



MVPD Security Architectures

Prepared for
FCC's Downloadable Security
Technical Advisory Committee (DSTAC)
Working Group 2

Petr Peterka
Jim Williams

March 19, 2015



MVPD Security Architectures

- ❑ Verimatrix Intro (PP)
- ❑ The business of security (JW)
- ❑ Existing architectures
 - ❑ Overview of security architectures (JW)
 - ❑ Verimatrix CAS multi-rights and multi-network example (PP)
- ❑ MultiRights and Downloadable security requirements (JW)
- ❑ Generalized downloadable security architecture (PP)
- ❑ Allocating responsibilities in this complex ecosystem (PP)
- ❑ Current Industry Solution (PP)
- ❑ Summary (PP)
- ❑ Q&A (PP, JW)

Verimatrix Profile:

Revenue security solutions for multi-network, multi-screen video services

100+ Deployment
countries

23 Awards

6+ Years as IPTV
global number one



\$7Bn+ Revenue protected

800+ Customers/Operators

62M+ Screens protected

110+ Ecosystem Partners

7 Global SIs

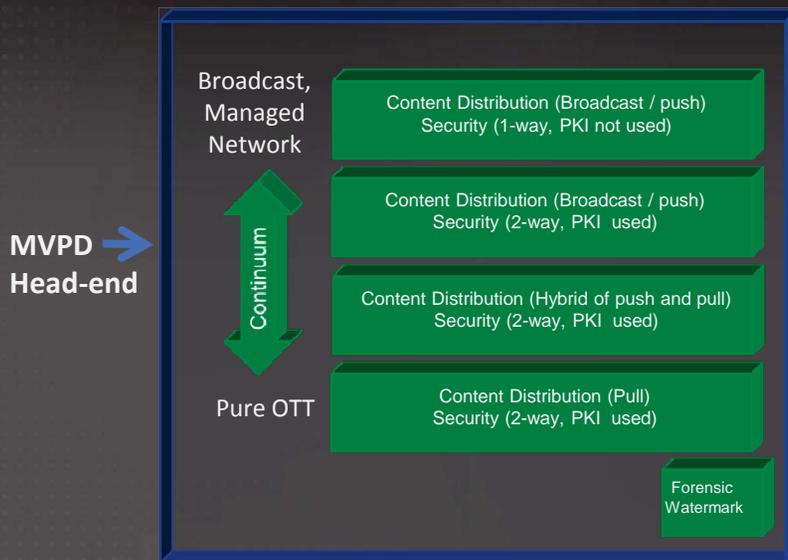
The business of security

- ❑ Service/revenue protection
 - ❑ MVPD-driven
 - ❑ Protect against professional pirates
 - ❑ Thwart theft of service and fraud
 - ❑ Typically provided by CA/DRM vendors including products, services and breach response
- ❑ Content protection
 - ❑ Content owner-driven
 - ❑ Hand off of protection responsibility from MVPD to “approved outputs”
 - ❑ Typically provided by Licensing Authorities
 - ❑ DTCP-IP via DTLA, LLC
 - ❑ HDCP via DCP, LLC
 - ❑ License, compliance & robustness rules, revocation, renewal and enforcement

Overview of Security Architectures



Delivery from MVPD to consumer



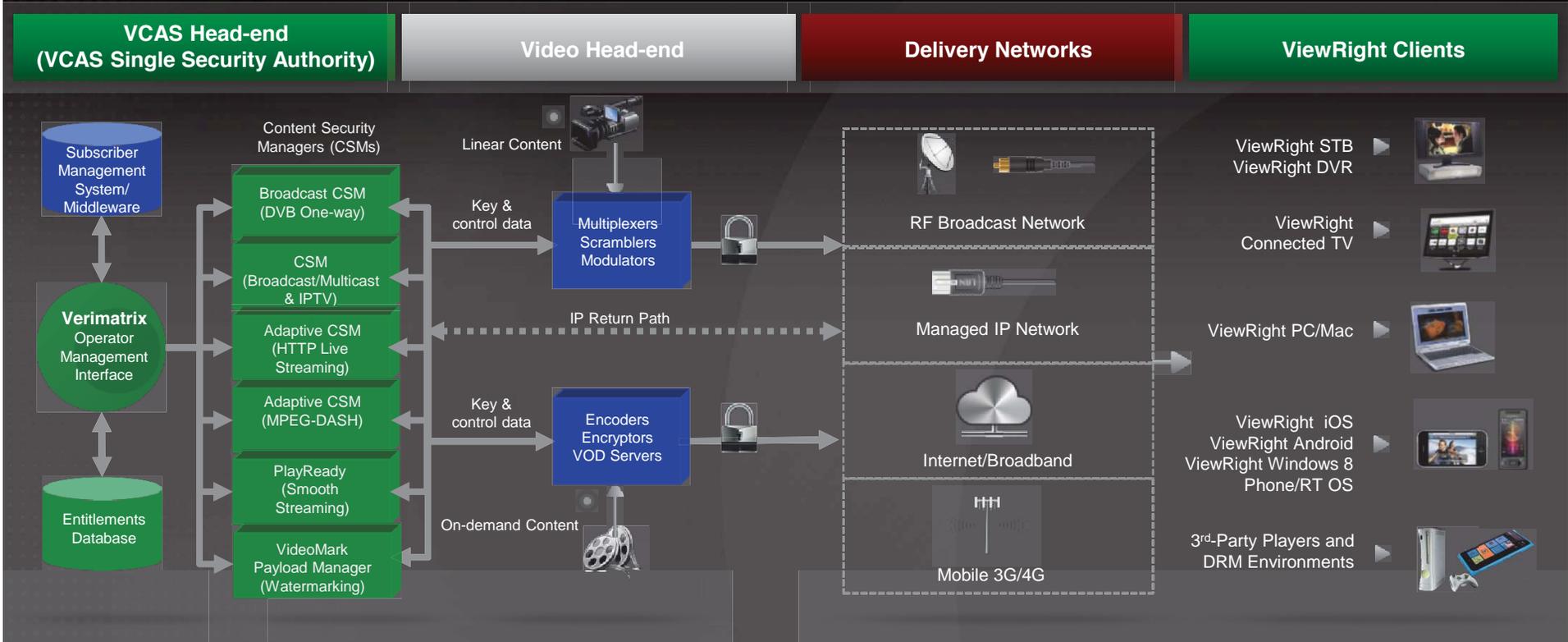
Hand-off of content protection responsibilities



