

# VIDIPATH AUTHENTICATION

Brant Candelore  
Sr. Staff Member  
Sony Visual Products of America  
Sony Electronics

June 2, 2015



**Presented to FCC Downloadable Security Technical Advisory Committee  
Working Group 3 Face-to-face Meeting**

**Note:**

Sony is a promoter company with DLNA, and does not represent DLNA at this meeting. Sony has been active in DLNA and is knowledgeable about VidiPath

Sony is a founder company of DTLA, and does not represent DTLA at this meeting.

**VIDI<sup>™</sup>PATH**

## Contributors in DLNA

Development led by service providers in conjunction with CE manufacturers and technology suppliers.



The DLNA VidiPath project introduces MVPD premium content into the home network.

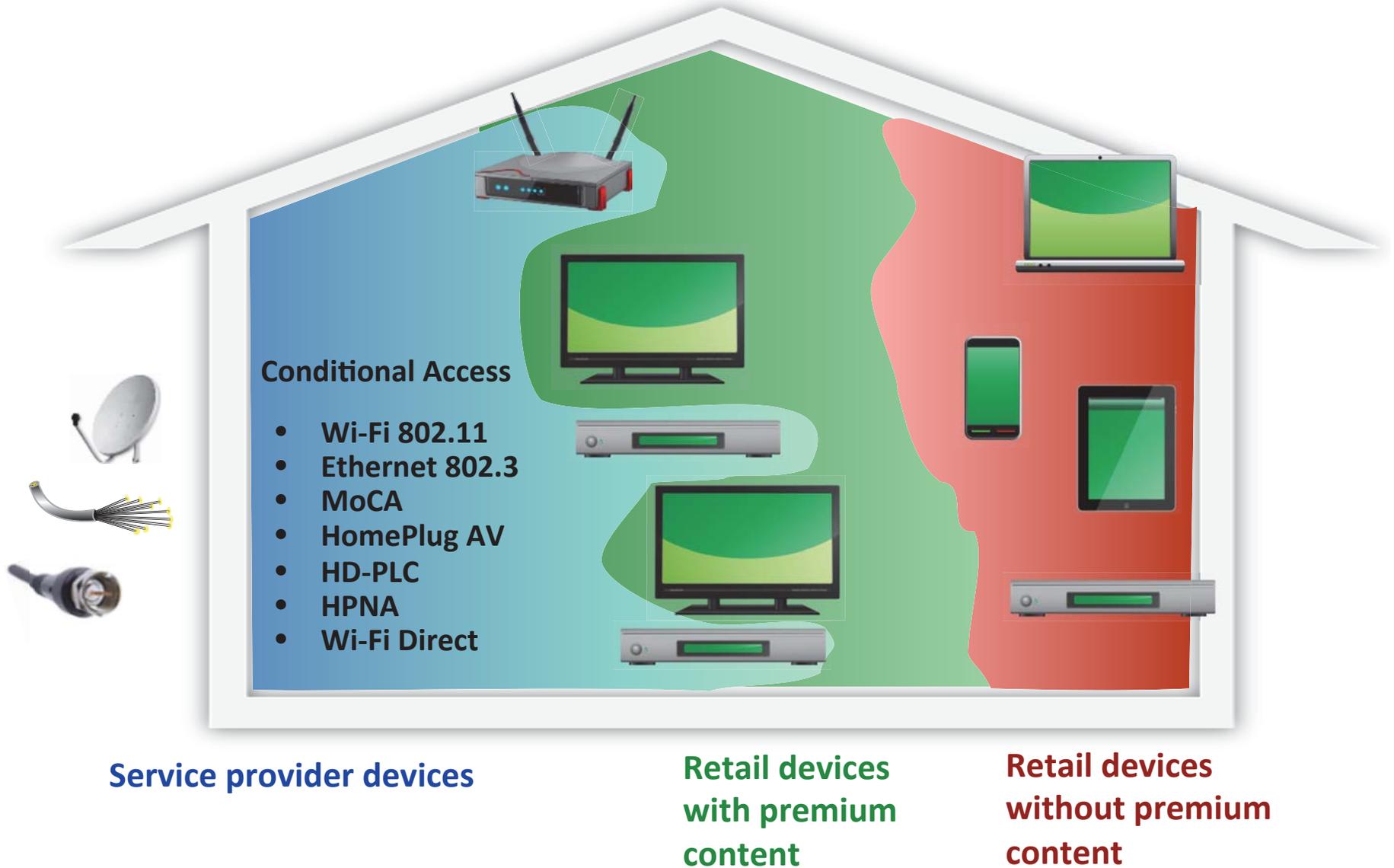
See the DLNA website for an overview of VidiPath:

