

DSTAC WG3 Report

I. Introduction

A. DSTAC Mission

The DSTAC's mission is "to identify, report, and recommend performance objectives, technical capabilities, and technical standards of a not unduly burdensome, uniform, and technology- and platform-neutral software-based downloadable security system" to promote the competitive availability of navigation devices (e.g., set-top boxes and television sets) in furtherance of Section 629 of the Communications Act. The DSTAC must file a report with the Commission by September 4, 2015 to detail findings and recommendations. [DSTAC Mission, www.fcc.gov/dstac]

B. DSTAC Scope

See *Scope of the DSTAC Report*, FCC, April 27, 2015 [DSTAC Scope, <https://transition.fcc.gov/dstac/fcc-staff-guidance-04272015.docx>]

C. Working Group 3 Description

The working group will identify performance objectives, technical capabilities, and technical standards that relate to the security elements of the downloadable security system. The working group will also identify minimum requirements needed to support the security elements of the downloadable security system. [*WG 3 & 4 Descriptions*, FCC, [April 27, 2015](#)]

D. Working Group 3 Product

The working group will deliver a written functional description its performance objectives, technical capabilities, and technical standards, and minimum requirements to the full DSTAC. It will present an outline of its work at the May 13, 2015 meeting, a first draft of its report at the July 7, 2015 meeting, and a final report for full DSTAC discussion and consideration at the August 4, 2015 meeting. [*WG 3 & 4 Descriptions*, FCC, [April 27, 2015](#)]

II. Downloadable Security System - Common Framework

A. Downloadable Security System – Common Definitions

In order to meet its goal of creating a functional description of performance objectives, technical capabilities, technical standards, and minimum requirements of a Downloadable Security System (DSS), WG3 worked to define common or alternate definitions of what a downloadable security system is, what functions it performs and what components it is comprised of. This effort aims to fulfill the DSTAC Mission of identifying “a not unduly burdensome, uniform, and technology- and platform-neutral software-based downloadable security system”.

Objectives, capabilities, standards and requirements are measured against this set of definitions in subsequent sections of this report.

Definition of a Downloadable Security System:

Downloadable Security System (DSS) is a software based security system selected or supported by the media provider that is capable of being transferred from a download server and installed onto a navigation device to securely receive the services offered by the media provider. The DSS download server may be operated by the media provider, the device maker or a DSS vendor. A DSS may be downloaded as part of a client application or downloaded as part of the client OS or downloaded as part of the client TEE or pre-installed on the navigation device at manufacture time. (Note: As in the latter case, while the DSS is always *downloadable* it may not always be *downloaded*.)

The DSS performs the required **functions** necessary to protect the media provider’s service from a variety of attacks. A DSS relies on a number of common **components** within the navigation device. These common components may preferably support one or more DSS’s from multiple media providers and one or more DSS vendors. A DSS may rely on a hardware root of trust capable of multiple hardware implementations.

“Modern computing devices consist of various hardware, firmware, and software components at multiple layers of abstraction. Many security and protection mechanisms are currently rooted in software that, along with all underlying components, must be trustworthy. A vulnerability in any of those components could compromise the trustworthiness of the security mechanisms that rely upon those components. Stronger security assurances may be possible by grounding security mechanisms in roots of trust. Roots of trust are highly reliable hardware, firmware, and software components that perform specific, critical security functions. Because roots of trust are inherently trusted, they must be secure by design. As such, many roots of trust are implemented in hardware so that malware cannot tamper with the functions they provide. Roots of trust provide a firm foundation from which to build security and trust.”¹

¹ <http://csrc.nist.gov/projects/root-trust/>

In the context of Downloadable Security, it is envisioned that **Hardware Roots of Trust** will be utilized for functions such as: the primary point of storage of consumption device secure identities, device key lists, key lists used for dissemination of information to intermediary security infrastructure, and revocation lists.

A common requirement within the hardware root of trust is a mechanism that allows the hardware to be uniquely identified explicitly or implicitly, giving each manufactured silicon chip its own “personality” (or unique number). Since no two chips are alike, the embedded secret key provides unique strength in how that device can be addressed by a secure ecosystem.

Additionally, it is important to understand the concept of service and user Authentication and Entitlement. Unless explicitly indicated, these terms represent concepts and functions, but not actual instantiations. For example Entitlements refers to the range of service states available from a pay service and not to specific implementations of license and entitlement distribution, such as entitlement management messages (EMMs). The functions may be part of a conditional access system, a DRM system, or another system that is part of the MVPD network.

Authentication – confirming a device or user is a subscriber of the MVPD service and authorized for service, and is typically encrypted. Examples of the authentication process could include the user entering a username and password, geo-location of the IP address, hardware device id, or the device presenting a certificate that is validated by a MVPD network component. Re-authentication may occur at different time intervals depending on authentication type.

Entitlements – refers to the control plane metadata indicating what services are available to the authenticated device and/or user, and is typically encrypted. For example a user may be entitled to a certain set of linear broadcast video channels, a pay per view (PPV) event, or a subscription VOD service. These may be functions of subscription level, time, device type and location. Entitlements are expected to change with time. The method by which entitlements are expressed and communicated have typically been an area where security solution providers (CAS or DRM) have differentiated their products in a competitive market.