Can MVPDs/others make new offers on already-delivered content?

- Possible with Persistent Protection or UVVU-like system
- Not possible otherwise

Full Verimatrix VCAS™ Multi-network Solution



MultiRights Requirements:

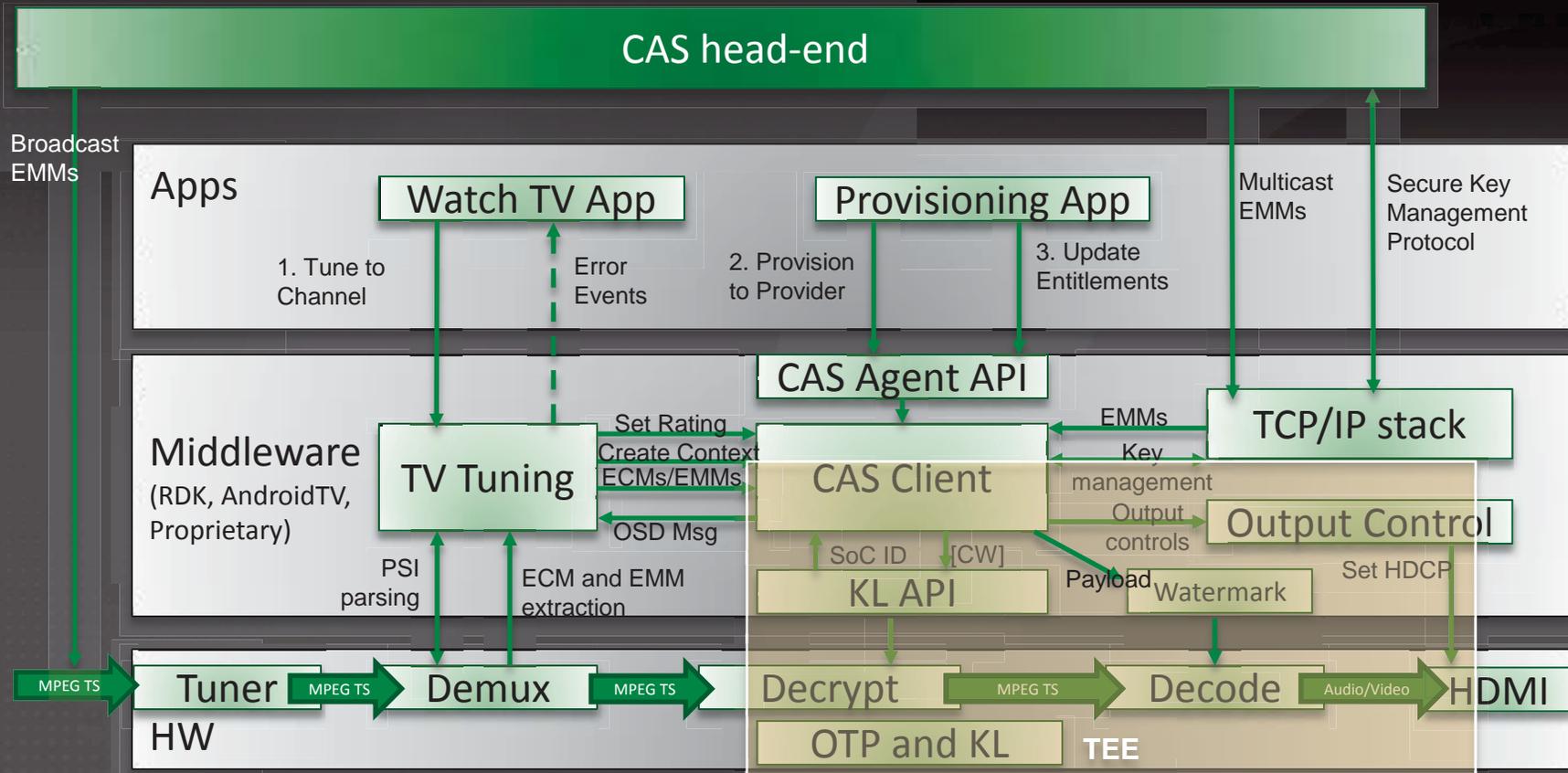
1. Protect content , revenue and service, including both technical and business components.
2. Retain diversity as part of security (multiple CAS/DRM systems).
3. MVPD must support multiple CAS/DRM systems to reach wide range of consumer devices.
4. Allow MVPDs to innovate with new service offerings.
5. Allow OEMs to build consumer devices using well-defined interfaces/APIs with a choice of CAS/DRM systems.
6. Must meet robustness requirements of content owners and CAS/DRM vendors.