Webinar/Videos: [www.dlna.org/dlna-for-industry/newsroom/cvp2-webinar-series](http://www.dlna.org/dlna-for-industry/newsroom/cvp2-webinar-series)

Guidelines: [www.dlna.org/dlna-for-industry/guidelines](http://www.dlna.org/dlna-for-industry/guidelines)

The objective of this deck is not to describe the VidiPath project, but rather the novel way that Authentication is performed.

# Yesterday: Service Providers and Retail Devices

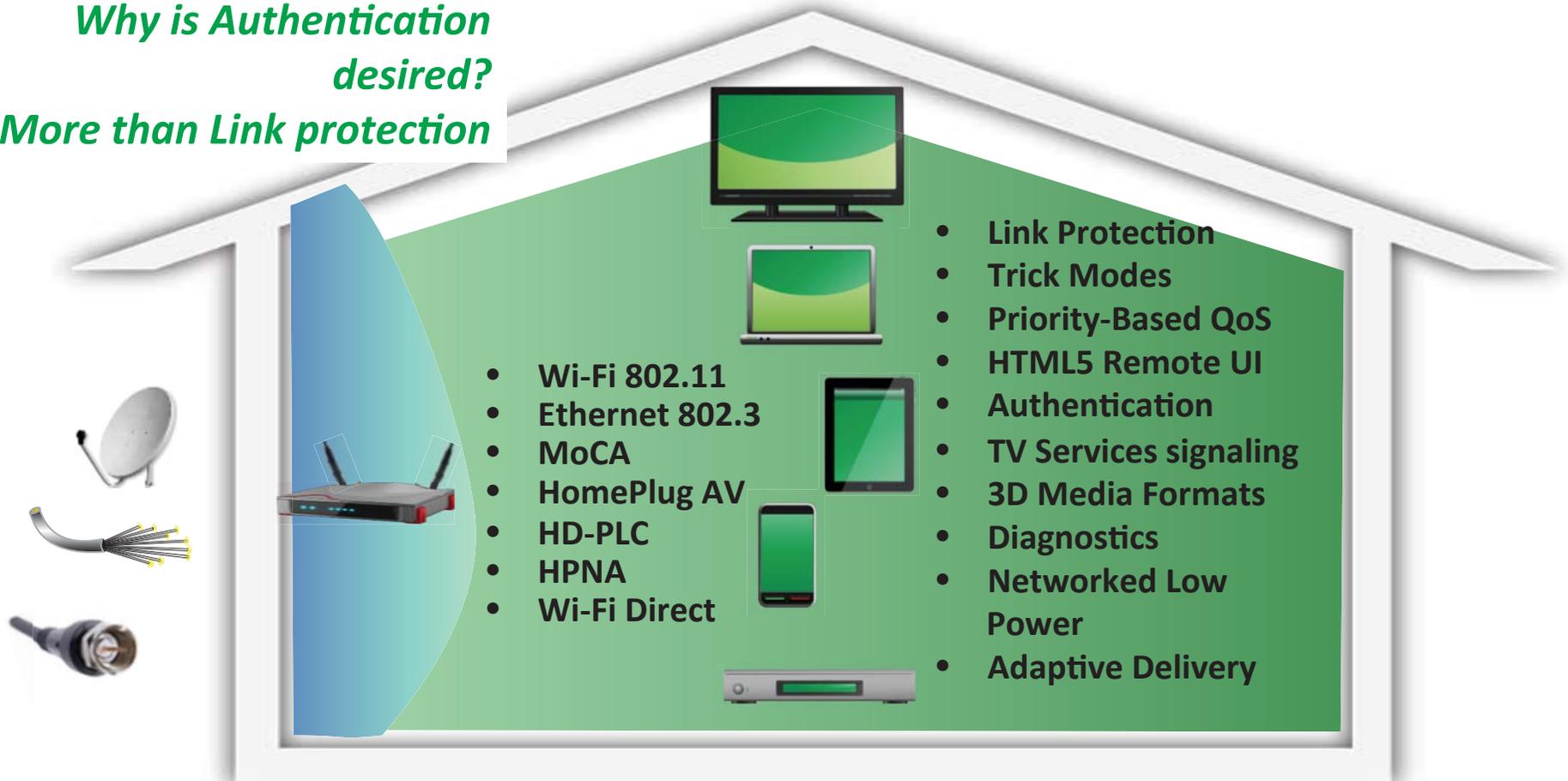


# Today: DLNA Delivers Premium Content to Retail Devices Through VidiPath

However, to provide content to devices, the service operators wanted to verify the functionality of devices receiving their content in order to maintain a QoS and regulatory issues (EAS, CC, Accessibility)