Usage Rights – an authenticated device and/or user that is entitled to a service may have certain usage rights associated with the content they receive from the service. For example Copy Control Information (CCI) indicates if copies of the content can be made, plus any restrictions on those copies such as how many copies can be made. Usage Rights are usually expressed using a Right Expression Language (REL) which “is a machine-processable language used to express copyright or similar status of data.”² Specific Usage Rights may be functions of subscription level, time, device type and location.

² https://en.wikipedia.org/wiki/Rights_Expression_Language

These concepts can also be seen as a process performed by the DSS or other component of the MVPD's network. Devices and their user interfaces utilize these processes to enable the user to access content services.

Further detail on how these processes are currently implemented in the MVPD network can be found in Section VIII.

B. Downloadable Security System – Common Requirements

1. DSS Functions, Core Components, Technical Capabilities, and Supported Services

a) *Functions of a Downloadable Security System*

Some of the main functions that a DSS performs:

- 1) Verifies the navigation device reports having the necessary components for receiving the media provider's service, and it identifies if the device has been tampered with or compromised.³
- 2) Verifies the integrity of the software components that are downloaded and installed in the navigation device to ensure that those components have not been compromised at download, installation, boot, or runtime. This is typically done by code signature verification.
- 3) Authenticates or supports the authentication of the user of the device as being authorized for receiving the media provider's service. This may be implicit when using a managed device assigned to a user.
- 4) Provides to the navigation device secure and verifiable information on the authorized services available to the device and user.
- 5) Enables descrambling of the authorized services available to the device.
- 6) Performs a secure download from the network to a client device, for either first time installation of content security software, or a software update.
- 7) In the network, encrypts content for later consumption, either on a real time or pre-encrypted basis, packetized in accordance with the target delivery system.
- 8) In the network, encrypts software to be downloaded, either on a per client device basis, or based on a parameter or set of parameters that enables a group of devices to be targeted for download as an ensemble.
- 9) In the network, distributes entitlement information in various forms, using either one way or two way protocols, depending on the delivery network type.

³ A DSS itself cannot independently verify that a device has met or supports all required robustness rules, hardware requirements or compliance requirements. These are typically done in a design audit, self-verification or other process (such as a legal agreement) to a set of Compliance Rules. The DSS and associated security servers verify, via a certificate or other highly secure mechanism, that a device reports such compliance. In typical implementations, any failure in this type of validation will deactivate the DSS and its associated device. In order to achieve this level of security, a DSS must be considered as part of a broadly defined security infrastructure which includes key management, secure manufacturing, audit, testing, standards development, etc. The level of the robustness and compliance will impact the content available, determined by the content licenses between content owner and distributor.

- 10) The DSS fulfills the commercial and/or regulatory obligations of an MVPD to protect content from content sources/owners. As an example, the Encoding Rules for CableCARD limited scope of MVPD obligations when applied to retail devices.

Optional Functions that may be required to enable a 3rd party User Interface to display and manage some or all of the media provider service:

- 1) Method to provide a 3rd party User Interface application knowledge of:
 - a) Device Authorization status
 - b) Media provider's Service Authorization status
 - c) License rights for media provider content

b) *Components of a Downloadable Security System*

The definition and functions of a DSS imply a set of core components that a DSS must contain. The components include:

- 1) One or more software components that are provided by the MVPD/OVD and downloadable to devices
- 2) Common methods for a navigation device to securely discover and obtain the software components from a media provider.
- 3) A method of determining the robustness of the platform and execution environment that runs the software components.
- 4) A set of device requirements to provide a hardware and software execution environment such as a hardware root of trust, software libraries and trusted operating environment that meet the required robustness and compliance requirements.
- 5) A system for replacing or upgrading the software components.
- 6) A system for validating and/ or revoking the validation of the software components.
- 7) Network elements to support secure code download, content encryption, and entitlement distribution functions.

Optional Components that may be required to enable a 3rd party User Interface to display and manage some or all of the media provider service:

- 1) Method to provide a 3rd party User Interface application the ability to:
 - a) Request a list of video services available to the device and user
 - b) Request a video service to be decrypted
 - c) Request license rights for media provider content
 - i. Make local recordings of content if permitted by the license rights

c) Technical capabilities of a Downloadable Security System

- 1) Makes use of a hardware root of trust, or other framework, if available, that can be utilized to support secure code download of the DSS software.
- 2) Can decrypt standard encryption algorithms including DES, CSA, AES with suitable performance for the target device.
- 3) Optionally provide support for software downloadable non-standard encryption schemes equal in computational complexity to AES, to support download of system-specific countermeasures.
- 4) Can decrypt content packetized in a variety of formats, including MPEG transport streams, HLS, MPEG-DASH.
- 5) Supports software implementation, or access to hardware implementation, of standard cryptographic functions such as decryption ciphers, check-sums, hashes, and other one-way functions.
- 6) Protects and delivers content protection key(s) to the navigation device in a way that meets the conformance and robustness rules of the whole DSS system.

d) Services provided to the rest of the Navigation Device

- 1) Decrypts content, and may copy protect content or validate copy protection for delivery to either a player app or hardware decoder.
- 2) Interprets copy control information provided by the DSS management system and securely applies relevant copy control to digital outputs.
- 3) Supports some secure mechanisms such as secure boot, secure download, decryption, and signature verification services.
- 4) Optionally authenticates credentials presented by the navigation device with respect to relevant license regimes.
- 5) Provides authorization status with respect to a specified class of content to client-resident applications.
- 6) Optionally supports session-based security services to other applications in the client device.

