



Current Cable Technologies and Architectures

Prepared for DSTAC WG2

March 12, 2015

Presented by: Ralph Brown, CableLabs

Cable Conditional Access System (CAS)

- Cable CA evolved to combine efficiency of broadcast distribution with two-way communication and security needed to provide access control, meet content providers' requirements, and protect against unauthorized (re-)distribution.
 - Broadcast content is shared by all receivers
 - Decryption key is securely delivered only to those receivers entitled to view the broadcast content
- The CA system makes use of cryptographic techniques and secure hardware components (e.g., chips) to achieve these objectives.
 - Copy and redistribution control signals also delivered to receivers
- The CA system implements an end-to-end chain of trust from the content provider through distributor to the subscriber's television.

The CA Trust Model*

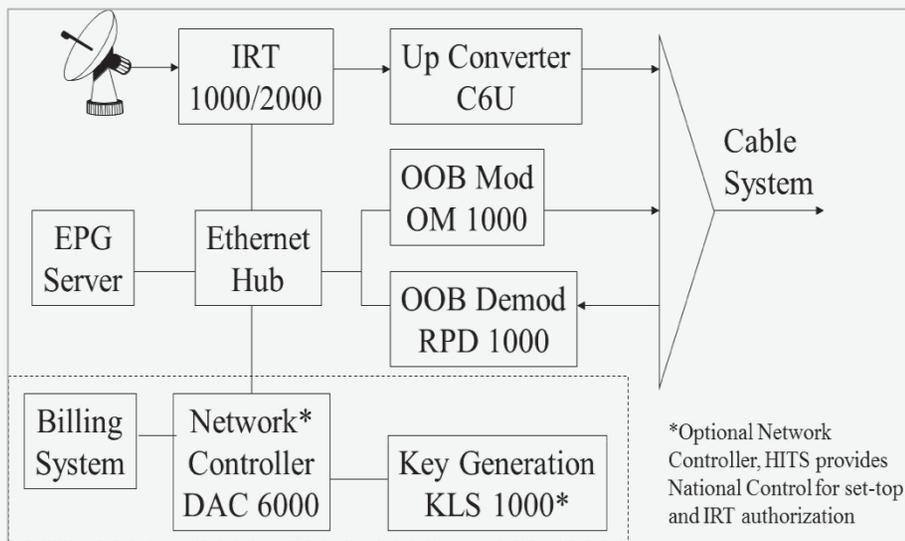
- Specifying and providing the System on a Chip (SoC) and/or manufacturer-based provisioning methods
- Specifying hardware requirements, SoC security firmware OS, software hardening measures, digital certificates
- Secure integration of SoC/OS/SW into receivers
- Copy protection/use restrictions carried through to receiver outputs
- Proactively detecting and disabling potential security threats; countering actual hacks and where possible prosecuting the perpetrators; supplying on-going software upgrades in response to threats/hacks
- Enabling and supporting renewability
- Trust conditions enforced through device licenses, device testing, affiliation agreements, third-party beneficiary clauses
- Trust model assures flow of content from content supplier to the distributor to the consumer

* Source: CableLabs and “The evolution of content protection”, Farncombe White Paper, June 2013.

