MVPD CAS and DRM Trust Infrastructures

Prepared for DSTAC WG2

April 14, 2015

Presented by: Ralph W. Brown, CableLabs

© Cable Television Laboratories, Inc. 2015. Prepared For FCC Downloadable Security Technical Advisory Committee (DSTAC).

Caveats and Acknowledgements

CableLabs®

- The specific implementation of a trust infrastructure, either CAS or DRM based, is unique to that implementation
- This is intended to show many of the various relationships, whether they are through license, contract, transfer of security data, or transfer of hardware/software
- Multiple functions may be performed or provided by the same organization depending on the implementation
- It is not intended to be exhaustive or cover all possible implementations and is intended to be illustrative
- Incorporates input from: Arris, AT&T, Cablevision, Charter, Cisco, Comcast, DISH, Nagra, Verimatrix, and Verizon

© Cable Television Laboratories, Inc. 2015. Prepared For FCC Downloadable Security Technical Advisory Committee (DSTAC).

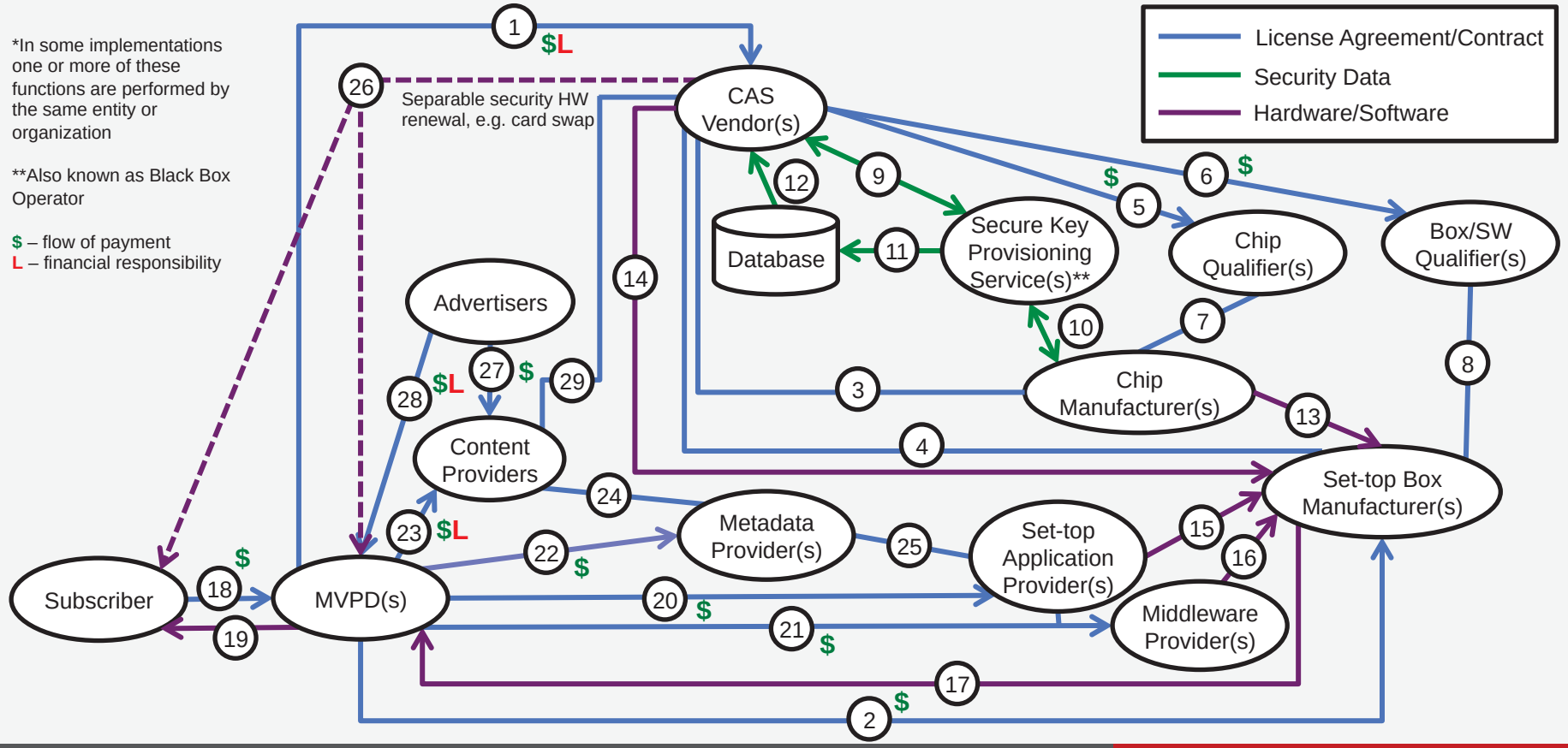
Example MVPD CAS Trust Infrastructure*

CableLabs

*In some implementations one or more of these functions are performed by the same entity or organization

**Also known as Black Box Operator

$ – flow of payment
L – financial responsibility



© Cable Television Laboratories, Inc. 2015. Prepared For FCC Downloadable Security Technical Advisory Committee (DSTAC).

Example MVPD CAS Trust Infrastructure (1 of 10)

CableLabs®

1. The MVPD contracts with a CAS vendor to provide a content protection solution for their network, including breach resolution, warranty, indemnification against IPR infringement, SLA, and other terms that are frequently derived from content licenses. In general, the CAS vendor incurs a financial responsibility for compromises to the CAS system that result in theft of service or theft of content.
2. The MVPD contracts with one or more set-top box vendors to provide set-top boxes incorporating this CAS system, including warranty, indemnification against IPR infringement and other terms. Incorporation of the CAS system can include an embedded secure micro, software, and a robustness specification that must be validated. Again, these terms are often in conformance to content license obligations.

© Cable Television Laboratories, Inc. 2015. Prepared For FCC Downloadable Security Technical Advisory Committee (DSTAC).

Example MVPD CAS Trust Infrastructure (2 of 10)

CableLabs®