2. System Requirements

a) *System components (an application environment, a communication path, a secure execution environment, secure hardware elements, trust model, etc.)*

A DSS must support the ability to download sufficient code and data to renew the security system – to download different keys, certificates, code, configuration parameters, etc., such that the renewed system is secure.

A DSS must have hardware resources to (1) uniquely identify the hardware, (2) store cryptographic keys securely, (3) enable secure updating of the securely-stored cryptographic keys, and (4) support a segregated execution environment for security operations (either by a separate CPU or by strong hardware segregation features, or equivalent).

Security without trust is impossible. We suggest that a DSS should (1) try to minimize the amount of trust placed in personnel, facilities and operations and (2) explicitly state what level of trust is required for the downloadable system to operate securely. Beyond these requirements, specification of a trusted registrar for keys may be necessary in some architectures.

b) Interfaces between system components

A CAS or DRM system is typically split into two main subsystems, (1) a “server” in the head-end or cloud that originates the viewing rights or licenses, and (2) a “client” subsystem located in the viewing device that securely applies the rights or license to descrambler to decrypt the content.

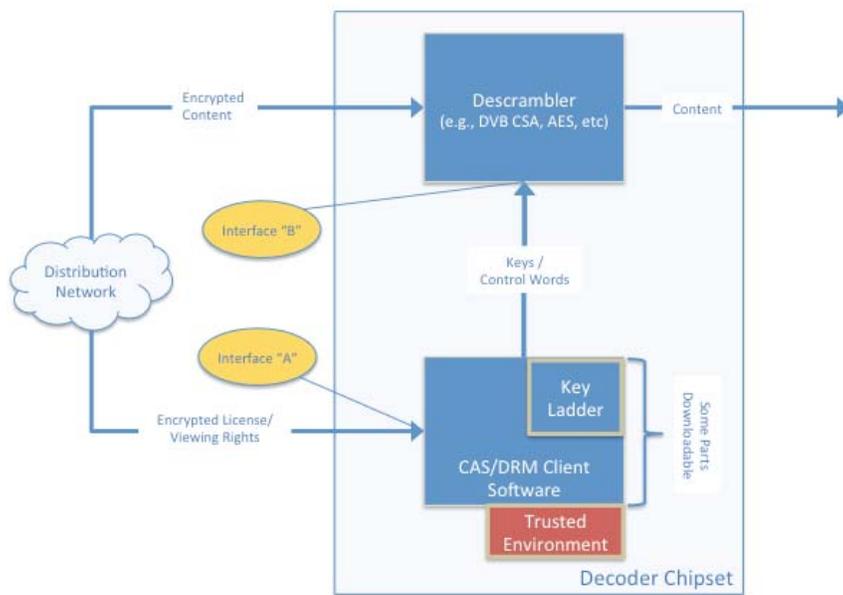


Figure 1 – Typical Communication Path Interfaces for Security Sub-system

The server head-end or cloud components also interface with subscriber management and in turn billing systems. These interfaces are outside the scope of this document.

The server system communicates viewing rights to the client in a one way broadcast CAS system through broadcast messages. If the system can be relied upon to be two-way, the rights can much more efficiently be requested via an IP call using traditional IP techniques. (Interface A in the graphic above)

For a DRM system, an IP channel is used by the client to request the viewing rights.

Within the client device, the rights are securely decrypted and a content or working key is securely connected to the content descrambler which forms part of the secure video path. (Interface B in the graphic above)

c) Compliance Rules

Devices implementing the downloadable security system need to be required to follow compliance rules. Generally, compliance rules describe things that the platform is required to do, and things that the platform is required not to do. For example, some of the compliance rules necessary may include:

- No Circumvention – A device shall not directly or indirectly provide access to content except as permitted in the compliance rules.
- Outputs – A device shall not emit the digital plaintext of encrypted audiovisual content on any interface that is not protected by a content protection system (such as DTCP-IP, HDCP, etc.). A device shall not emit unprotected audiovisual content on any output at a resolution higher than “standard definition” (720x480x60i or less).
- Watermark – A device shall not knowingly or intentionally disrupt, remove or interfere with a watermark that is widely used to enforce or track copy controls or copy control circumvention.

However, compliance rules are typically applied to a *product* – including both the hardware platform, and the firmware and software that runs on it. Compliance rules will need to be developed that are applied to the hardware platform; separately, compliance rules will need to be developed that are applied to the firmware and software.

d) Robustness Rules

Devices implementing the downloadable security system need to be required to have a certain level of robustness to attack. Generally, robustness rules describe how the hardware must be constructed so as to provide a certain level of resistance to attack.

Robustness rules have typically been an area where security solution providers (CAS or DRM) have differentiated their products in a competitive market. In general, content owners will refuse to license content to less robust solutions and MVPDs or OVDs will refuse to make use of them.