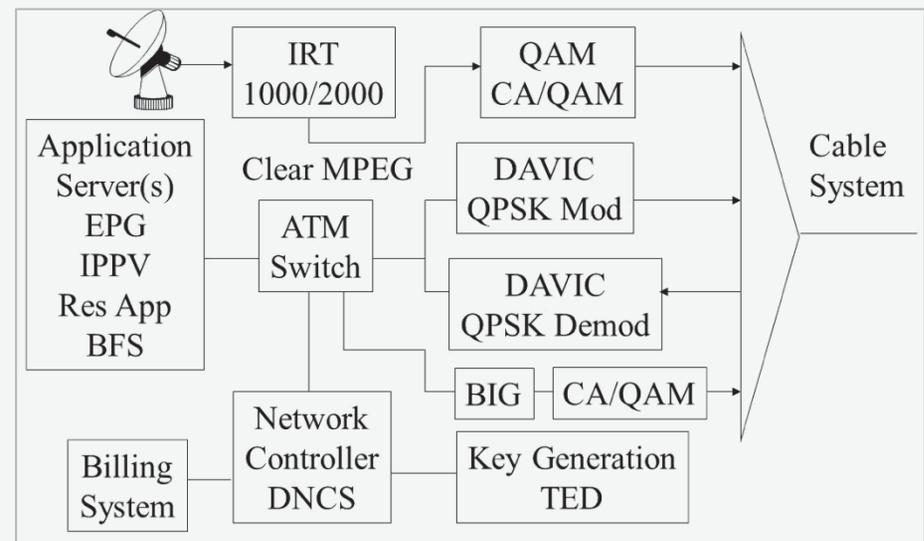
Current Digital Cable Architectures

- Cable systems not built to common spec like Bell System
- Cable Multiple System Operators are roll-ups of different technologies
- General Instruments' (GI now Arris) designed (primarily for TCI) to:
 - Increased channel capacity
 - Minimize head-end cost
 - Centralized set-top control and authorization
- Scientific-Atlanta's (SA now Cisco) designed (primarily for TWC) to:
 - Two-way interactive services, e.g. Video-on-Demand (VoD)
 - Ability to add applications and services to set-top over time
 - Local control and authorization
- Downloadable and OMS

Original Cable Architectures



General Instruments (now Arris)



Scientific-Atlanta (now Cisco)

- MPEG-2 video compression and Dolby® AC-3 audio compression (support for MPEG-4/AVC added later)
- QAM modulation for transmission of MPEG-2 transport streams carrying the audio/video signal
- Data Encryption Standard (DES) encryption for core cipher of CA systems capable of supporting the SCTE 52 2008 DES-CBC variant
- SCTE-65 format to communicate basic channel line-up information, not including channel related metadata

Variable Elements

- Conditional Access (CA) system
 - GI - DigiCipher™ II
 - SA - PowerKey™
- Out-of-band (OOB) communications channels used for command and control of the set-top box
 - GI – SCTE 55-1 (DigiCipher II) – MPEG-2 TS based
 - SA – SCTE 55-2 (DAVIC based) – IP based
 - DOCSIS®-based DSG OOB communications
- Network transport
- Video Codecs (choose among 26+ profiles)
- Specifics of Core Ciphers (DES-CBC vs. DES-ECB)
- Advanced System Information (e.g. network configuration and program guide information)

Variable Elements (continued)

- Session management for PPV, VOD, and SDV applications
- Operating system (OS) and processor instruction set
 - GI – Initially a proprietary kernel on a Motorola 6800 processor
 - SA – Initially PowerTV™ OS on a SPARC processor instruction set
 - Other OS options (LINUX) and processor Instruction sets (MIPS)
- Middleware
- Applications necessary for presentation of services
- Interactive services, t-commerce, interactive video enhancements, application data synchronized with content, switched digital video, diagnostics, advertising, ad reporting, software updates, etc.
- Billing and audit trails
- Proprietary EPG Application and guide metadata formats
- In order for a device to be portable across networks, it must support all of these elements in every variant

Set-top Box CAS Implementations

- SmartCard
 - Separates ECM/EMM processing
- CableCARD
 - Separates ECM/EMM processing and core cipher
 - OOB Channels
 - Separate QPSK front-end (Host) from FEC and MAC layers (CableCARD)
 - Integration of DOCSIS Set-top Gateway (DSG)
 - Only implemented for one-way linear services in retail
 - Implemented for two-way services with common middleware
- Downloadable
 - ECM/EMM processing, other CAS functions done entirely in the secure portion of the SoC
 - Critical rights processing at time of manufacture and in a secure cloud environment
 - Entitlements (and EMMs) are unique for each connected device

Diversity of Digital Video Systems in U.S.