Downloadable Security Requirements:



1. Protect content , revenue and service, including both technical and business components.
2. Retain diversity as part of security (CAS/DRM renewal).
3. Allow MVPDs to innovate with new service offerings.
4. Allow MVPDs to select from among multiple security vendors.
5. Allow OEMs to build consumer devices using well-defined interfaces/APIs with clear robustness obligations.
6. Meet robustness and downloadability requirements by combining HW root of trust with renewable SW security

Generalized Downloadable Security Architecture



Application Use Cases:

1. Tuning/Navigation
 - a) Tune to live channel
 - b) Play local DVR recording or network DVR recording
 - c) Play on-demand title
2. Initialization/Provisioning
 - a) Provision to Service Provider X
3. Entitlements
 - a) Entitle Device/Refresh Entitlements
4. On-screen Display (OSD)
 - a) CA/DRM Client may provide messages to be displayed on the OSD
 - b) CA/DRM Client may provide video fingerprinting information

Responsibilities in this complex ecosystem:



1. HW SoC and HAL
 - a) Tuning, demux, decrypt, decode, render/output
 - b) Secure video path
 - c) CAS key ladder (KL), OTP secrets (unique device key, unique device ID)
 - d) Trusted Execution Environment (TEE)
2. Middleware (RDK, Android.TV, HTML5, proprietary, etc.)
 - a) TV tuning functions
 - b) Interactions with CAS client
 - c) Interaction with HAL/SoC HW
 - d) Report platform capabilities to Apps
 - e) Manage multiple concurrent video sessions
3. Application
 - a) Present desired use cases to the user (e.g. EPG, VOD Store, DVR, etc.)
 - b) Interact with platform Middleware
 - c) Interact with CAS Agent

Responsibilities (cont.):



4. CAS Client (proprietary library abstracted by CAS Agent)
 - a) Provides a secure key management protocol to head-end/license server
 - b) Processes ECMs and EMMs (EMMs from MP2TS or from IP Multicast)
 - c) Sets content decryption keys to the descrambler or Key Ladder
 - d) Provides output control settings (e.g. HDCP, DTCP, etc.)
 - e) Manages content rating restrictions (a.k.a. parental control)
 - f) Provides messages and/or fingerprinting for OSD (onscreen display)
 - g) CA configuration and capability (CA system ID, security/robustness level, etc.)
5. CAS Agent
 - a) Common abstraction over a native proprietary CAS Client from a specific vendor
 - b) Exposes CAS functions to Applications

Current Industry Solutions

(not mutually exclusive)

1. MultiRights and App Model:

Operator supports 2 or more CAS/DRM systems

Requirements and standards:

- a) Common Encryption
 - E.g. DVB Simulcrypt, CENC, HLS, UUVU, etc.
- b) Common Signaling
 - E.g. ECM/EMMs, MPEG-DASH MPD/PSSH, HLS playlist key URL, etc.
- c) Common Application Interface
 - E.g. W3C HTML5/EME

2. Downloadable Client:

Device supports 2 or more downloadable CAS/DRM clients

Requirements and standards:

- a) Common HW Root of Trust
 - E.g. SCTE 201 OMS, ETSI K-LAD
- b) Secure download environment
 - E.g. GlobalPlatform Trusted Execution Environment (TEE)
- c) Abstract CAS/DRM API
 - E.g. RDK, Android.TV, TBD

Summary

- ❑ PayTV industry is moving to an IP-based ecosystem
- ❑ PayTV industry is migrating to cardless SW-based CAS/DRM systems
- ❑ Device SOCs provide robust HW root of trust
- ❑ Devices increasingly support TEE and secure SW upgradability
- ❑ Multiple standards allow for open interoperable ecosystem
 - ❑ SCTE, DVB, GlobalPlatform, MPEG-DASH, DLNA, W3C, UUVU, etc.
- ❑ Application model (e.g., TV app store, Play Store, iOS App Store, etc.) is well accepted by consumers
- ❑ Additional choices via home networking standards such as DLNA/VidiPath
- ❑ Consumers have increasing choices of content sources (cable, satellite, IPTV, OTT) and consumption devices (STBs, Connected TV, tablets, smartphones, game consoles)



Thank You!

ppeterka@verimatrix.com