*Why is Authentication desired?*

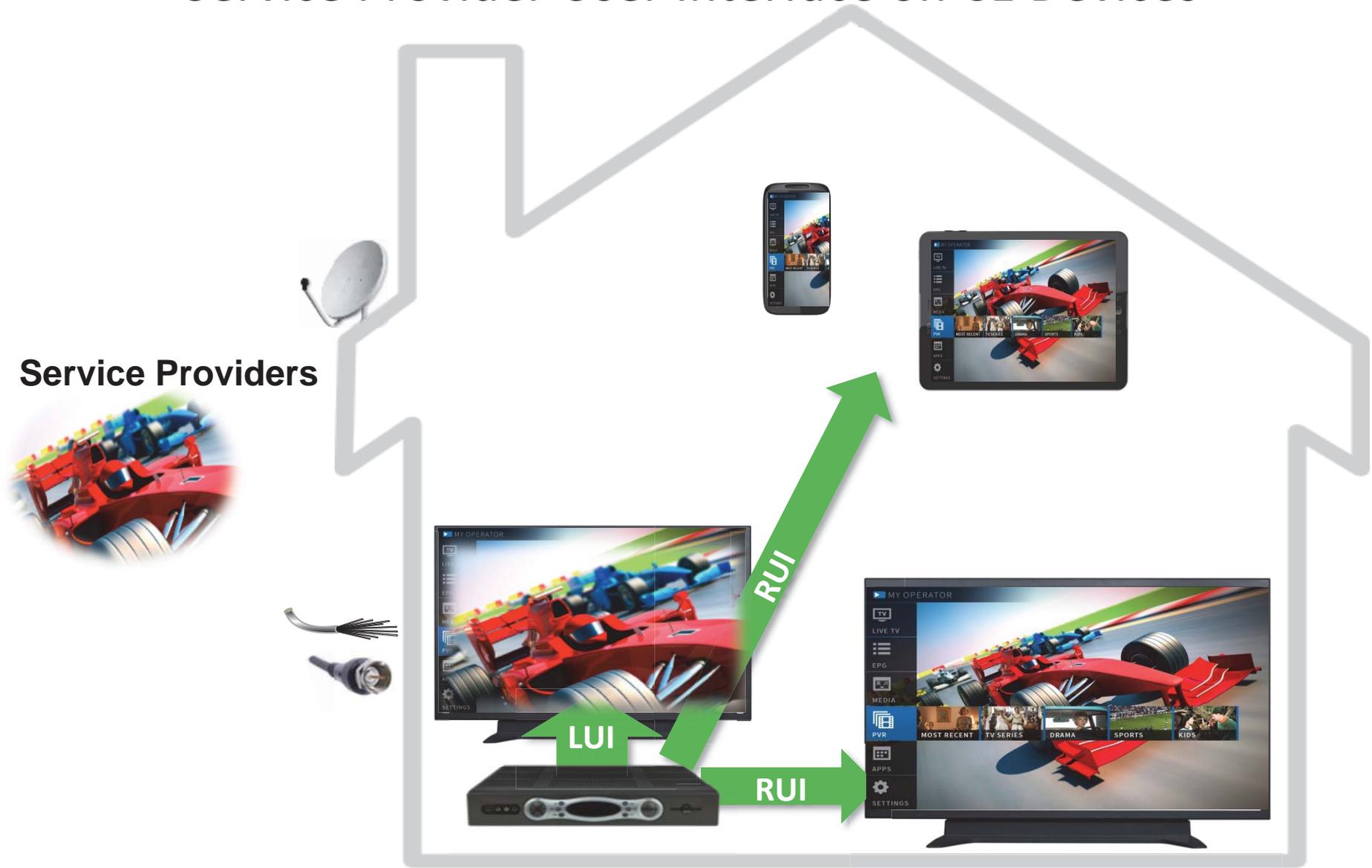
*- More than Link protection*



Service provider device

Retail devices enjoying premium content

# Remote User Interface: Service Provider User Interface on CE Devices



# HTML5 RUI: Renders Service Provider User Interface on CVP-2 Devices



- Enables service providers to render their UIs (e.g. program guide) onto CVP-2 Clients.
- HTML5 RUI profile for DLNA Clients conformant to commercial browsers implementations.
- HTML5 provides a consistent user experience.
- HTML5 allows for a single unified user interface adapted to screen resolution.