3. The CAS vendor may license IPR to a chip vendor for use in their SoC to provide differentiated capabilities in support of the CAS system requirements. These can include, custom logic blocks that have roots of trust, key ladders, and some recovery/ countermeasure logic.
4. The CAS vendor may license IPR to a set-top box manufacturer for use in their set-top box design to integrate additional capabilities in support of the CAS system requirements that are not fully captured in the SoC.
5. The CAS vendor may contract with a third-party chip qualifier to validate the robustness against attack of SoCs provided by different chip vendors.

© Cable Television Laboratories, Inc. 2015. Prepared For FCC Downloadable Security Technical Advisory Committee (DSTAC).

Example MVPD CAS Trust Infrastructure (3 of 10)

CableLabs®

6. The CAS vendor may contract with a third-party set-top box hardware and software qualifier to validate the robustness against attack of the set-top hardware and software provided by different set-top box vendors.
7. The chip qualifier has an agreement with the chip vendor to enable the chip qualifier to validate the robustness of the SoC.
8. The set-top box hardware and software qualifier has an agreement with the set-top box manufacturer to enable the set-top box hardware and software qualifier to validate the robustness of the set-top hardware and software (operating system, drivers, middleware and applications).

© Cable Television Laboratories, Inc. 2015. Prepared For FCC Downloadable Security Technical Advisory Committee (DSTAC).

Example MVPD CAS Trust Infrastructure (4 of 10)

CableLabs®

9. The CAS vendor may exchange security data (keys and identifiers) with the secure key provisioning service. The CAS vendor and the secure key provisioning service have an obligation to keep this security data protected.
10. The secure key provisioning service will inject security data into the SoC and set-top box at the time of manufacture. Injection of security data into SOC typically occurs at SOC fabrication, which is typically than the time and place of STB manufacture. Consequently, the pairing information is usually tracked separately. This may include security data not only for the SoC and set-top box, but also for the home network, DRM, PVR and other security functions. The secure key provisioning service has the obligation to keep all the security data protected, and to deliver it to the various parties in a protected form.

