

Technical Appendix To CVCC Comments
MB Docket No. 16-42, CS Docket No. 97-80
April 22, 2016

Introduction

This Technical Appendix describes the details of a standards-based implementation that would satisfy the three information flows of Service Discovery, Entitlement Information, and Content Delivery as outlined in the NPRM. The details provided track the ex parte submission filed by Public Knowledge for CVCC in MB Docket No. 15-64 on October 20, 2015. The technical references listed below illustrate clearly that existing technologies, with specific minor changes, may be readily formulated to support full compliance with the FCC's objectives and proposed rules. Hence, standards formulation and recognition can and should be expeditious. The functionality of this technology in practice was demonstrated in the CVCC's real-time demonstrations in late 2015 and early 2016, as referenced in the CVCC Comments ("CVCC Comments") to which this document is appended, and by CVCC ex parte submissions in MB Docket No. 15-64. The technologies relied upon in those demonstrations are described below. Development based on the specific details of what is described below is already in progress and will be completed soon, after which a complete specification would be available for reference, as discussed in the CVCC Comments.

Overview

The three data flows are to be provided over a standard wired or wireless IP network, as used in home networks today. The communication between a client (navigation device) and the server (either an in-home MVPD-supplied device or a MVPD-provided web-based "cloud" service) is via a set of widely-deployed protocols with minor changes. The server may communicate with clients directly (i.e., through an existing end-to-end or local IP network), or by any other means made necessary by the MVPD's choices and architecture (e.g., through a proxy device or service). The MVPD may choose its preferred implementation and no additional in-home device is required.

Service Discovery Interface

The Service Discovery Interface provides information on the services and relevant metadata for content. Services supported include linear TV channels (with PPV) and VOD (transactional, entitled, and free). The content metadata includes uniquely identifiable program details, availability, and purchasing information where relevant. Specifics are described in (1) below on implementation of the Service Discovery Interface. The services and metadata are advertised

using the Universal Plug and Play (UPnP) “Content Directory Service”¹ (CDS), which is specified in (1)(d) below.

Parental Control information is included as a required metadata field in the CDS, described in (1)(g) below. Emergency Alert System (EAS) is handled as part of the CDS, described (1)(i) below.

Entitlement Information Interface

Communication of available linear TV and VOD services the user is authorized to receive is included in the CDS. The CDS includes details of the available services the subscriber is authorized to access, and may include details for all content available from the MVPD, which is especially relevant for purchasable content. The server is not required to output content that the subscriber is not authorized to access, but if it does, the content protection methods prevent access to unauthorized content. The Entitlement Information Interface is informational so as to allow the client device to properly indicate to a user what content is already authorized for access and what is not. The Entitlement Information Interface is described in (2) below (the content protection system enforces the entitlement information through secure means).

Content Delivery Interface

The Content Delivery Interface is used to deliver the actual content itself (e.g., linear TV or VOD) to the client device from the server, and is described in (3) below. Through an appropriate content protection method (such as DTCP-IP, DTCP-HE, DTCP-2, Widevine DRM, or PlayReady DRM), the content is protected between the server and clients. The specifications referenced herein contain the technical details about transport of the actual media content between server and clients, which is via Digital Living Network Alliance (DLNA) HTTP Streaming Mode or Dynamic Adaptive Streaming over HTTP (DASH).

Closed captioning data is provided across the content delivery interface by embedding CEA-608² and/or CEA-708³ data into the media stream itself or using sideband SMPTE-TT.⁴

¹ ContentDirectory:4, UPnP Forum, June 30, 2015. Latest version available at: <http://www.upnp.org/specs/av/UPnP-av-ContentDirectory-v4-Service.pdf>

² CTA-608-E R-2014 - Line 21 Data Services

³ ANSI/CTA-708-E - Digital Television (DTV) Closed Captioning

⁴ SMPTE ST 2052-1:2010 Timed Text Format (SMPTE-TT)

Specifics

Overall, the implementation is based on existing DLNA & UPnP specifications.

The following outlines the specific existing technologies used and standards referenced, including Reasonable and Non-Discriminatory (RAND) licensable DRM, and where minor extensions to those standards are needed to facilitate the three information flows from an MVPD implementation:

1. Service Discovery Interface
 - a. Requires DLNA Digital Media Server (DMS) as specified in DLNA Guidelines Part 1.⁵
 - b. Requires Streamable Extended Tuner Support as specified in DLNA Guidelines Part 1.
 - c. Adds vendor-specific UPnP Feature, UPnP State Variable, and UPnP Action for expressing support of multiple tuners and introspection of their usage.
 - d. Requires EPG Controller support via a CDS as specified in DLNA Guidelines Part 1.
 - e. A CDS must provide information on all linear TV channels, EPG for linear TV channels, and VOD and must include all the programs and channels that are accessible via an MVPD's own UI.
 - f. EPG and VOD items in the CDS must provide full metadata that matches what is in the MVPD's UI or provide enough information to look up that content in a licensable third party content database (via an EIDR or enough other information to uniquely identify the content).
 - g. All EPG and VOD items must contain parental ratings information in the CDS via the *upnp:rating* property, which will conform to the ratings specifications as described in CEA-766-D.⁶ Additional ratings data for purely informative purposes may be provided in the *upnp:rating@advice* property.
 - h. Information required for purchasing either transactional VOD or PPV must be provided by utilizing the *upnp:foreignMetadata* property of the CDS. This information will either consist of a URL for performing the purchase process via a web browser or use a vendor-specific UPnP action that may require entry of a customer specific PIN code for directly purchasing the content. Details regarding

⁵ DLNA Guidelines Part 1 - Architectures and Protocols

⁶ ANSI/CTA-766-D - U.S. and Canadian Region Rating Tables (RRT) and Content Advisory Descriptors for Transport of Content Advisory Information Using ATSC Program and System Information Protocol (PSIP)

usage rights for purchased content will be expressed through the CDS using the *res@usageInfo* UPnP property.

