and challenges for delivering premium cable content on customer owned and managed devices in the home. The paper then provides the details of a multi-industry effort in Digital Living Network Alliance for defining the Commercial Video Profile-2 specifications that enable distribution of premium content over home networks to various CE devices such as TVs, tablets, mobile phones, game consoles, HDMI sticks, and PCs. Benefits of the DLNA CVP-2 specifications to consumers, CE manufactures and service providers are discussed. The paper also presents an overview of the architecture and components of open source implementations of the DLNA CVP-2 Server and Client specifications that are aligned with the Reference Device Kit.

INTRODUCTION

Consumers increasingly expect to consume premium entertainment content on any device of their choice, at any time and at any place (inside or outside of the home). Cable operators are interested in leveraging IP-based home networks to deliver their QAM-sourced content from an in-home video gateway to devices of customers' choice in any room within the home. This serves as a transition strategy for providing content to IP-based devices in the home before migrating to End-To-End IP video architecture. Such a solution would also help U.S. cable operators to fulfill their regulatory obligation of enabling a standards-based IP output from their high-definition set-tops (HD-STBs) to serve retail Consumer Electronics (CE) devices as a part of Federal Communications Commission's (FCC) CableCARD™ order #3 [1].

This paper first discusses cable operator requirements that customer-owned-and-managed (COAM) retail CE devices need to support in order to receive premium cable content over the home network. These requirements include a consistent cable user experience across all devices, support for cable regulatory and contractual services (e.g., closed captions, parental controls, descriptive video services, and Emergency Alert System messages), content protection and quality of service. Consumer Electronics (CE) manufacturers and service providers from all over the world, including north American cable operators, led an effort to define Commercial Video Profile-2 (CVP-2) specifications within Digital Living Network Alliance (DLNA) to enable premium content to retail CE devices [2].

This paper presents a detailed overview of the CVP-2 specifications that include features such as HTML5 Remote User Interface (RUI), Authentication, Diagnostics, Low Power, MPEG-DASH, and DTCP-IP [3]. Benefits offered by CVP-2 to consumers, OEM manufacturers and service providers are also discussed. To support market adoption and implementation of CVP-2, CableLabs has developed an open source implementation of CVP-2 Server and Client reference devices [4] using the same set of base libraries as used in Reference Device Kit (RDK) [5]. The Server and Client reference devices serve as reference platforms for CE device manufacturers and cable operators to test their CVP-2 implementations. An overview of the architecture and various components of CVP-2 Server and Client implementations is also provided.

REQUIREMENTS FOR ENABLING PREMIUM CONTENT ON COAM DEVICES

Traditionally, the model for delivering cable content (or any subscription TV content) has been to supply a cable operator specified set-top box (STB) for each display device in the home. The STB ensures a consistent navigation experience using a cable operator guide and video playback for different video formats and bit rates. Using such a device, cable operators are able to fulfill their contractual agreements with content providers in terms of support for features such as content security, ad insertion, and enhanced TV (ETV) applications including Video on Demand (VoD) and television commerce (T-commerce) transactions. In addition, the STB, in conjunction with a cable operator guide, supports cable operators' regulatory compliance requirements such as providing closed captions, parental controls, Emergency Alert System (EAS) messages, Secondary Audio Programming (SAP), and Descriptive Video Services (DVS). Thus, in order to serve cable operator premium content from a video gateway over the home network to COAM CE devices in any room, without requiring a cable operator STB, COAM devices need to be able to fulfill the aforementioned functional requirements. The subsequent subsection provides detail overview of the key requirements for COAM devices.

Application Framework

COAM devices need to support an application framework that allows cable operators to serve their guide to COAM devices, either from a video gateway in the home or directly from the cloud. This application framework needs to enable playback of video inside the user interface. Support for cable operator 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 cable 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.

Content Protection

As premium cable content is streamed from a video gateway over the home network to COAM devices, the content needs to be protected to prevent unauthorized copying. Thus, a video gateway and COAM devices need to support a content protection solution that is acceptable to the content owners.

Media Formats

In order to support a full set of cable services such as live/linear content, Video On Demand (VoD), Digital Video Recorder (DVR), and Pay-Per-View (PPV), COAM devices need to support an appropriate set of audio and video codecs with specific resolution, bit rate, and frame rate. QAM-sourced cable 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 cable operators may have a need to stream video over Wi-Fi networks to portable devices.