For a system to be secure it needs to preserve and maintain three basic properties: (1) confidentiality – secret data and secret operations are kept secure from unauthorized parties, (2) integrity – secret data and secret operations are kept secure from modification by unauthorized parties, and (3) availability – unauthorized parties are kept from disrupting or limiting access to the secured system. Whatever components (hardware, software) are used to build a downloadable system should ensure that these properties are not violated.

For example, some of the robustness rules necessary may include:

- Preservation of Secret Data – Devices shall be designed and manufactured such that they resist attempts to discover, reveal and/or

use without authority any secret keys (including without limitation content keys, entitlements, or other authentication and decryption keys). Some attacks that chip designers should resist include: invasive imaging using powerful state-of-the-art microscopes, access to the keys using unsecured JTAG ports, attacks that use side-channel information such as power consumption, electromagnetic emissions, temperature difference, acoustic outputs, optical side-channel information or digital side-channels through on- and off-chip microarchitectural structures.

- Secure Content Path – Devices shall be designed and manufactured such that unencrypted digital audiovisual data is never transmitted or observable using standard board-level hardware debugging tools such as logic analyzers, JTAG debuggers.
- Unique Identification – The device and system shall be designed, implemented and manufactured to prevent an adversary from emulating the hardware platform in software to violate the security properties of the system. The device shall be required to provide an unforgeable proof to the software about the authenticity of the device.
- Software Attestation – The downloadable system shall be designed and implemented to provide an unforgeable proof of the authenticity of the software portion of the downloadable system. Specifically the adversary should not be able to modify the computer instructions of the downloadable system before or during the operation of the downloadable system. For maximum security, the attestation must be provided during the life-time of the software but one time attestation, i.e., when the system is rebooted each time, is acceptable if the device fulfills the non-interference robustness requirement.
- Non-Interference – The downloadable system shall be designed, implemented and manufactured to ensure that the execution of trusted components shall be not be influenced by the execution or presence of untrusted components executing on the system for the entire life-time of the downloadable software.
- Preservation of secret operations – The downloadable system shall be designed, implemented and manufactured to ensure to operations based on secret data cannot be subverted by the adversary to produce incorrect results. Further such subversion should be reported in an unforgeable manner to the provider.
- Forward Revisioning – The downloadable system shall be designed, implemented and manufactured such that the system can never be rolled back to an older version of the system than what exists in the system as identified by an unforgeable revision number associated with a system.

e) *(if you do assume IP connectivity) DBS STB must act like DCAS server device – robustness, capabilities, etc.*

Unique system requirements for a one-way environment (ie. DBS).

DBS services are inherently one way in nature, but must interface over 2-way IP networks to other devices in the home. It is unclear whether anchoring a DSS system on an adjunct and unmanaged IP connection is in harmony with the overall mission of designing a "uniform" and "platform-neutral" system. Because DBS devices have no a priori knowledge about reliability, bandwidth, cost, or other factors in any broadband-like connection they find, DBS CPE does not rely on this path for enabling two-way communications as part of the conditional access system. Existing DBS security and business practices assume that IP connectivity is intermittent or non-existent, and function effectively absent such communications. Broadband-like IP connectivity can be used to enhance the available content for a particular subscriber, but the basic system must function without IP connectivity.

Specifications would need to be developed to address how this intermittent, unreliable communications path would function in a standard way. Would there be one box with IP connectivity that would proxy for other boxes in the home? Would each box have its own IP connection through a customer-provided gateway? How would IP connectivity be established and maintained in a secure or reliable manner? These would be important factors that would need to be decided upon for the design of such a DBS gateway.

f) Countermeasures must be supported

Once a security compromise has been detected (through inline monitoring mechanisms or out-of-band mechanisms) it shall be possible for the security system to be refreshed the systems in the field to protect against future compromises.

For some compromises (e.g., key extraction using hardware reverse engineering, or deep probing into the hardware, or through other hardware means) the cure for the breach requires changing the hardware itself, and may not be cured without hardware change. For other compromises (including, but not limited to, software compromises or software vulnerability), cure may be effected by downloading different software.

g) Device and system testing by multiple parties must be supported

In the same way that stronger robustness and compliance rules provide greater levels of assurance that content licenses will be enforced, stronger and more thorough testing regimes provide greater levels of confidence that the functionality and, indirectly, robustness is compliant as well. The traditional MVPD CAS trust ecosystem, for example, implements a more thorough level of testing. Multiple parties are involved in this testing and validation regime. The SoC and set-top are validated from the robustness and compliance perspective in addition to functional testing to insure the MVPD service is appropriately supported.

The security system must support multiple testing parties. The device and system testing process should be designed in a way that a particular tested component (e.g., a retail navigation device) can be tested by any one of a set of testing entities, without any compromise in security or functionality.

For devices that attach directly to the MVPD network, the retail device would have to be designed to meet the required testing for each MVPD, focused on protecting the integrity of the MVPD physical network. Recognizing that testing against each and every MVPD would be a significant task, a solution would be needed to consolidate the test requirements to reduce the effort.