- Discovery is based on UPnP Remote User Interface specification.
- Pixel-accurate relies on CANVAS, a HTML5 tag for dynamic, scriptable rendering of 2D shapes and bitmap images.
- Supports the same mandatory trick modes and media format profiles as DLNA Device Classes DMS/DMP/DMR
- Supports presentation of MSO regulatory services such as closed captions, Secondary Audio Programming, Descriptive Video Services

**Extension may be possible that would might allow 3<sup>rd</sup> parties to create independent RUIs**

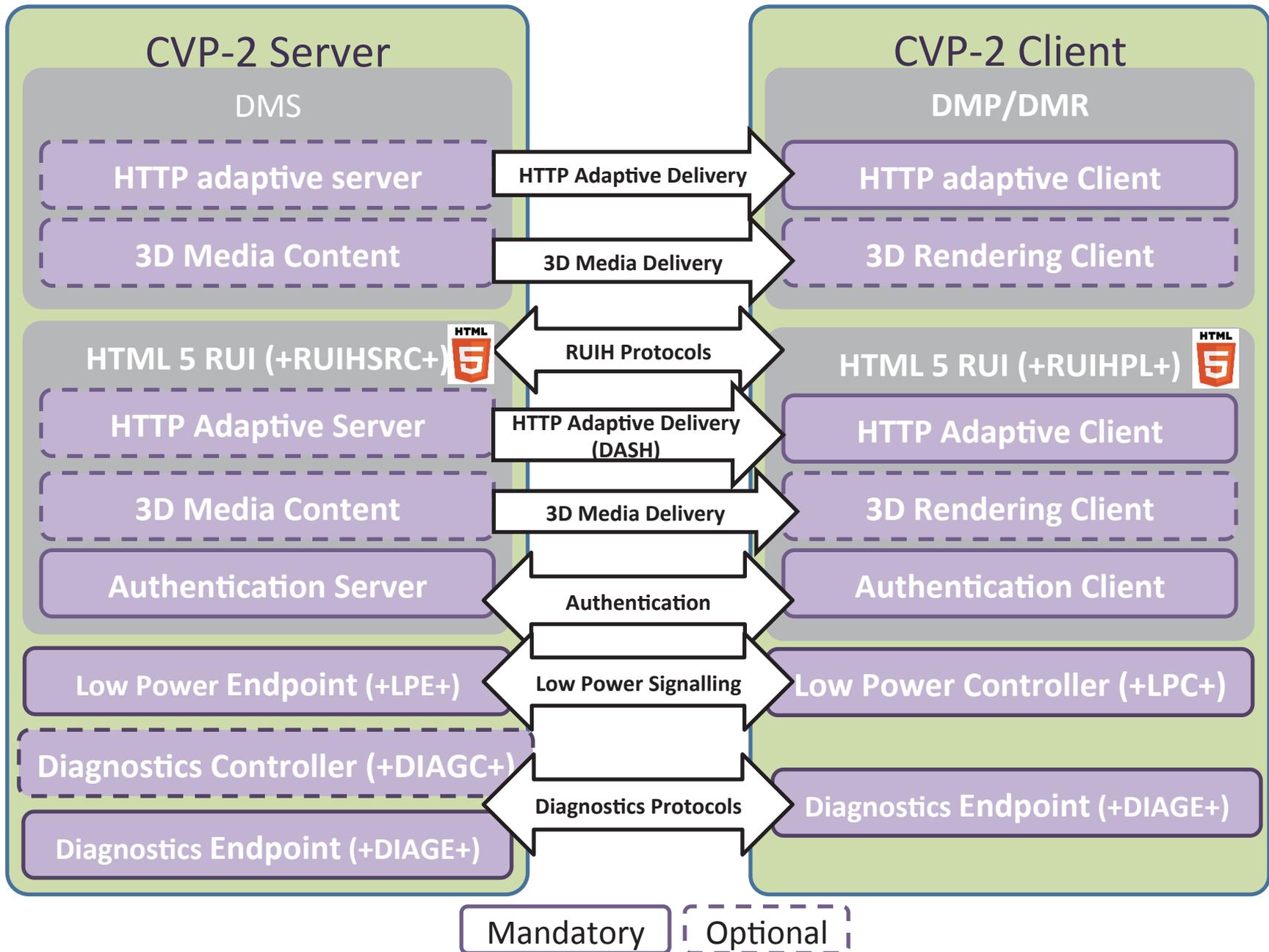
# Authentication: Verifying CVP-2 Functionality