MVPD	CAS	Core Cipher	Transport	Control Channel	Video Codec
Cable	<ul style="list-style-type: none"> DigiCipher 2 MediaCipher PowerKey NDS VideoGuard Conax Nagravision DTA OMS BBT 	<ul style="list-style-type: none"> DES-CBC DES-CBC DES-ECB CSA CSA CSA DES-CBC/ECB CSA/DES/AES AES 	<ul style="list-style-type: none"> QAM/MPEG-2 TS 	<ul style="list-style-type: none"> SCTE-55-1 SCTE-55-1/DOCSIS SCTE-55-2/DOCSIS Generic IP Generic IP SCTE-55-2/DOCSIS In-Band DOCSIS Generic IP 	<ul style="list-style-type: none"> MPEG-2/AVC
Satellite	<ul style="list-style-type: none"> NDS VideoGuard Nagravision Terrestrial free-to-air 	<ul style="list-style-type: none"> DES/AES CSA/DES/AES N/A 	<ul style="list-style-type: none"> QPSK/DSS TS, DVB-S2/MPEG-2 TS QPSK, 8-PSK Turbo/MPEG-2 TS 8-VSB/MPEG-2 TS 	<ul style="list-style-type: none"> In-Band In-Band N/A 	<ul style="list-style-type: none"> MPEG-2/AVC MPEG-2/AVC MPEG-2
Telco	<ul style="list-style-type: none"> Mediaroom DRM MediaCipher/PowerKey 	<ul style="list-style-type: none"> AES CSA 	<ul style="list-style-type: none"> Multicast/Unicast-IP/VDL/FTTP QAM/MPEG-2 TS & IP/BPON or IP/GPON 	<ul style="list-style-type: none"> IP/VDL/FTTP SCTE-55-1/SCTE-55-2 	<ul style="list-style-type: none"> AVC MPEG-2/AVC
Google Fiber TV	<ul style="list-style-type: none"> Widevine 	<ul style="list-style-type: none"> AES 	<ul style="list-style-type: none"> IP/GPON 	<ul style="list-style-type: none"> IP/GPON 	<ul style="list-style-type: none"> AVC

- Each CAS has its own unique licensing and trust infrastructure
- A retail device must be capable of supporting this diversity of elements to be portable across MVPDs

Content Providers' Requirements

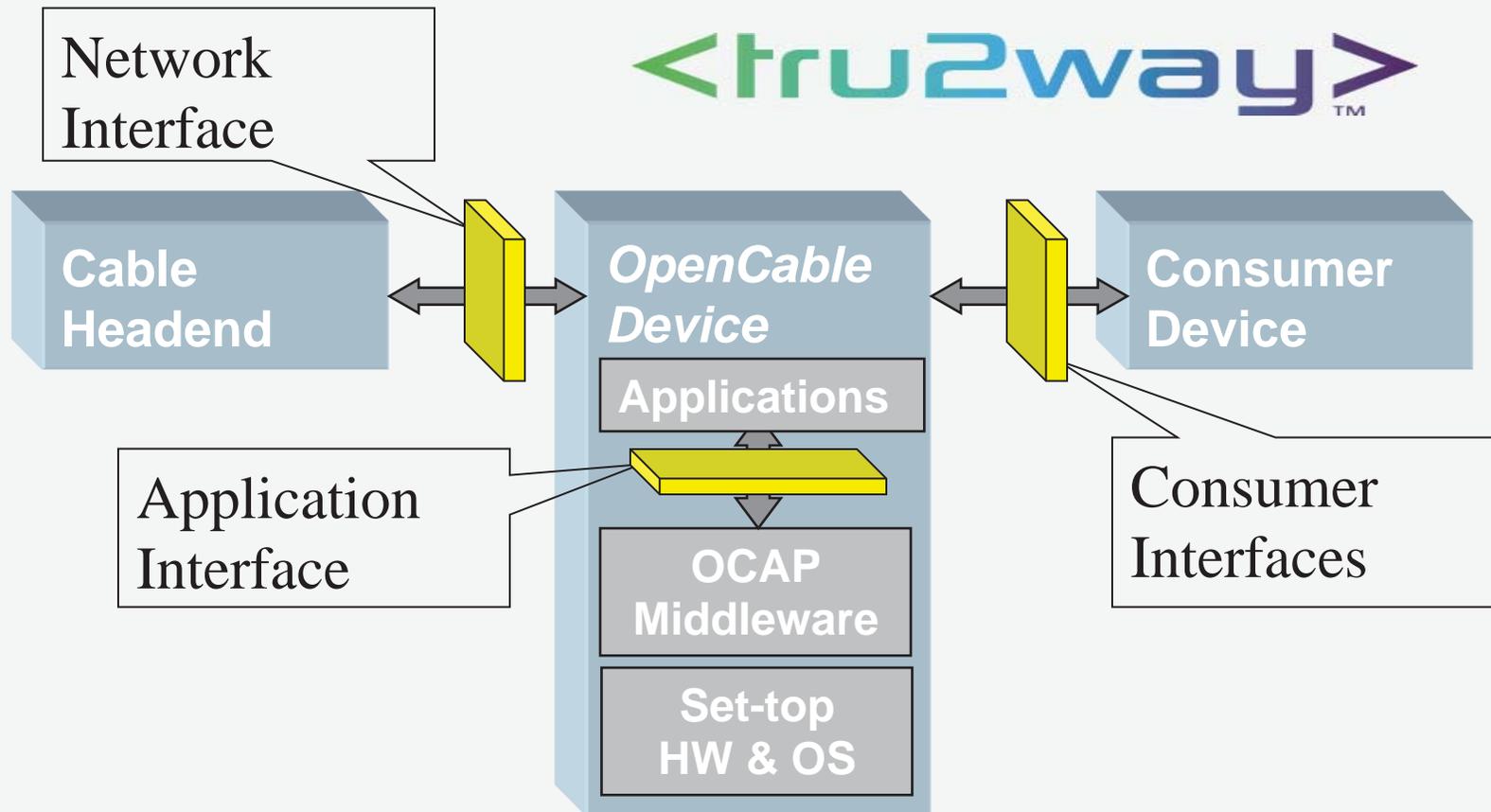
- Commercial video content providers segment the market:
 - Content is generally valued higher closer to its original release than at later dates
 - Content at higher resolution is generally valued higher than at lower resolution
 - Geographic and mobility (OOH) restrictions on distribution or blackouts
 - May segment devices and platforms
- “Windows” specify availability of content on different platforms (theatrical release, airlines, hotels, DVD, cable) over time
- MVPDs have historically built to the highest security requirements to obtain high value content and planned for a 5 to 7 year device retirement /refresh
- Content licenses also define channel position, tier placement, acceptable advertising, scope of distribution permitted, security requirements and consistent presentation of branded content
- Video Distribution Systems, including CAS, must be able to enforce these rules