Network Quality of Service

Cable operators, as well as content providers, want to ensure that their services are offered with the highest quality when the content is streamed over the home network from video gateway to COAM 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 video gateway and COAM 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.

Home Network Diagnostics & Management

As premium cable content is streamed over the home network from a video gateway to COAM devices, cable operators 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 COAM devices, provide network topology, and information about network throughput. In addition, the ability to query information about COAM devices such as device model, manufacture, and, firmware version needs to be enabled by this mechanism.

Energy Save Operation

In order to meet consumer expectations and cable operator requirements for energy consumption, cable operator 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 cable content on a COAM device, it is necessary that the COAM device is able to wake up the video gateway from sleep mode.

Device Authentication

When a COAM device requests a service from a cable operator video gateway, the cable operator wants to ensure that the COAM device meets aforementioned requirements so that cable operator guide, video and related services are presented correctly to consumers. Thus, it is necessary that the COAM device supports a secure mechanism for device authentication based on digital credentials.

SOLUTION: DLNA COMMERCIAL VIDEO PROFILE (CVP-2)

To enable secure distribution of premium content from an in-home video gateway to COAM CE devices, major cable operators in the U.S. (Comcast, Cox, and TWC) and CableLabs led an effort, in partnership with CE manufacturers and other service providers all over the world, to define Commercial Video Profile-2 (CVP-2) specifications within Digital Living Network Alliance (DLNA) [2].

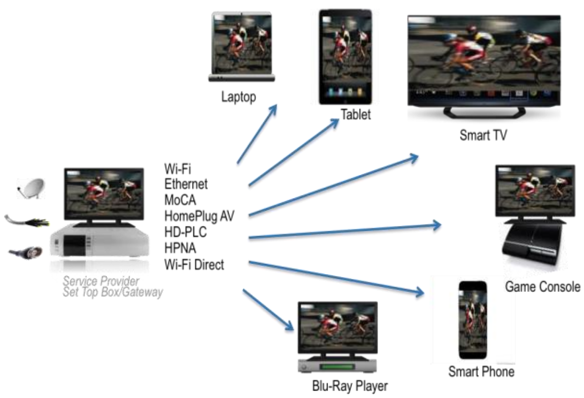

Figure-1: DLNA CVP-2 Overview

Using CVP-2 specifications, cable operators can stream various cable services (e.g., live/linear VoD, DVR, PPV) from a video gateway to COAM CE devices, such as TVs, game consoles, tablets, mobile phones, and laptops, with a consistent cable operator user interface across different devices without the need of a dedicated cable operator supplied STB per device.

DLNA CVP-2 specifications guidelines were published in March 2014 and the certification program is scheduled to be launched in October 2014 [2].

The DLNA CVP-2 Specifications define the following set of features for CVP-2 Server and Client [3]:

- 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
- Digital Media Player & Digital Media Renderer; mandatory for Client only

The following sub-sections describe various features defined in the CVP-2 specifications.

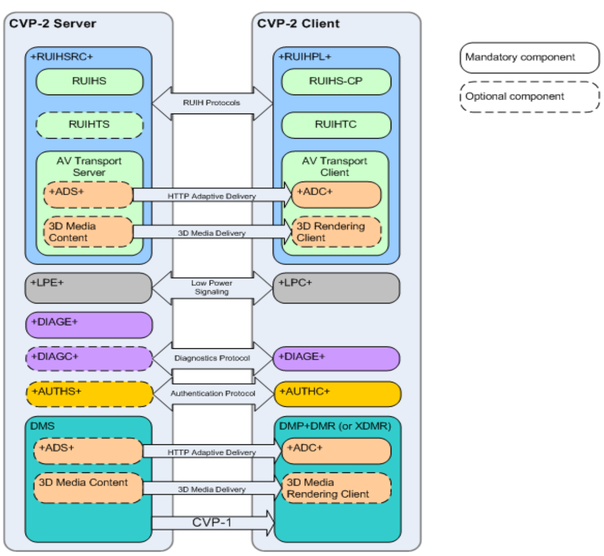

Figure-2: DLNA CVP-2 Architecture

<u>HTML5 Remote User Interface (RUI)</u>

In order to support consistent cable operator user interface to different form factors of COAM CE devices (e.g., TVs, tablets, mobile phones, and, game consoles) and requirements identified in the Application Framework subsection, DLNA CVP-2 specifications specify support for an HTML5-based Remote User Interface. DLNA HTML5 Remote RUI specification defines a profile of W3C's HTML5 specification [6] 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 cable operators 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 cable operators to offer their guides directly from the cloud, thereby enabling them to rapidly evolve their services and applications to consumers.