There are two significant aspects to VidiPath authentication:

- CVP-2 Clients “reuse” existing Link Protection DTCP-IP Keys and have extra “CVP-2” bit in Cert
- HTTPS (HTTP over TLS 1.2 with Supplemental Data “Authz” extension) where DTCP certificates can be used to provide trust
  - Browser based
  - Server can be in-home or on the web

# VidiPath Features (DLNA has complete set of Guidelines)



# Authentication: DTCP Method

## In-home Authentication Server

*Are you really a  
CVP-2 client?*

*Are you really a  
CVP-2 server?*

*Client provides  
DTCP CVP-2 Certificate in  
TLS Supplemental Data  
signed with Client's DTCP  
Private Key*

**Service Providers**



←-----→  
HTTPS (HTTP over TLS 1.2)



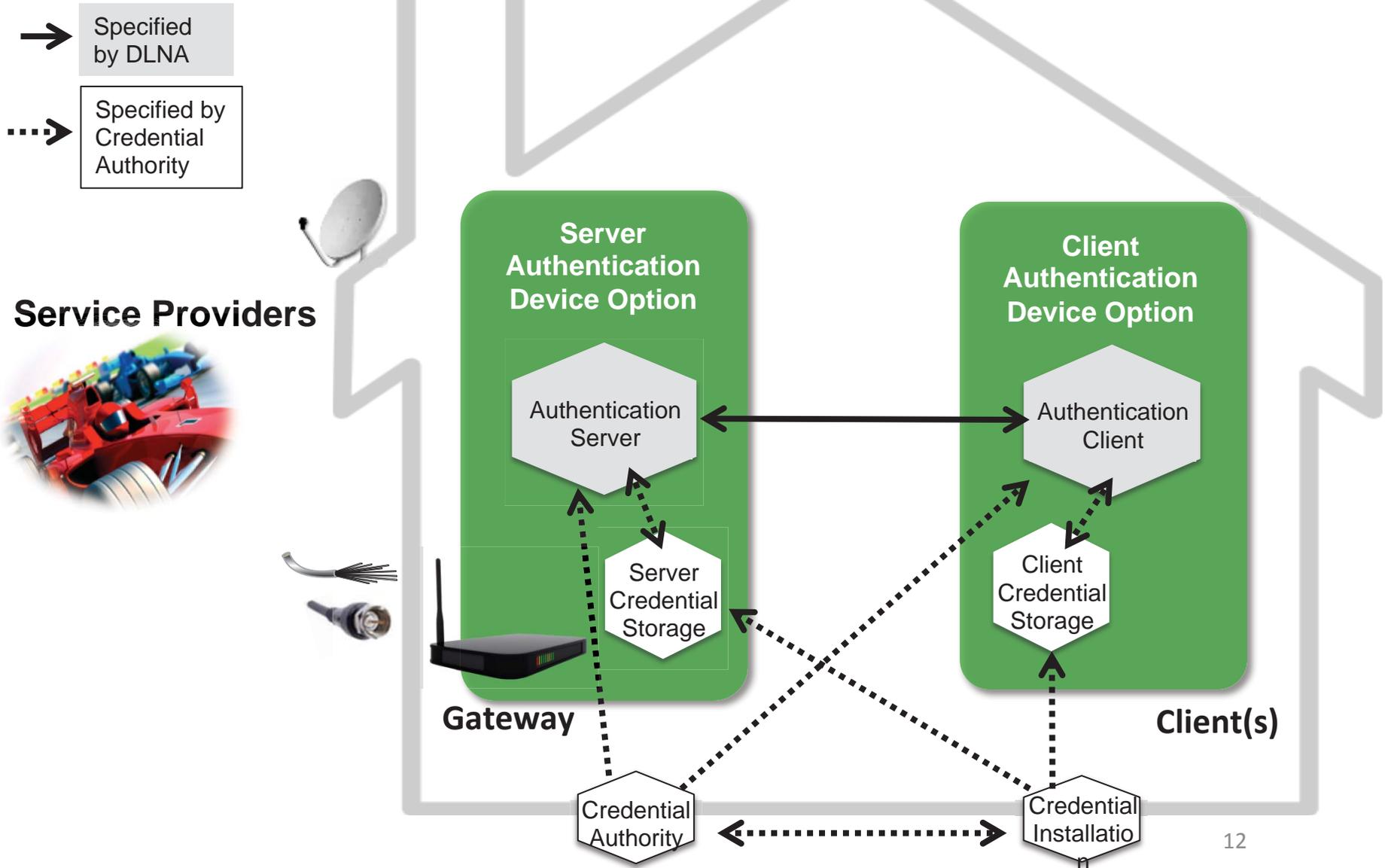
*In-home Server provides  
A Self-signed server X.509 Certificate  
with DTCP CVP-2 Certificate in TLS  
Supplemental Data signed with  
Server's DTCP Private Key*

DLNA Guidelines Part 5 – Device Profiles, Annex A.3, B.3 and B.4

# Authentication: CVP-2 Certificate Exchange

- CVP-2 Clients shall use DTCP CVP-2 Certificate:
  - Same certificate is used for DTCP Link Protection and CVP-2 Authentication.
  - This certificate has the CVP-2 bit set, which indicates that the Client is CVP-2 certified.
- CVP-2 Servers shall use **one** of the following:
  - Option 1: In-home Authentication Server with DTCP CVP-2 Certificate (DLNA Guidelines Part 5 – Device Profiles, Annex A.3):
    - Same certificate is used for DTCP Link Protection and CVP-2 Authentication.
    - Also, a self-signed (non-trusted) X.509 Certificate is used to setup the TLS connection with a CVP-2 client for exchange of DTCP CVP-2 Certificate.
  - Option 2: Cloud Authentication Server with CVP-2 X.509 Certificate (DLNA Guideline Part 5 –Device Profiles Annex A.4):
    - Authentication Server uses trusted CVP-2 X.509 cert provided by DTLA, which is used for both encrypted tunnel establishment between client and server and for server authentication (since it is trusted).

# Authentication: Architecture



# How does this fit with Downloadable CAS?

- Linear and VOD content could be handled via VidiPath and DTCP coming from the Gateway
  - Gateway could be fatter or thinner depending on Client Needs
  - Obfuscates RF attachment, legacy decryption and security details in the Gateway
- VidiPath RUI allows a graceful transition for content coming from the cloud (likely using DASH)
  - Cloud content will be DRM encrypted
  - More and more content may come from the cloud
- Standardization of security interfaces and downloading of DRMs may be important
- DSTAC work is relevant to VidiPath

**THANK YOU!**