© Cable Television Laboratories, Inc. 2015. Prepared For FCC Downloadable Security Technical Advisory Committee (DSTAC).

Example MVPD CAS Trust Infrastructure (5 of 10)

CableLabs®

11. The secure key provisioning service will store security data into a database that is used by the CAS provider.
12. The CAS provider extracts security data from the secure database for purposes of provisioning and management of the set-top boxes
13. The chip vendor sells appropriate SoCs to the set-top box vendor. The specific SoC version will be a variant that includes the IPR from the CAS vendor. The chip vendor has the obligation to implement a secure process to protect the security data on the chip.
14. The CAS vendor may provide a separable security element, e.g. SmartCard to the set-top box vendor.

© Cable Television Laboratories, Inc. 2015. Prepared For FCC Downloadable Security Technical Advisory Committee (DSTAC).

Example MVPD CAS Trust Infrastructure (6 of 10)

CableLabs®

15. The set-top box application provider will deliver application software developed to the specifications of the MVPD to the set-top box vendor for integration. The application implements portions of the overall service security. This software may also be delivered to the MVPD for software upgrades over the network of the software in fielded set-tops. Typically, the set-top box application provider will provide indemnification against patent infringement for their application.
16. If middleware is used in the implementation, the set-top box middleware provider will provide middleware developed to the specifications of the MVPD or application developer to the set-top box vendor for integration. This software may also be delivered to the MVPD for network upgrades of the middleware in fielded set-tops. Typically, the set-top box middleware provider will provide indemnification against patent infringement for their middleware.

© Cable Television Laboratories, Inc. 2015. Prepared For FCC Downloadable Security Technical Advisory Committee (DSTAC).

Example MVPD CAS Trust Infrastructure (7 of 10)

CableLabs®

17. The set-top box manufacturer sells set-tops to the MVPD in accordance with their contract with the MVPD. The set-top box manufacturer has an obligation to comply with the necessary robustness requirements. The MVPD typically will receive a shipping file that includes the public SoC and set-top box identifiers included in the shipment. The CAS vendor often receives similar, or the same, information.
18. When a subscriber signs up for service the MVPD executes an agreement with the subscriber specifying services provided, the subscription fee, and acceptable use policies.
19. The MVPD provides, installs, and provisions the set-top box at the subscribers' premises.
20. The MVPD contracts with a set-top application provider to develop set-top application software.

© Cable Television Laboratories, Inc. 2015. Prepared For FCC Downloadable Security Technical Advisory Committee (DSTAC).

Example MVPD CAS Trust Infrastructure (8 of 10)

CableLabs®

21. If middleware is used in the implementation, the MVPD or application developer contracts with a set-top box middleware provider to develop the set-top middleware.
22. The MVPD contracts with a metadata provider to provide metadata to be consumed by the set-top application.
23. The MVPD licenses content from multiple content providers under terms that include breach resolution, liability, warranty, as well as geographic, differentiated device, differentiated output, differentiated resolutions, and potentially other restrictions. In addition the MVPD agreement with the content providers include advertising opportunities (avails) to sell local advertising. In general, the MVPD incurs a financial responsibility for compromises that result in theft of content. Content Providers may include language regarding specific security systems and platforms in their content agreements.

© Cable Television Laboratories, Inc. 2015. Prepared For FCC Downloadable Security Technical Advisory Committee (DSTAC).

Example MVPD CAS Trust Infrastructure (9 of 10)

CableLabs®

24. The content provider licenses content metadata to multiple metadata providers.
25. The metadata provider licenses metadata to the set-top application provider.
26. In instances of system breach, one form of breach resolution is the issuance of new separable security elements, e.g. SmartCard sent either to the MVPD or to the subscriber directly. In addition to addressing system breach, separable security allows an MVPD to increase their security robustness by creating a moving target that makes it more difficult for hackers to attack the system.

© Cable Television Laboratories, Inc. 2015. Prepared For FCC Downloadable Security Technical Advisory Committee (DSTAC).