An example of how device and system testing processes work today is described in Section [QVHH](#).

h) Registrar for keys

A single entity, or a federated registrar consisting of multiple entities with secure exchange of credentials, should span all MVPDs and manage keys. Care has to be taken in the governance of this body or bodies with perhaps a board consisting of a wide cross section of stakeholders. The complexities and challenges of systems like this are outlined in the Working Group #2 Report, Section XII: Summary of MVPD CAS and DRM Trust Infrastructures [<https://transition.fcc.gov/dstac/wg2-report-01-04212015.docx>].

i) Devices need to support multiple MVPD simultaneous subscriptions

As a general rule most subscribers only subscribe to one MVPD at a time. However, there are instances where a subscriber may subscribe to multiple MVPDs simultaneously. The downloadable security system must not prevent a single device from supporting simultaneous subscriptions to more than one MVPD.

This use case could be handled in the following ways for the models referenced above:

- MVPD TV Apps – This solution enables multiple concurrent MVPD subscriptions. Each MVPD provides its own App, and the subscriber chooses which App to use at any point in time.
- HTML5 Web Apps – This solution enables multiple concurrent MVPD subscriptions. Each MVPD provides its own website and Web App, and the subscriber chooses which web site to visit at any point in time.
- VidiPath/RVU – The subscriber would have to have at least one VidiPath or RVU server from each MVPD and all of his devices connected to the home network. In this case the subscriber chooses which VidiPath or RVU server he wishes to use at any given point in time.
- Two Contexts – This solution would enable a device to have two (or more) distinct DSS instances, one per each MVPD.

For devices that attach directly to the MVPD network, the retail device would have to be designed to connect to multiple MVPD networks concurrently.

j) Devices need to support portability across MVPD subscription services

Retail navigation devices must be portable to other networks (e.g., when a consumer changes MVPD or moves into another cable operator's footprint). To support this, the downloadable security solution must support normal network registration, device authentication, device provisioning, secure download of the security software, and secure provisioning of service entitlements, as well as transitions from one MVPD network to another. The transition from one MVPD to another may involve an overlap of service (both services active) or a gap in service (neither service is active) and may involve a disruption of power to the device or may not, depending on the specific transition scenario. The activation of the new MVPD service may or may not involve an installation visit by an installer from the new MVPD. Regardless, a confirmation that the subscriber is receiving the desired service from the new MVPD is required. A retail device must support all of these transition scenarios.

3. Performance Objectives

The WG2 report captures several high level requirements regarding Scalability, Latency, and Addressability (see e.g. S13, S14, S15). A commercially viable DSS solution will need to fully address a broad set of performance objectives. Additionally, it is recognized that there are unique requirements for operating in one-way and two-way distribution architectures.

4. Technical Standards

See Annex C for relevant Standards references.

5. Representative devices to be considered

- Standard/High Definition/Ultra High Definition STB
- High Definition and 4K Ultra HD TV – for IP and other delivery paths
- RVU certified TV
- VidiPath certified TV
- Home Media Server
- Home Video Gateway from MVPD, Residential Gateways (RG)
- Digital Transport Adapter (DTA)
- Simple Digital Video Recorder
- Whole Home DVR Ecosystem
- Media Player Box from Retail (e.g. Roku, Apple TV, Amazon, WD)
- Media Player Sticks (e.g. USB, HDMI)
- Connected Tablet with Data Plan
- Connected Tablet with Wi-Fi
- Connected Smart Phone with Data Plan
- Connected Smart Phone with Wi-Fi
- Broadband Connected Blu-Ray Players
- Notebook or Laptop Computer (e.g. Apple, Windows, Linux)
- All-in-One or Desktop Computer (e.g. Apple, Windows, Linux)
- Gaming Consoles (e.g. PS4, Xbox)
- Connected AV Receivers
- Internal/External Tuners (e.g. Hauppauge, Silicon Dust, Sat-IP)

C. Existing Downloadable Security System Solutions

DSTAC Working Group 3 conducted a review of 16 existing security system solutions and components including both hardware (SoC) and software. The review included both a presentation of the technology to DSTAC members and, where relevant, a detailed response to survey of questions developed by Working Group 3 regarding the technical details of the respective security system solutions. The 16 security solutions and technologies reviewed were:

- Broadcom SoC
- PolyCipher
- W3C HTML5 Encrypted Media Extensions (EME)
- Open Media Security (OMS)
- Cisco VideoGuard
- Digital Transport Adaptor (DTA) Security
- Adobe Primetime
- Verimatrix VCAS
- Arris SecureMedia
- Nagra anyCast Connect
- RVU Alliance
- DLNA VidiPath
- Alticast XCAS
- MStar SoC
- Intel SGX Technology SoC
- Microsoft PlayReady

The presentations of the solutions reviewed are included in Appendix A, the survey questions developed by Working Group 3 in Appendix B, and the survey responses received in Appendix C.

A table summarizing all of the responses can be found in [Error! Reference source not found. Table 1](#) of Annex D. The following section provides a shorter summary of this information.

1. Description of existing solutions

The downloadable security solutions that were reviewed ranged from the hardware technologies employed in current or next generation SoCs, to CAS and DRM solutions, to standards based solutions. The SoC vendors reviewed were: Broadcom, MStar, and Intel. The CAS and DRM solutions reviewed were: PolyCipher, OMS,

VideoGuard, DTA Security, Adobe Primetime, VCAS, SecureMedia, anyCast Connect, XCAS, and PlayReady. The standards based solutions reviewed were: HTML5 EME, RVU Alliance, and VidiPath.

