Flexible CAS/DRM Model

… needs beyond content protection and security

Prepared for
FCC DSTAC Working Group 4

Petr Peterka
Jim Williams

June 19, 2015

Context for Verimatrix presentation to WG4

- Verimatrix to WG2 (Mar 19) and WG3 (June 2)
  - In order to avoid the intractable problem of requiring all devices to support all CAS/DRMs, we proposed a two-pronged approach combining a MultiRights head-end and a Downloadable Security system on the client end.
    - Head-ends support multiple DRMs
    - Devices support two or more downloadable CAS/DRM clients
  - Discussed components that need to be standardized and ones that don't
  - Recommended our two-prong approach as a model for DSTAC
- Verimatrix today to WG4 (June 19)
  - ***Needs beyond content protection and security***, holding to our two-pronged flexible CAS/DRM model

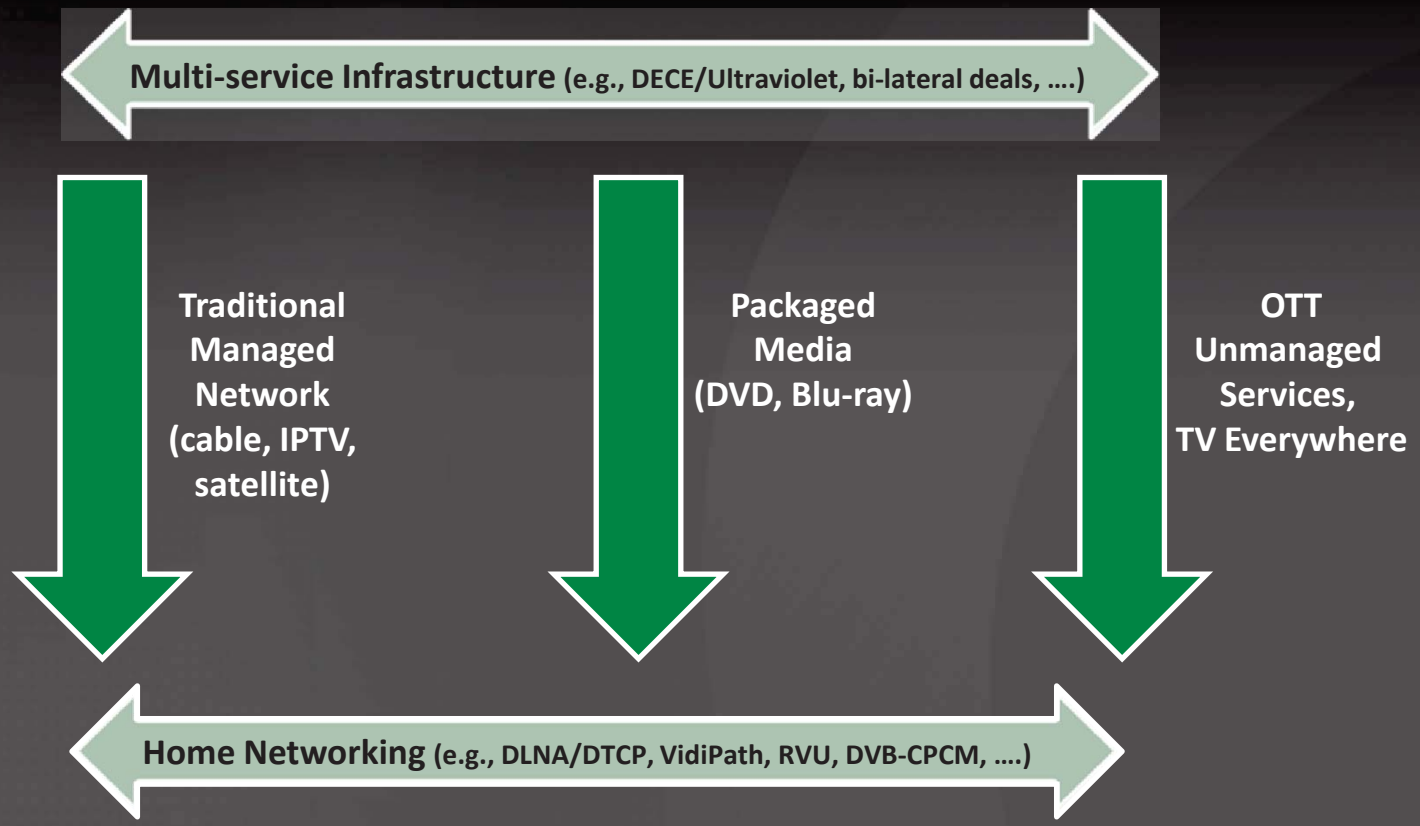
© Copyright 2015 Verimatrix, Inc.