Example MVPD CAS Trust Infrastructure (10 of 10)

CableLabs®

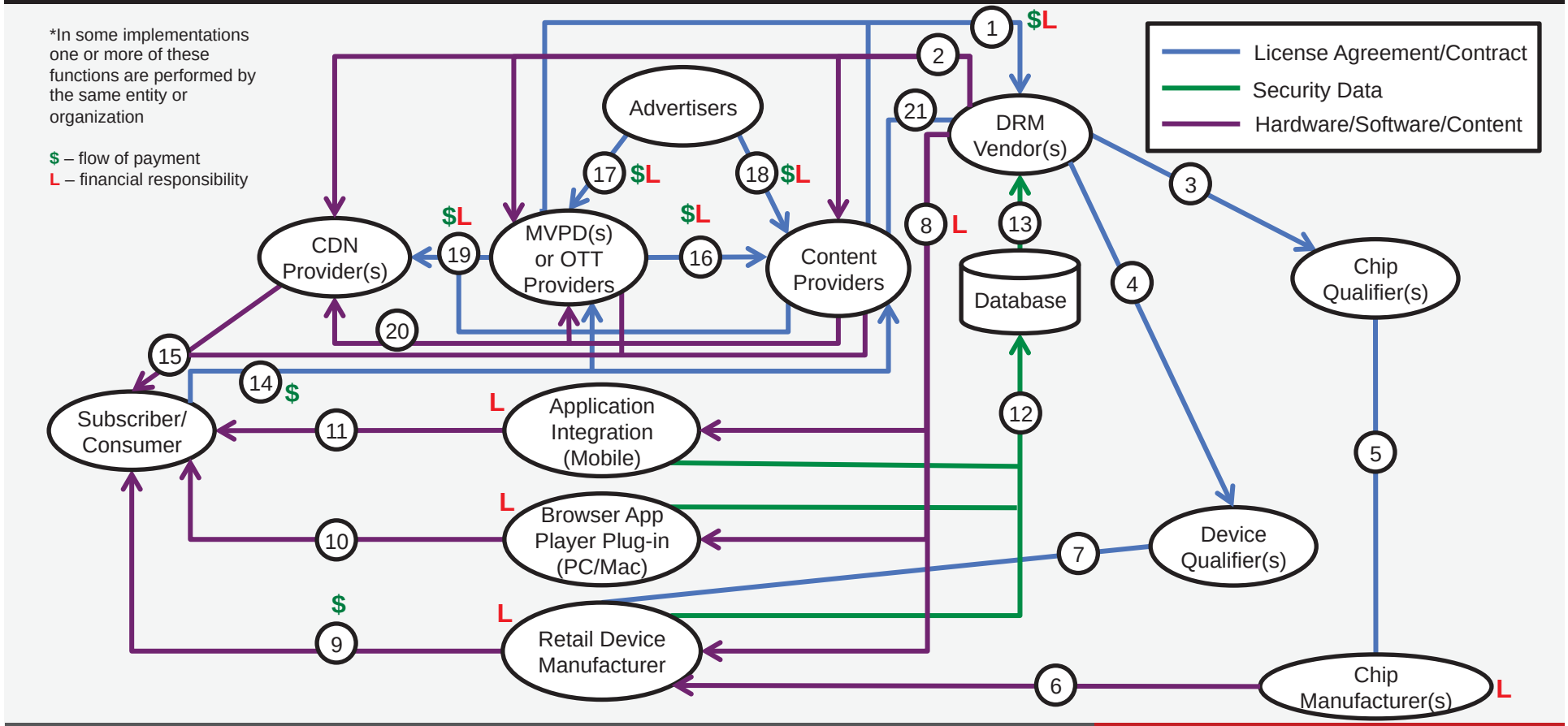
27. Advertisers contract with content providers to carry advertising specific to programming, time slot and geographic distribution.
28. Advertisers also contract with MVPDs (avails) to carry advertising specific to programming, time slot and geographic distribution. In general, the MVPD incurs a financial responsibility to insure that advertising is aired in accordance with the advertising requirements and is subject to audits to validate their performance.
29. Content providers will review CAS vendors' security solutions under NDA to understand the robustness of the implementation.