There are several key observations that can be drawn from this review:

- Many of the solutions presented noted that CAS and DRM solutions are beginning to converge, blurring the line between the two. Several solutions presented an integrated CAS and DRM solution.
 - Most of the solutions reviewed identified a hardware root of trust, secure boot, secure software download, and a trusted execution environment as important elements of a downloadable solution.
 - The market supports and encourages a diversity of solutions that compete, driving innovation and cost reduction. All of the SoC, CAS, and DRM vendors have developed successful businesses providing security solutions to the market. SoC vendors have integrated security features into their chips to reduce costs, meet content providers' requirements, and compete in the market for hardware components. CAS and DRM vendors introduce new features into their systems to address evolving business models and content license requirements in the content distribution market. Standards are developed to provide scale for these systems, whether over the Internet or within home networks.
 - A diversity of trust infrastructures including different robustness and compliance rules has developed to address different market opportunities. One presentation explicitly stated, "Permissions and security expectations vary widely and no one size fits all."
 - Some of the solutions indicated support for both 1-way and 2-way networks, other solutions indicated that they were designed for 2-way networks only.
 - There were strong recommendations to avoid rigid and/or single implementations (one-size-fits-all) that significantly limits innovation, competition, or increases security risk.
 - Standards are carefully developed to allow for different, even proprietary, implementations to meet the requirements enabling differentiation among the implementations.
2. Existing applicable or related specifications
- UPnP and DLNA Guidelines
 - W3C HTML5 Specification, *A vocabulary and associated APIs for HTML and XHTML*. <http://dev.w3.org/html5/spec/>
 - W3C WOFF File Format 1.0. <http://www.w3.org/TR/WOFF/>

- W3C MSE, *Media Source Extensions*. <http://www.w3.org/TR/media-source/>
- W3C EME, *Encrypted Media Extensions*. <http://www.w3.org/TR/encrypted-media/>
- W3C Crypto, *Web Cryptography API*. <http://www.w3.org/TR/WebCryptoAPI/>
- RVU Alliance Specifications

III. Download Security System Threat Models

A Threat Model describes the level of tools available to the attacker, combined with a description of the amount of power or influence that the attacker has on the content delivery network.

Some examples of “level of tools” are:

- **Widely Available Tools** means tools or equipment that are widely available at a reasonable price, including items such as screwdrivers, jumpers, chip clips, file editors, and soldering irons.
- **Semi-Professional Tools** means specialized electronic tools that are widely available at higher prices than Widely Available Tools, but still affordable by a broad spectrum of the population. Within this category are tools such as memory readers and writers, debuggers, decompilers, or similar software development products.
- **Professional Software Tools** means professional tools, such as the software equivalent of in-circuit emulators, disassemblers, loaders, or patchers, implemented in software, that require professional skill and training to utilize.
- **Professional Hardware Tools** means tools or equipment, such as logic analyzers, chip disassembly systems, or in-circuit emulators, implemented in hardware, that require professional skill and training to utilize.
- **Highly Sophisticated Tools** means tools or equipment such as scanning electron microscopes, black box programming equipment and other equipment that might be available to an inside attacker, that require very specialized professional skill and training to utilize.

Some examples of “amount of power” are:

- **Level 0** – This least-powerful attacker has no control over any computer in the content delivery network.
- **Level 1** – This class of attacker has knowledge of the network infrastructure and can observe and manipulate everything in the network environment of the consumer
- **Level 2** – This class of attacker has knowledge of the network infrastructure, can observe and manipulate everything in the network environment of the consumer, and also has resources and ability to fake services, falsify authorization levels, manipulate service provider databases, and disable encryption systems as example capabilities. This would equate to a sophisticated inside attacker.

The threat model considered is described below.

A. Level of attacker capability

The attacker is a well-organized, well-funded organized crime syndicate, with significant technical, monetary and personnel available to devote to attacking the security system. Such an attacker can be expected to have access to Highly Sophisticated Tools with the skill and expertise to use them, and Level 1 access to the content delivery network.

B. Describe robustness from attackers

It is desirable for the DSS (at the highest level of capability) to be able to withstand and repel an attack assuming a combination of Level 1 access to the network, along with access to both Professional Hardware Tools, and Professional Software tools.

C. Threats not in scope

Bribery and corruption are outside the scope of threats to be considered.

We are assuming that threats corresponding to rogue network operator employees who grant service authorizations using the official systems, then proceed to hide their tracks via actions such as deletion or editing of transaction logs, are not within the scope of DSS to deal with. Similarly, attackers with Level 2 access to the system, along with Highly Sophisticated Tools, are also considered to be out-of-scope.

D. Diversity

It is anticipated that various levels of DSS capability will continue to be implemented on different device classes, as is the case today. Some implementations will not be sufficiently robust to withstand the highest level of attack identified above. We assume that in such cases, the type of content enabled on the weaker platforms will be limited to exclude content whose value is deemed to warrant the higher level of protection.

An additional level of diversification will occur through commercial competition in a future DCAS market. The output of the DSTAC group, and/or any subsequent groups may result in a broad definition or set of definitions, or a recommendation in DSS implementation specifications. However many areas that relate to security will still be open for innovation and hence differentiation. Thus by its very nature, competitive implementations will offer a degree of diversification.