- High-level requirements for “Enhanced Content Protection”
 - Encryption AES-128 or better
 - HDCP 2.2 or better
 - Selectable output control
 - Secure media pipeline & secure computation environment
 - Hardware root of trust
 - Forensic watermarking
 - Cinavia watermark playback controls
- Corresponding video requirements address 4K and Ultra-HD video

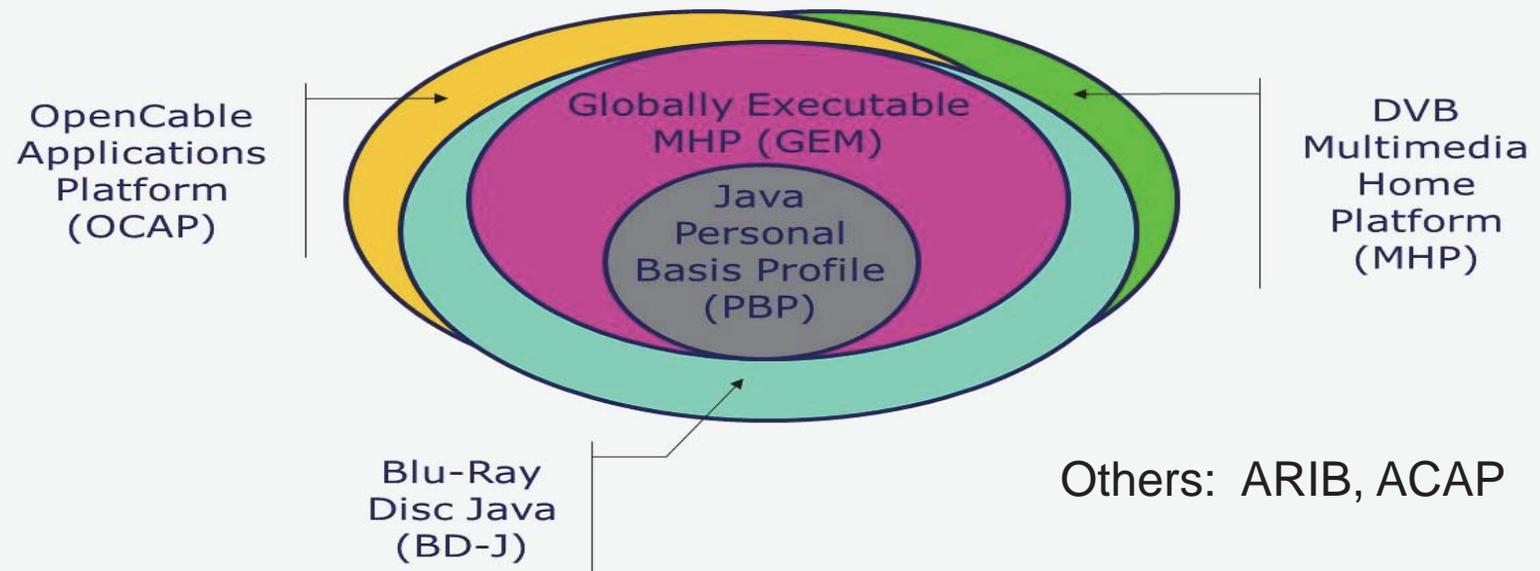
*Source: <http://www.movielabs.com/ngvideo/index.html>