- Downloadable Conditional Access System (DCAS) architectures add another layer of trust hierarchy (an independent Trust Authority or federation of Trust Authorities above the individual CAS systems) to this diagram.

© Cable Television Laboratories, Inc. 2015. Prepared For FCC Downloadable Security Technical Advisory Committee (DSTAC).

Example DRM Trust Infrastructure*

CableLabs®



© Cable Television Laboratories, Inc. 2015. Prepared For FCC Downloadable Security Technical Advisory Committee (DSTAC).

Example DRM Trust Infrastructure (1 of 9)

CableLabs®

1. The MVPD, OTT Provider, or Content Provider contracts with one or more DRM vendors to provide a content protection solution for their network, including breach resolution, warranty, indemnification against IPR infringement, SLA, and other terms that are frequently derived from content licenses. In general, the DRM vendor incurs a financial responsibility for compromises to the DRM system that result in theft of content.
2. The DRM vendor supplies a DRM license server to the CDN Provider, MVPD, OTT Provider, or Content Provider for use in protecting the content they deliver. The license server provides the content license, which includes the rights conveyed to the subscriber and the keys necessary to decrypt the content, to the DRM client, which could be embedded in an application, a browser plug-in, or a retail device.

© Cable Television Laboratories, Inc. 2015. Prepared For FCC Downloadable Security Technical Advisory Committee (DSTAC).

Example DRM Trust Infrastructure (2 of 9)

CableLabs®

3. The DRM vendor may contract with a third-party chip qualifier to validate the robustness against attack of SoCs provided by different chip vendors.
4. The DRM vendor may contract with a third-party device qualifier to validate the robustness against attack of devices provided by different retail device manufacturers.
5. The chip qualifier has an agreement with the chip vendor to enable the chip qualifier to validate the robustness of the SoC.
6. The chip vendor sells appropriate SoCs to the retail device manufacturer. The chip vendor has the obligation to implement a secure process to protect the security data on the chip.

© Cable Television Laboratories, Inc. 2015. Prepared For FCC Downloadable Security Technical Advisory Committee (DSTAC).

Example DRM Trust Infrastructure (3 of 9)

CableLabs®

7. The device qualifier has an agreement with the retail device manufacturer to enable the device qualifier to validate the robustness of the retail device.
8. The DRM vendor supplies a DRM client together with robustness and compliance requirements to application developers to integrate the DRM into their application, browser app player plug-in developers to integrate into the player plug-in, and retail device manufacturers to integrate into their retail device. Because the DRM vendor does not typically perform the integration of the DRM, the DRM vendor may have a smaller liability and the other parties a greater liability under breach.

© Cable Television Laboratories, Inc. 2015. Prepared For FCC Downloadable Security Technical Advisory Committee (DSTAC).

Example DRM Trust Infrastructure (4 of 9)

CableLabs®

9. The consumer purchases a retail device for their personal use and installs and/or provisions the device. The retail device manufacturer assumes some liability in meeting the DRM vendor's compliance and robustness rules. The MVPD or OTT provider's app for the device implements portions of the overall service security.
10. The consumer may download a browser DRM plug-in for their browser or download a browser with a pre-installed DRM or CDM in order to view protected content on the Internet. The browser and web application implement portions of the overall service security. The provider of the browser DRM capability assumes some liability in meeting the DRM vendor's compliance and robustness rules.

© Cable Television Laboratories, Inc. 2015. Prepared For FCC Downloadable Security Technical Advisory Committee (DSTAC).

Example DRM Trust Infrastructure (5 of 9)

CableLabs®

11. The consumer may download a mobile app onto their tablet or smart phone in order to view protected content via their mobile device. The DRM is sometimes included in the downloaded app and sometimes in the consumer device. The mobile app implements portions of the overall service security. The provider of the mobile app or the mobile device manufacturer assumes some liability in meeting the DRM vendor's compliance and robustness rules.
12. The DRM client implementations report security data to the DRM database personalizing the specific instance of the DRM client to the specific device on which it is installed. This assures that the DRM client has a unique identity based upon the device on which it will execute.