Finally, deliberate diversification is a well-known technique used in obfuscated software components of a security system. Here the software is compiled or assembled in a way that makes reverse engineering very difficult AND it is done in such a way that there are multiple versions of the same or similar products deployed simultaneously. In this way a commercial hacker has a much larger challenge in deploying hacks to a wide enough population to make his criminal enterprise sustainable.

IV. Download Security Systems

The DSTAC WG3 has prepared two proposals for implementing a software-based downloadable security system. Proposal 1: HTML5 Security API's, was authored by Mark Vickers, Comcast and Proposal 2: Virtual Headend System was authored by Adam Goldberg, representing Public Knowledge. There are a number of commonalities between the two proposals that are important to highlight:

- Both proposals acknowledge the diversity of technologies across MVPDs and even within MVPDs of a similar type,⁴
- Neither proposal recommends a solution based on common reliance,⁵
- Both proposals acknowledge that it is unreasonable to expect that retail devices connect directly to the various MVPDs' access networks and rather connect via an IP connection with specified APIs/protocols,⁶
- Both proposals acknowledge that it is unreasonable to expect that MVPDs will modify their access networks to converge on a single common security solution,⁷
- Both proposals acknowledge that the downloaded security components need to remain in the control of the MVPD.⁸

These commonalities represent significant agreement on the underlying principles involved.

⁴ "Each of these systems and permutations have specifics which make them different even from others of a similar type. For example, among direct broadcast satellite systems, there are different conditional access systems in use with different signaling protocols, and different content encryption mechanisms."

⁵ *Proposal 2: Virtual Headend System*, "It should not be necessary to disturb the potentially multiple present and future DCAS and other network technology choices made by cable, DBS and IPTV systems, which leave in place several proprietary systems for delivering digital video programming and services across MVPDs, while still supporting competitive navigation devices."

⁶ *Proposal 2: Virtual Headend System*, "It would not be a step forward to return to an environment in which, to offer access comparable to that of MVPD-sourced devices, across all MVPD programs and services, a competitive manufacturer would have to equip a device with RF tuners for cable and satellite, varied semiconductor platforms to support the dozen-plus proprietary DCAS technologies that may be used, and IP connections for IPTV implementation, and provide for all associated application and field testing."

⁷ *Proposal 2: Virtual Headend System*, "Nor is it reasonable to expect that all operators will radically re-architect their networks, and converge on a common solution in order to avoid the obstacles to competitive solutions."

⁸ *Proposal 2: Virtual Headend System*, "The downloaded security components of the Virtual Headend System do not need to be standardized to a particular hardware platform or CPU architecture, as these aspects remain in the MVPD's control."

A. Proposal 1: DSTAC WG3 HTML5 Security API's Proposal

1. Summary

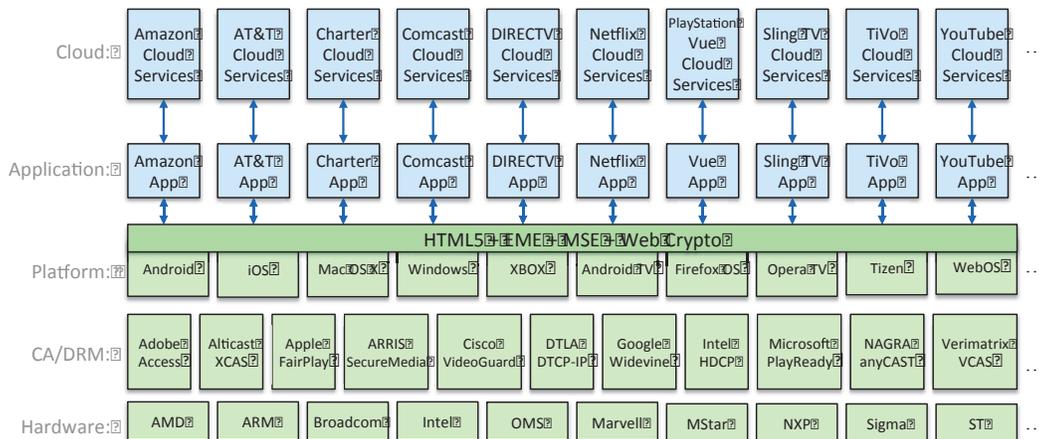


Figure 1 HTML5, EME, MSE & Web Crypto

MVPD/OVDs and CE/CPE companies should adopt the HTML5 media model with Encrypted Media Extensions [EME], Media Source Extensions [MSE] and Web Crypto [WEBCRYPTO] as a non-exclusive, open standard software downloadable security system interface between MVPD/OVD services and consumer electronic devices.

Video providers and distributors have developed a common and open approach to deliver streaming media based on the Internet and the HTTP protocol in particular. HTML has emerged as a strong foundation on which video providers and distributors have based such services. This proposal seeks to leverage these same market forces.

HTML5 is a full application foundation, supporting both security elements (corresponding to DSTAC WG3) and non-security elements (corresponding to DSTAC WG4.) The following proposal will only discuss HTML5 related to the FCC DSTAC WG3 security element requirements.