A cable operator video gateway advertises that the Uniform Resource Locator (URL) of the cable operator HTML5 guide and CVP-2 devices discover the URL using the UPnP RUI Discovery mechanism [7]. 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, cable operators are able to display video within their guide user interface pages. DLNA HTML5 RUI Specification defines DLNA specific extensions to support playback Digital Transmission Copy Protection (DTCP) over IP link protected video content using <video> tag. 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 [8] that defines a standardized mechanism for exposing information about cable operator 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 cable operator HTML5 applications can provide these services to consumers. DLNA HTML5 RUI requires implementation of this specification, so that cable operators can fulfill their regulatory and contractual obligations while offering cable services to CVP-2 devices. DLNA HTML5 RUI Specification also requires support for W3C's Server Sent Events (SSE) specification [9]. Using SSE, cable operators are able to provide EAS messages to cable operator HTML5 RUI applications running on CVP-2 devices. Figure-3 shows various HTML5 RUI entities and their functions.

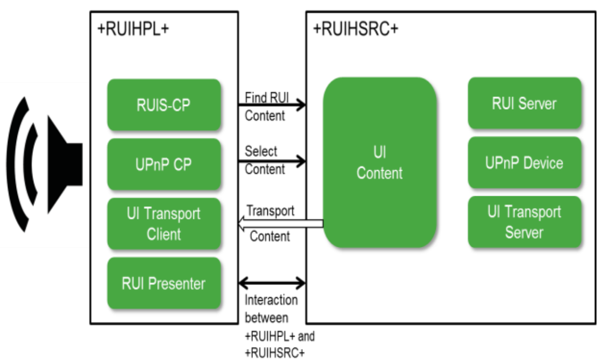

Figure-3: CVP-2 HTML5 RUI Usage Model

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 CVP-2 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.

<u>MPEG-2/AVC Media Formats:</u>

In order to ensure baseline interoperability between the CVP-2 Server and the CVP-2 Client, the DLNA CVP-2 specifications define a required set of Media Format profiles for both CVP-2 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 is 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. CVP-2 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 cable operators offer their content using one of the media format profiles from the CVP-2 server implemented in the video gateway, a CVP-2

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 CVP-2 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 cable operator video gateway to a CVP-2 client device. DTCP-IP is a link protection specification published by Digital Transmission License Administrator [10].

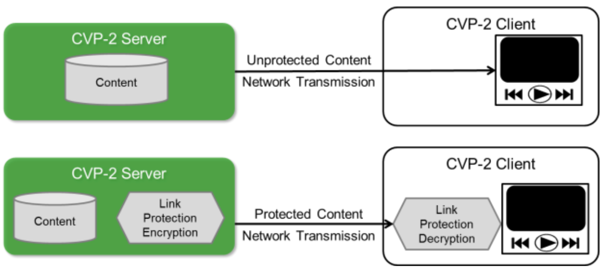

Figure-4: Secure content transmission using DTCP-IP

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 protect content as it moves across the local home network. In accordance with the CVP-2 specifications, digital content can be shared securely between products in a user's home, but not with third parties outside the home network.

Diagnostics:

The DLNA CVP-2 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 cable operator or a user can take appropriate steps to troubleshoot and diagnose service-related issues. The CVP-2 diagnostics feature relies on UPnP Device Management [11] as a required functionality, and IEEE 1905.1 [12] 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-5 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 [13] as a required service and UPnP Configuration Management Service v2 [14] as an optional service. DLNA CVP-2 Specifications requires certain actions to be implemented, such as Ping, Trace Route, and NSLookup. Both the CVP-2 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 CVP-2 device profiles, although it is expected that a Diagnostics Controller may be included on a CVP-2 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 CVP-2 server using a TR-069 or SNMP management interface. Alternatively, a cable operator technician or end-user may access the diagnostics application through a browser or screen interface as shown in Figure-5.