Security models serving content business needs today

- Variety of architectures serving a variety of business models
  - Single proprietary CAS (typically on a managed linear TV service)
  - Multiple CAS systems
    - Using DVB Simulcrypt or equivalent
    - Optionally using standardized HW security (e.g. SCTE 201 OMS)
  - Applications with a single pre-integrated DRM
  - Set of pre-approved DRMs with each device type supporting 1 of them and retailers supporting all of them (DECE/Ultraviolet model)
  - Application model using one of several supported DRMs
    - Pre-integrated into a downloadable application or
    - Pre-integrated into a device accessed via an abstraction API (e.g. W3C EME browser model)
    - Operator supporting multiple DRMs (MultiRights model)
- Not a one-size-fits-all model

© Copyright 2015 Verimatrix, Inc.

Content delivery framework



© Copyright 2015 Verimatrix, Inc.

Reminder of security standardization needs (WG3)

1. To standardize
   a) CAS Client interfaces:
      i. Application API
      ii. CAS Client – Tuning API
      iii. CAS Client – HW Abstraction API (e.g. OMS K-LAD, GP TEE, etc.)
   b) CAS metadata containers (MPEG-2 TS, MPEG-DASH, HLS, etc.)
   c) Content format and encryption (AES-128, CENC, etc.)
   d) Secure OS and downloadability (e.g. GlobalPlatform TEE)

2. To not standardize
   a) CAS system (Authentication, Key management, etc.)
   b) SW/HW hardening (Obfuscation, key derivation, etc.)

© Copyright 2015 Verimatrix, Inc.

Needs beyond content protection and security (WG4)

1. Separation of an application and the underlying DRM
   a) Multiple apps can use a DRM integrated with a device
   b) Ability to innovate on user experience

2. Access to service provider metadata (in standard format)
   a) Ability to search available services/channels and on-demand assets (discovery)
   b) Ability to tune to authorized services
   c) Ability to provide an accurate and reliable single access point for end users

3. Richer rights expression
   a) Move beyond CCI (copy-once, copy-never) to innovate
   b) Ability to upgrade content rights (e.g. upsell rental or DVR recording to EST)
   c) Provide consistent user experience across DRMs and devices

© Copyright 2015 Verimatrix, Inc.

Needs beyond content prot. and security (WG4, cont.)

4. Multi-device domain management
   a) Group device into a user/household domain across DRMs
   b) Richer user experience without illegal sharing

5. Industry and content owner agreed usage models
   a) Consistent domain size (e.g. DECE usage rules)

6. Standardized global asset identification
   a) Entertainment Identifier Registry Association (EIDR)

© Copyright 2015 Verimatrix, Inc.

Needs beyond content prot. and security (WG4, cont.)

7. Flexibility to innovate in the future
   a) Unnecessary regulation must not prevent new use cases (i.e., do not prevent unforeseen future innovation similar to DVR, early release window, etc. in the past)

8. Content providers common robustness rules
   a) Movie Labs Enhanced Content Protection specification

9. Independent 3rd party security and robustness certifications
   a) GlobalPlatform Security Evaluation Secretariat (SES)

© Copyright 2015 Verimatrix, Inc.

Conclusion

- In the area of WG4's purview, DSTAC should highlight/recommend the following:
  - Current trends in standardization are addressing many of these problems
  - Sometimes innovation gets ahead of standardization
  - But forced standardization may miss the mark and stifle innovation

- Verimatrix urges that DSTAC's report
  - Encourage the two-prong approach of MultiRights and Downloadable Security
  - Encourage advances in the necessary security standards presented to WG3 (June 2)
  - Encourage addressing the non-security needs presented to WG4 today (June 19)
  - Not stifle innovation by premature forced standardization on a one-size-fits-all approach

© Copyright 2015 Verimatrix, Inc.

Thank You!

ppeterka@verimatrix.com