OpenCable Client Architecture

CableLabs®



Common Middleware Approach



Open Cable Host Core Functional Requirements

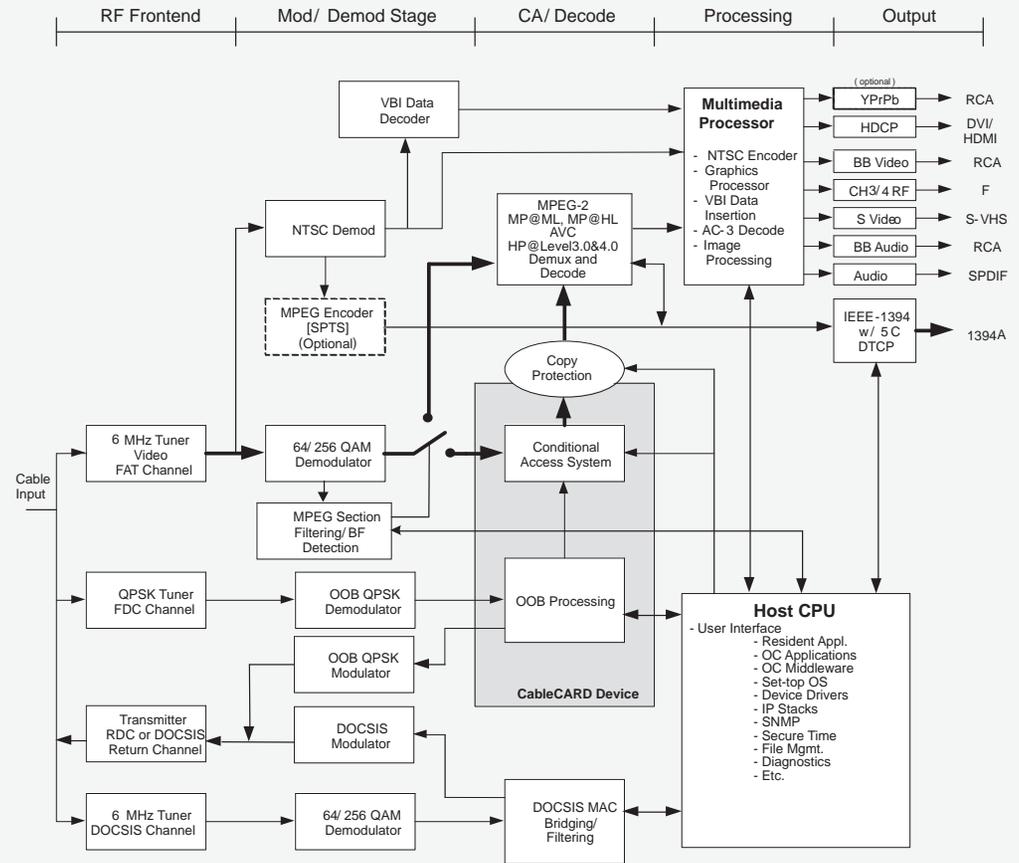


- Host incorporates common functions:

- RF Frontend and MOD/DEMOMOD:
 - QAM & QPSK tuners/demodulators
 - QAM & QPSK modulators/transmitters
 - MPEG-2 TS Demux
 - DOCSIS/DSG MAC processing
- CableCARD Interface:
 - OOB/DOCSIS
 - Copy protection
- Host CPU and Multimedia processing
 - Application execution
 - Audio/Video decode
 - Graphics generation
 - Output controls

- CableCARD incorporates proprietary functions:

- CAS functions
- Copy protection
- OOB Processing



tru2way Market Adoption

- Many cable operators implemented tru2way as common middleware
- Panasonic launched a retail tru2way TV in 2008, but withdrew it from market
- Major CE manufacturers committed to tru2way in 2008, but did not bring product to market