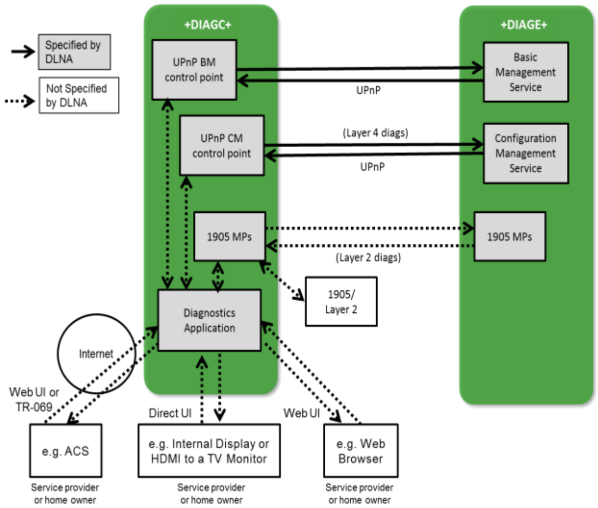

Figure-5: CVP-2 Diagnostics Architecture

<u>Low Power:</u>

To account for service provider STB/video gateway devices implementing energy saving operations, e.g., different levels of sleep modes, the DLNA CVP-2 specifications provide wake-up or reservation mechanisms to CVP-2 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 CVP-2 Low Power feature is based on the UPnP Energy Management Service [15].

Power savings is modular within a physical device. In the context of DLNA networked devices, as shown in Figure-6, 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 CVP-2 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 CVP-2 Server is required to implement Low Power Endpoint (+LPE+) capability, and the CVP-2 Client is required to implement Low Power Controller (+LPC+) capability. This enables CVP-2 Clients to query information about power save mode operations of a service provider's CVP-2 Server and invoke appropriate actions to wake-up the CVP-2 Server when its services are needed for the consumer. Waking up a CVP-2 Server from the low-power mode can introduce some latency and longer response time, so it is expected that a CVP-2 Client provides appropriate messages to the user to provide a good user experience.

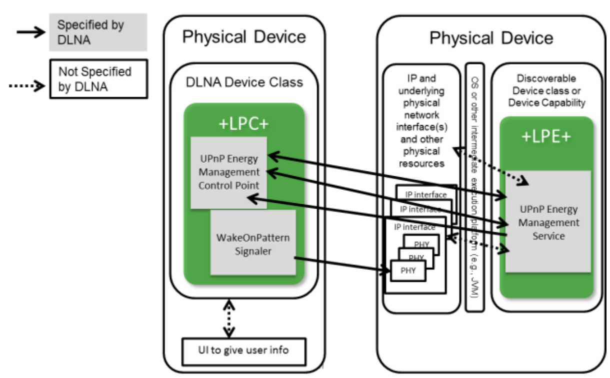

Figure-6: DLNA Low Power Architecture

<u>HTTP Adaptive Delivery:</u>

The HTTP Adaptive Delivery feature of CVP-2 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 [16]. Additionally, DLNA CVP-2 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.

Different logical entities of the HTTP Adaptive Delivery feature are shown in Figure-7.

CVP-2 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 CVP-2 Servers, but if it is supported, then the CVP-2 Server is required to support at least one of the HTTP Adaptive media format profiles.

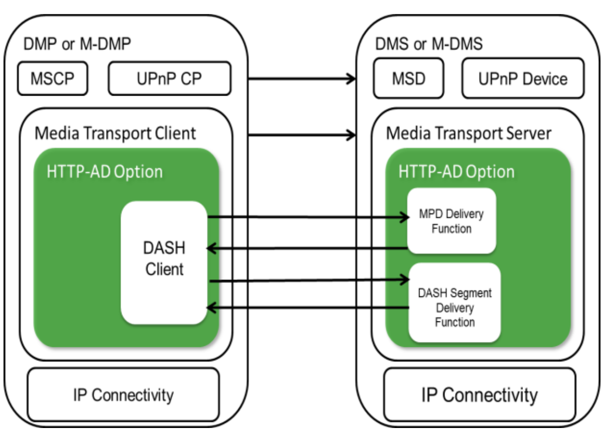

Figure-7: HTTP-Adaptive Delivery Entities

On the CVP-2 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 CVP-2 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 CVP-2 Authentication feature, service providers can verify that the CVP-2 client has been certified to the DLNA CVP-2 specifications. This provides confidence to service providers that a CVP-2 Client is able to display their HTML5 RUI guide, meet regulatory requirements, and deliver content services appropriately to meet consumer expectations.