© Cable Television Laboratories, Inc. 2015. Prepared For FCC Downloadable Security Technical Advisory Committee (DSTAC).

Example DRM Trust Infrastructure (6 of 9)

CableLabs®

13. The DRM vendor extracts security data from the secure database for purposes of provisioning and management of the DRM clients.
14. The consumer/subscriber purchases content from the CDN Provider, MVPD, OTT Provider, or Content Provider, either on a subscription or transactional basis.
15. The CDN Provider, MVPD, OTT Provider, or Content Provider delivers the appropriate content and DRM license to enable the consumer/subscriber to view the content they purchased. The DRM license will convey the specific rights the consumer/subscriber has purchased.

© Cable Television Laboratories, Inc. 2015. Prepared For FCC Downloadable Security Technical Advisory Committee (DSTAC).

Example DRM Trust Infrastructure (7 of 9)

CableLabs®

16. The MVPD, or OTT Provider licenses content from multiple content providers under terms that include breach resolution, liability, warranty, as well as geographic, differentiated device, differentiated output, differentiated resolutions, and potentially other restrictions. In general, the video distributor incurs a financial liability for compromises that result in theft of content. In some instances the Content Provider itself may license content from other sources. In other instances, the Content Provider, the MVPD or the OTT Provider may develop the content exclusively for his or her own distribution. Content Providers may include language regarding specific security systems and platforms in their content agreements.

© Cable Television Laboratories, Inc. 2015. Prepared For FCC Downloadable Security Technical Advisory Committee (DSTAC).

Example DRM Trust Infrastructure (8 of 9)

CableLabs®

17. Advertisers contract with MVPD or OTT Provider to carry advertising specific to programming, consumer profile and geographic distribution. In general, the MVPD or OTT Provider incurs a financial responsibility to insure that advertising is aired in accordance with the advertising requirements and is subject to audits to validate their performance.
18. Advertisers also may contract with Content Providers directly to carry advertising specific to programming, consumer profile and geographic distribution. In general, the Content Provider incurs a financial responsibility to insure that advertising is aired in accordance with the advertising requirements and is subject to audits to validate their performance.

© Cable Television Laboratories, Inc. 2015. Prepared For FCC Downloadable Security Technical Advisory Committee (DSTAC).

Example DRM Trust Infrastructure (9 of 9)

CableLabs®

19. MVPDs, OTT Providers, or Content Providers may contract with CDN Providers for content distribution and optionally DRM management services. If DRM management services are required, the CDN Provider will incur liability for maintaining the security of the content.
20. If they have contracted for CDN services, MVPDs, OTT Providers, or Content Providers provide content to the CDN provider for distribution and optionally DRM management services.
21. Content providers will review DRM vendors' security solutions under NDA to understand the robustness of the implementation.

- Not shown in this diagram are 3rd-party piracy-monitoring services that may be retained by DRM vendors, MVPDs, or content providers to detect instances of pirated content to activate their own breach detection and response activities, or into joint action in some cases.

© Cable Television Laboratories, Inc. 2015. Prepared For FCC Downloadable Security Technical Advisory Committee (DSTAC).

Risks of a Single, Uniform Security Solution

CableLabs®

- There is an intrinsic risk in selecting a single, uniform security solution for all MVPDs
- "Security through diversity" is an important principle in the design of security systems
- Microsoft's Windows and Internet Explorer have been primary targets of attack due to their dominance in the market
- Monocultures are recognized as being particularly susceptible to attack and disease
  - Y. Zhang, et. al., "Heterogeneous Networking: A New Survivability Paradigm", 2001
  - D. Geer, et. al., "Cyberinsecurity: The Cost of Monopoly", 2003
  - A. Stamp, "Risks of Monoculture", 2004
- The more CA and DRM systems can differentiate, the more a competitive market of CA and DRM products thrives, providing technology innovation and continual improvement.

© Cable Television Laboratories, Inc. 2015. Prepared For FCC Downloadable Security Technical Advisory Committee (DSTAC).