Innovations After CableCARD

CableLabs®

- Start Over™
- Look Back™
- Quick Clips
- U-Verse™
- Remote access to DVR
- Switched digital video
- Addressable advertising
- FiOS™
- Widgets and Video Manager
- Interactive applications within programming
 - Showtime
 - Weather Channel
 - DirectTV NFL Ticket/RedZone
 - HSN Shop-by-Remote
 - RFI ads
- Recommendations
- History
- Personal profiles
- Social apps
- Online photos from Flickr
- Audience measurement
- Network DVR/Whole Home DVR
- Account management (e.g., upgrade subscription package from EPG)
- Voice control
- Search tools
- Sports and news tickers
- Traffic and weather apps
- Android tablets and smartphones, RIM,
- On-screen caller ID and voicemail notifications
- On-screen voice to text playback
- Home control
- Home networking output with remote user interface (RUI)
- Cloud delivery to consumer-owned and managed devices (iOS tablets and smartphones, Android tablets and smartphones, RIM, Kindle Fire, Xbox, Roku, PC, Mac, Smart TV, ...)
- 3D
- UHD

Applications Approach

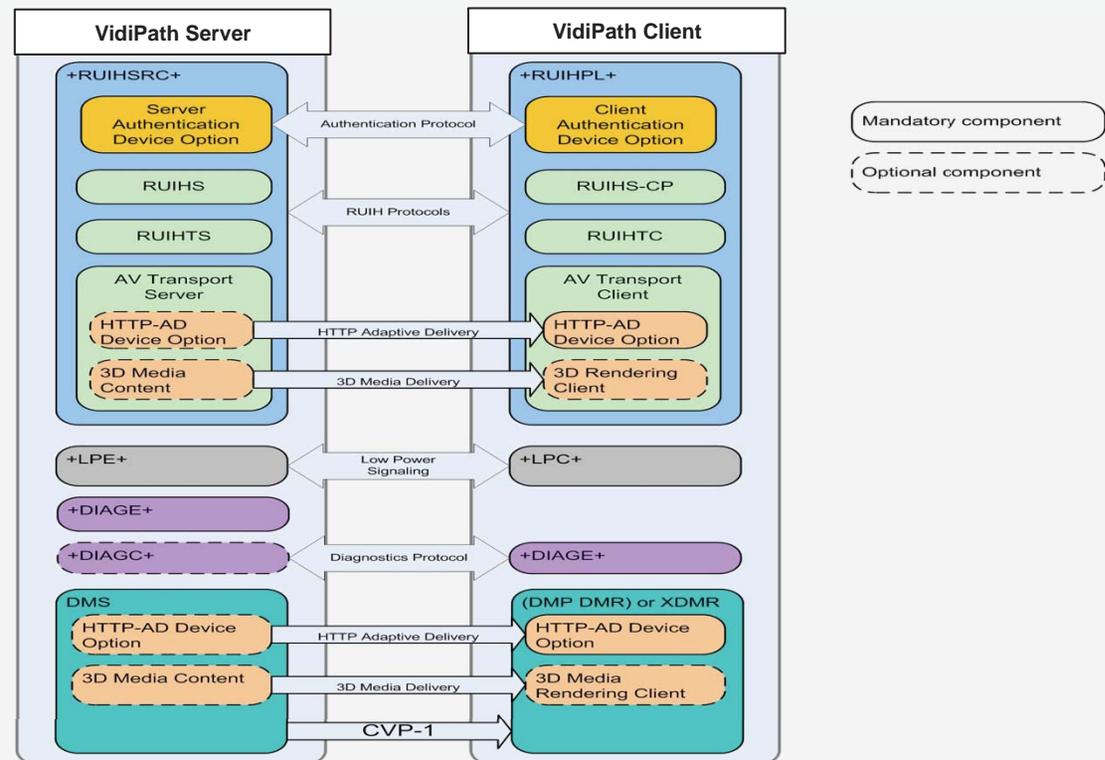
CableLabs®

- With the evolution of the W3C HTML5 and the decline of Java on client devices, the cable industry shifted focus to the evolving technology landscape
- Many cable operators use apps to deliver linear channels plus video-on-demand to various smartphones, tablets, PCs, game consoles, and Smart TVs
- Each video provider appears as clickable retail icon
- Similar to Netflix, Amazon, YouTube, HBO
- Video distributors also have B2B agreements that allow for additional flexibility and experimentation



HTML5

- DLNA VidiPath embraces HTML5 with W3C extensions
- Developed by:
 - Major CE – Samsung, Panasonic, & Sony
 - Chip manufacturers – Intel & Broadcom
 - MVPDs – Comcast, TWC, AT&T, & DISH
- Reference Design Kit (RDK) embraces HTML5



VIDI-PATH™

CableLabs[®]