The CVP-2 authentication feature also supports authentication of a CVP-2 Server by a CVP-2 Client. A CVP-2 Client can optionally authenticate a CVP-2 Server to ensure that the Client is talking to a legitimate CVP-2 Server to protect consumers from rogue servers.

Upon DLNA certification of a CVP-2 device (Client or Server), a device manufacturer obtains a DTLA CVP-2 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 CVP-2 certified. The same certificate is used by the device for CVP-2 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 CVP-2 X.509 certificate from DTLA.

DLNA CVP-2 Authentication uses Transport Layer Security Supplemental Data (TLS-SD) extensions, defined in RFC 4680 [17], to carry CVP-2 client's DTLA CVP-2 certificate over Hypertext Transfer Protocol over Transport Layer Security (HTTPS). Standard Transport Layer Security [18] protocol only supports transport of X.509 certificates. A TLS-SD extension allows transport of arbitrary pieces of information over the TLS protocol.

The HTML5 RUI browser implemented by the CVP-2 Client is responsible for performing authentication using HTTPS with cable operator Authentication Server. Cable operator Authentication Server verifies that the device requesting service is a DLNA Certified CVP-2 device based on the DTCP CVP-2 certificate supplied using the DLNA CVP-2 authentication protocol.

Figure-8 shows various CVP-2 authentication logical 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.

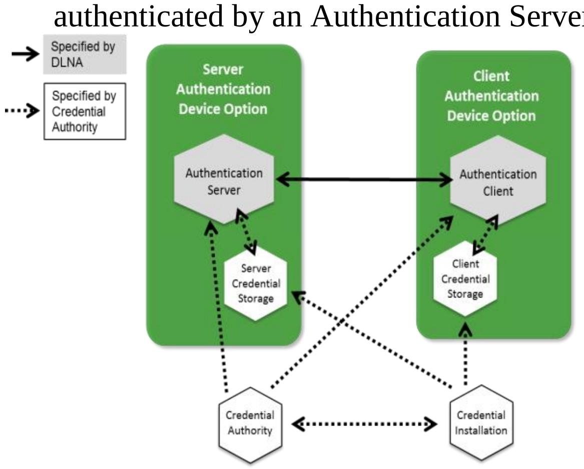

Figure-8: CVP-2 Authentication Entities

- 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 CVP-2 Authentication supports two different scenarios for the Client/Server Authentication:

1. In the first scenario, shown in Figure-9, 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 CVP-2 certificate and client uses DTLA CVP-2 certificate.

2. The second scenario is shown in Figure-10, 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 CVP-2 certificate, and client uses DTLA CVP-2 certificate.

<u>Other CVP-2 Features:</u>

- **Digital Media Server (DMS)**: CVP-2 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).

- **Digital Media Player (DMP)/Digital Media Renderer (DMR):** CVP-2 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 CVP-2 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 CVP-2 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.

- **3D Media Formats:** DLNA CVP-2 specifications conditionally mandate support for 3D media formats for CVP-2 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 CVP-2 client supports rendering of 3D video, then it is required to implement support for these DLNA defined 3D media formats.

CVP-2 DEPLOYMENT SCENARIOS

The DLNA CVP-2 Specifications support two deployment scenarios: Hybrid In-Home + Cloud scenario, and In-home only scenario.

Hybrid In-Home + Cloud Scenario:

In the hybrid In-home+Cloud Scenario, the cable operator's HTML5 RUI server and authentication server reside in the cloud, but all other functions of CVP-2 server reside on an in-home video gateway or STB. A CVP-2 Client discovers URL of the cable operator's cloud guide from an in-home CVP-2 gateway/STB. The CVP-2 Client is authenticated with a cloud Authentication Server, which may be co-located with the cloud RUI server (server uses trusted X.509 CVP-2 certificate). Upon authentication, the CVP-2 Client downloads cable operator 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 CVP-2 Client.