- i. EAS events must be transmitted via a UPnP State Variable in the CDS using XML data that conforms to ANSI/CEA-2035 (J-STD-070).⁷
2. Entitlement Information Interface
 - a. Entitlement information must be transmitted as part of the CDS using the *res@allowedUse* property.
 - b. Copy protection and output protection information must be transmitted as part of the DRM or link protection used as specified in 3(b).
 3. Content Delivery Interface
 - a. Requires support for content delivery using either DLNA HTTP Streaming Mode or DASH as specified in DLNA Guidelines Part 1.
 - b. Supports content protection via either DLNA link protection or a RAND DRM technology. DTCP or DTCP-2 may be used for link protection as specified in DLNA Guidelines Part 3.⁸ Common Encryption⁹ should be used for DRM, with support for either Widevine or Microsoft PlayReady DRM clients for key exchange. Alternate DRMs may also be used, as long as they utilize Common Encryption and also provide support for key exchange with either Widevine or Microsoft PlayReady DRM clients.
 - c. When DRM is used for content protection, the DRM license server should be specified in the DASH manifest or be specified in the CDS using the *DRMInfo:foreignMetadata* property. When an in-home MVPD device is used for providing the Service Discovery Interface, then it also must act as a proxy to the DRM license server for the DRM key exchange and perform all authentication with that license server itself. Handling of license acquisition for cloud-based servers is outlined in 5(d).
 - d. Supported media formats are restricted to those specified as part of the CVP-2 (Commercial Video Profile) specification in DLNA Guidelines Part 5.¹⁰
 - e. Closed Captions, Secondary Audio Program (SAP), Video Descriptive Services (VDS) and other accessibility related information will be embedded in the content streams themselves using existing standardized techniques such as CEA-608/CEA-708 for closed captioning and multiple audio language support as part

⁷ ANSI/CTA-2035 (J-STD-070) - Emergency Alert Metadata for the Home Network

⁸ DLNA Guidelines Part 3 - Link Protection

⁹ ISO/IEC 23001-7:2015 Information technology -- MPEG systems technologies -- Part 7: Common encryption in ISO base media file format files; ISO/IEC 23001-9:2014 Information technology -- MPEG systems technologies -- Part 9: Common encryption of MPEG-2 transport streams

¹⁰ DLNA Guidelines Part 5 - Device Profiles

of the MPEG specifications. Additionally support for external closed captioning information via SMPTE-TT will be allowed.¹¹

4. Certificate Handling

- a. All HTTP requests made to the server over any of the three information flows must include an HTTP header that specifies the URL that hosts a webpage that indicates compliance with all the aspects of the Certificate as specified in the NPRM. Requests that do not contain this URL, contain an invalid URL, or contain a URL that has been deemed to be from a non-compliant source should be rejected.

5. Extensions to support use cases with no MVPD-supplied device in the home (this type of implementation will be referred to as cloud-based):

- a. Any implementer who creates a cloud-based server must post on its website the URL utilized to access the Service Discovery Interface (the expectation here is that these URLs will be aggregated by a third party to enable programmatic lookup of them).
- b. Authentication to the cloud-based server located at 5(a) should be done via techniques similar to what MVPDs use for TV Everywhere login (i.e., either automatic or via webpage login with their MVPD credentials). Upon successful login the client should receive an OAuth2¹² token, which should be used in HTTP headers for all further communication with the CDS and content delivery systems. The client should then be redirected to the URL that presents the CDS itself. The OAuth2 token allows the server to be able to identify the subscriber as well as the mode in which the subscriber is accessing the content (i.e. out of home vs. in home, which can be determined by the IP from which the request originated) and then use that to determine what content is accessible. The MVPD should require renewal of this token via performing the login again no more frequently than they require renewal of logins in their own application if they provide an application.
- c. In order to enable delivery of UPnP events from cloud-based servers, an extension to the UPnP event mechanism will be added utilizing WebSockets. This will establish a bidirectional HTTP link to enable clients sending requests to the server and the server also sending events as HTTP requests back to the client (i.e. both endpoints of the WebSocket connection will be an HTTP Server and an HTTP Client where SUBSCRIBE, UNSUBSCRIBE, and NOTIFY messages will be sent).

¹¹ See *Closed Captioning of Internet Protocol-Delivered Video Programming: Implementation of the Twenty-First Century Communications and Video Accessibility Act of 2010*, Report and Order, 27 FCC Rcd. 787, ¶¶ 124-126 (2012).

¹² RFC6749 - The OAuth 2.0 Authorization Framework

- d. When playing back content from a cloud-delivered server, the OAuth2 token obtained in 5(b) will be used to verify access rights. This requires that for DRM license acquisition that the DRM license server authenticate a client and provide credentials for decryption based on that OAuth2 token. Servers may also restrict access based on the trust level of the DRM client implementation for higher-valued content such as 4K or HDR.