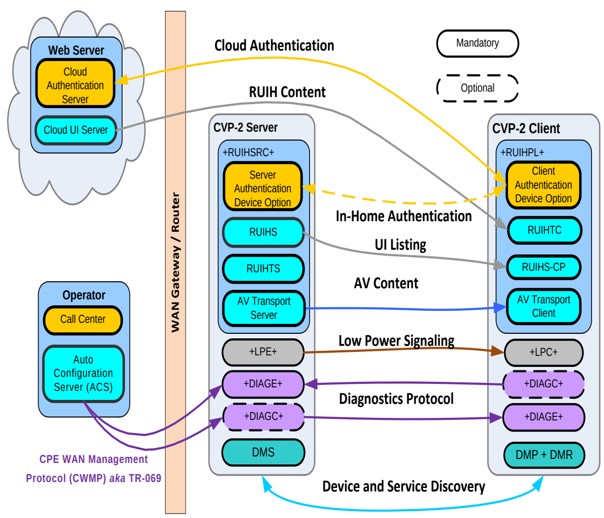

Figure-9: Hybrid In-home + Cloud Deployment

In-Home Only Scenario:

In the In-home only deployment scenario, the cable operator's HTML5 RUI server and Authentication Server reside in the in-home gateway/STB along with all other CVP-2 Server functions. A CVP-2 Client discovers URL of the cable operator's guide from an in-home CVP-2 gateway/STB, which is served from within the home from the same gateway/STB. The same gateway/STB also hosts the Authentication Server.

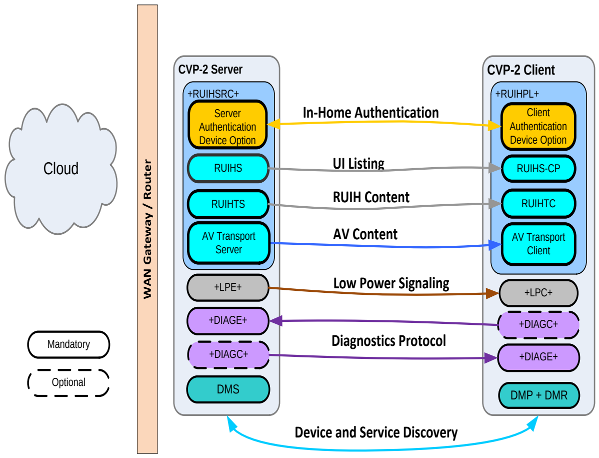

Figure-10: In-home only Deployment

The CVP-2 Client is authenticated with the in-home Authentication Server (the server uses self- signed or trusted X.509 certificate signed with CVP-2 certificate). Upon authentication, the CVP-2 Client downloads cable operator HTML5 guide to access content services from the in-home gateway/STB CVP-2 Server.

OPEN SOURCE IMPLEMENTATIONS

CableLabs, in partnership with industry participants such as Intel and ARM, has developed open source implementations of CVP-2 Server and Client [4]. These implementations are aligned with libraries used by Reference Device Kit (RDK), an integrated software platform initiative for cable operator customer premise equipment (CPE) led by major cable operators in the U.S. and Europe [5]. The main objectives for the CVP-2 open source implementation efforts are as follows:

- Provide reference devices to DLNA to help launch CVP-2 certification program
- Provide reference devices to the industry for testing and development of CVP-2 products
- Foster CVP-2 adoption and speed time to market

The following sub-sections provide an overview of open source implementations of CVP-2 server and client.

CVP-2 Server:

CableLabs' open source CVP-2 Server implementation is Linux-based and built on the same libraries as RDK (e.g., gUPnP, OpenSSL, etc.), so that it can potentially be integrated in the RDK. Figure-11 shows various components used by the CVP-2 server. Rygel, an open source DLNA DMS implementation provided as a part of the Gnome project [19], is the foundation for the CVP-2 Server. CableLabs developed CVP-2 specific extensions to Rygel such as UPnP RUI Service, Diagnostics, and Low Power. As a part of this project, CableLabs also provided upstream contributions to the OpenSSL library to include support for TLS-SD to enable carriage of DTLA CVP-2 Certificate over HTTPS for the purposes of CVP-2 authentication. The CVP-2 Server implementation also supports an Apache-based web server for delivery of HTTP-Adaptive content and serving of HTML5 RUI content.

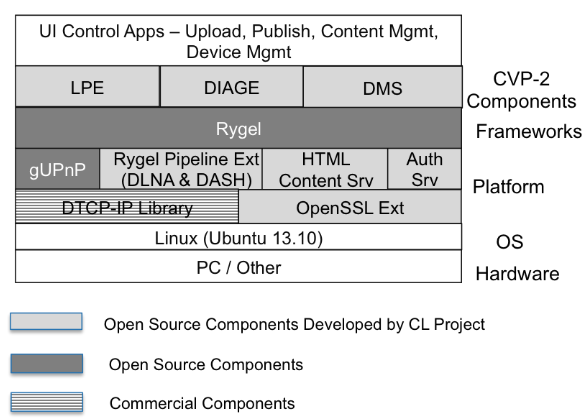

Figure-11: CVP-2 Server Implementation Components

As shown in Figure-11, CVP-2 Server implementation uses a commercial DTCP-IP library. Due to DTCP-IP requirements and content protection/encryption needs, open source implementation of DTCP-IP is not available. Thus, DTCP-IP stack is not part of the open source distribution of CVP-2 Server. However, the open source implementation of CVP-2 Server provides appropriate APIs so that vendors can include their own DTCP-IP library to have a complete CVP-2 Server solution that includes DTCP-IP support. CableLabs' CVP-2 server implementation is available at [4].

CVP-2 Client:

CableLabs' open source CVP-2 Client is Linux-based and built on the same libraries as RDK (such as gUPnP, Gstreamer, and WebKit). The CVP-2 Client also uses Rygel to provide basic DLNA functionality of Digital Media Renderer. It uses dLyena [20], which is an open source project by Intel that provides UPnP control point functionality for implementation of DLNA Digital Media Controller (DMC) and DMP. CableLabs, in partnership with Intel, developed extensions to dLeyna to support CVP-2 specified features such as Low Power Controller and Diagnostics Controller. Figure-12 shows the CVP-2 Client different software components.

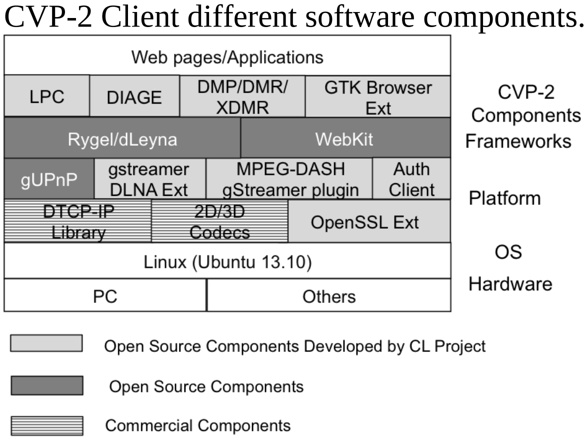

Figure-12: CVP-2 Client Implementation Components

HTML5 RUI browser implementation that meets DLNA CVP-2 requirements is the key component of the CVP-2 Client implementation. Figure-13 shows the details of the HTML5 RUI browser implementation that is part of CableLabs' CVP-2 Client. The HTML5 RUI browser uses WebKit [21] and GTK [22] at its core. CableLabs contributed extensions to WebKit to support DLNA HTML5 RUI requirements such as mapping of MPEG-2 TS elementary streams carrying TV services such as closed captions, SAP, ETV, and ad insertion.

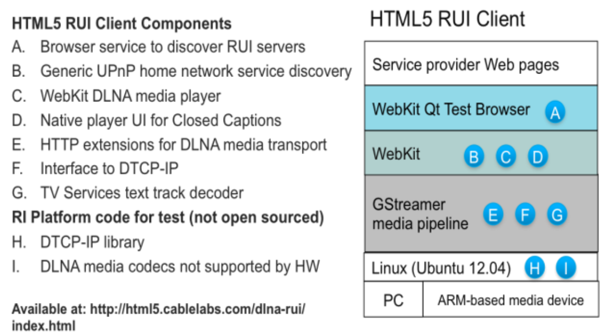

Figure-13: HTML5 Browser Implementation Components

The CVP-2 Client (both HTML5 RUI browser as well as DMP/DMR components) use Gstreamer [23] for media pipeline. CableLabs developed extensions to Gstreamer 1.0 to include support for DLNA streaming with trick modes and DTCP-IP support. CableLabs also developed a Gstreamer plug-in that supports playback for HTTP-Adaptive (MPEG-DASH) content. The CVP-2 client implementation also includes Authentication client, based on OpenSSL [24], that supports client authentication using DTLA CVP-2 certificates. As in the case for CVP-2 Server, commercially available DTCP-IP library is part of the CVP-2 Client implementation and is not part of the open source distribution. The CVP-2 client supports APIs, however, for vendors to plug in their own DTCP-IP library. Similarly, the CVP-2 Client uses commercially available 2D & 3D codecs to include support for required DLNA media formats. CableLabs' CVP-2 Client implementation is available at [4].

CVP-2 BENEFITS

The CVP-2 specifications offer benefits to consumers, service providers, and CE manufacturers alike. Consumers will be able to consume premium subscription TV content such as live/linear HD programs, VoD, and DVR content on devices of their choice anywhere in the home without having to download different platform-specific applications or obtain additional equipment from service providers. A consistent user experience is deliverd across all devices. Using CVP-2, service providers are able to offer all their services to a wide variety of COAM CE devices by maintaining their own user experience on all the devices. Using CVP-2 HTML5 RUI, service providers are able to evolve their services more rapidly and reduce time-to-market for new services and products. Auto service discovery feature supported by CVP-2 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.

CVP-2 authentication provides assurance to service providers and content providers that only certified CVP-2 devices access their services and provides assurance for their user experience on CE devices. CVP-2 offers a single, interoperable solution to CE manufacturers to enable premium subscription TV services from different service providers. This avoids having to develop one-off solutions and platform specific development, which is likely to speed time-to-market for their products.

CONCLUSIONS

The industry has been investigating solutions for enabling premium cable content to retail CE devices in a manner that meets cable operators' contractual, regulatory and business requirements for a long period of time. The DLNA CVP-2 specifications, with its key constituent features such as HTML5 RUI, Device Authentication, a well-defined set of media formats and diagnostics, offers a solution that meets these requirements. It allows cable operators and other subscription TV providers the ability to offer all their subscription TV services with consistent user experience to retail CE devices with different form factors and platforms, without the need for providing additional STBs.

CVP-2 offers consumers more choices in consuming their subscription TV content. With CVP-2, CE manufacturers need to only implement a single unified platform to receive subscription TV content from different service providers. Open source implementations of CVP-2 Server and Client are available to the industry for development and testing of CVP-2 products.

ACKNOWLEDMENTS

The author thanks Ken Barringer, Joan Branham, Jud Cary, Christie Poland, Darshak Thakore, and Eric Winkelman for their review and contributions to the paper.

REFERENCES

[1] Federal Communication Commission's Third CableCARD Report & Order, October 14, 2010 http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-10-181A1.pdf

[2] 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

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

[4] Open Source Implementations of CVP-2 Server and Client, CableLabs, http://html5.cablelabs.com/dlna-cvp-2/index.html

[5] Reference Device Kit, http://rdkcentral.com

[6] HTML5, A vocabulary and associated APIs for HTML and XHTML, W3C Candidate Recommendation 04 February 2014, http://www.w3.org/TR/2014/CR-html5-20140204/

[7] 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

[8] Mapping from MPEG-2 Transport to HTML5, I03, CL-SP-HTML5-MAP-I03-140207, Cable Television Laboratories, Inc. Specifications, Web Technology, February, 7, 2014

[9] Server Sent Events, W3C Candidate Recommendation, 11 December 2012, http://www.w3.org/TR/eventsource/

[10] 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

[11] UPnP Device Management: 2, http://upnp.org/specs/dm/dm2/

[12] 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

[13] 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

[14] 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

[15] EnergeyManagement: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

[16] ISO/IEC 23009-1:2012, Information technology -- Dynamic adaptive streaming over HTTP (DASH) -- Part 1: Media presentation description and segment formats, http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=57623

[17] S. Santesson, TLS Handshake Message for Supplemental Data, IETF RFC 4680, September 2006, http://tools.ietf.org/html/rfc4680

[18] T. Dierks, et al, The Transport Layer Security (TLS) Protocol, Version 1.2, IETF RFC 5246, August 2008, http://tools.ietf.org/html/rfc5246

[19] Gnome's Rygel Project, https://wiki.gnome.org/action/show/Projects/Rygel?action=show&redirect=Rygel

[20] dLeyna Project, Intel Open Source Technology Center, https://01.org/dleyna

[21] The WebKit Open Source Project, http://www.webkit.org

[22] The GTK+ Project, http://www.gtk.org

[23] GStreamer, Open Source Multimedia Framework, http://gstreamer.freedesktop.org

[24] The Open SSL Project, https://www.openssl.org