HTML5 is the open standard defined by the World Wide Web Consortium (W3C) as the cornerstone of the Open Web Platform. Many MVPDs, OVDs, vendors, and members of the DSTAC are members of the W3C, including Adobe, Apple, AT&T, CableLabs, Cisco, Comcast, Cox, EFF, Facebook, Google, HBO, Huawei, IBM, Intel, Microsoft, Mitsubishi, MovieLabs, Mozilla, NAB, Netflix, Opera, Samsung, Sony, Verimatrix, Viacom and Yahoo [W3CMEMBERS].

HTML5 is supported by all major browsers (both on PCs and embedded devices) including Apple Safari, Google Chrome, Microsoft Edge, Mozilla Firefox and Opera.

HTML5, EME, MSE and Web Crypto are being deployed across the Web today by multiple vendors on hundreds of millions of devices, including mobile, PCs, TVs, set-tops and game machines. HTML5 is a software system portable across content protection systems, device hardware and CPU architectures (including AMD, ARM, Broadcom, Intel, OMS, Marvell, MStar, NXP, Sigma and ST).

HTML5, EME and MSE are already being used for multiplatform commercial services such as Netflix, YouTube movies, Google Play, and Apple movies. It is also the basis for multiplatform DLNA VidiPath cloud services.

W3C HTML5 provides a uniform architectural framework for access to media streams. HTML5 uses IETF MIME types for identifying media formats. HTML5 is sufficient to play unencrypted media and link level protected media (e.g. DTCP-IP or HDCP).

EME extends HTML5 to support common-encrypted media decryption by one or more DRM. MSE extends HTML5 to support adaptive video. MSE and EME are designed to work closely together. Almost all content protection companies surveyed and discussed in WG3 now support or plan to support EME, including Adobe Access, Alticast XCAS, Apple FairPlay, ARRIS SecureMedia, Broadcom, Cisco VideoGuard, Google Widevine, Intel SGX, Microsoft PlayReady, NAGRA anyCAST and Verimatrix VCAS.

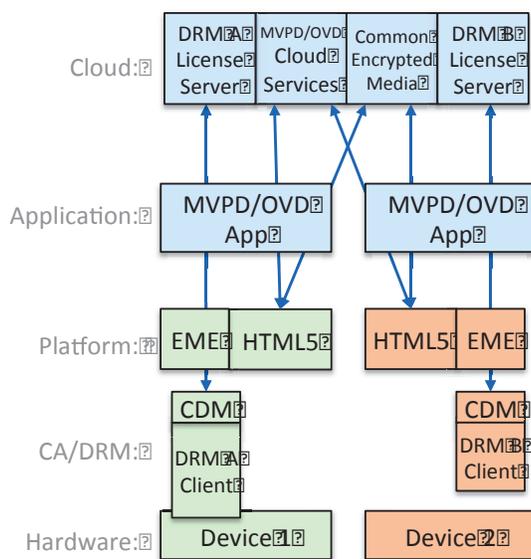


Figure 2 HTML5 EME Common Encryption

Common Encryption (AKA key-sharing or simulcrypt) allows multiple security systems of potentially diverse and divergent design to simultaneously operate on the same content stream or file. This powerful property acts a safety net for choice and for countering attempts of vendor lock-in. The technique is widely deployed in numerous systems today including several major US MVPD's and almost all external to North America. It is also widely used in OTT

and Internet delivery systems and called out in the related standards. Implicit in common encryption is the use of a standardized encryption algorithm (e.g. AES).

W3C Web Crypto provides basic cryptographic operations to support use cases such as user authentication and certificate access.

Note that while these W3C APIs are used in Web browsers, they can also be used outside of a browser in a traditional native application, in a widget or as a Web view exposed by the device platform.

Note that this discussion should be considered informative - the normative references are the latest versions of the referenced W3C & IETF specs.

2. System Description

The system consists of MVPD/OVDs supplying media streams over HTTPS and CE/CPE devices accessing and decrypting those media streams by supplying devices that implement the HTML5, EME, MSE and Web Crypto APIs.

a) Software components

(1) MVPD/OVD Media Requirements

The following describes how MVPD/OVDs supply media streams over HTTPS.

- (a) MVPD/OVD provides media via HTTP(S) [HTML5].
- (b) MVPD/OVD supplies MIME types with codecs and profiles for all media files. [RFC 2045][RFC6381]
- (c) MVPD/OVD media may be made available on any mix of cloud-based URLs and/or home LAN-based URLs. The distribution of media across cloud vs. LAN is flexible.
- (d) MVPD/OVD media on cloud-based URLs may be unencrypted or encrypted with a common encryption method. (e.g. ISO Common Encryption). [EME]
- (e) MVPD/OVD media on home LAN-based URLs may be unencrypted, encrypted with a common encryption method or sent via a link level encryption method (e.g. DTCP-IP or HDCP).
- (f) MVPD/OVD supports at least one key server (for any DRM that supports EME) for each common encryption format supported by that MVPD/OVD. [EME]
- (g) MVPD/OVDs can support adaptive bit-rate video access for cloud-based media and optionally for home LAN based media. [MSE]

(2) CE/CPE Platform Requirements

The following describes how CE/CPE devices access and decrypt MVPD/OVD media streams by supplying devices which implement the HTML5, EME, MSE and Web Crypto APIs.

- (a) CE/CPE provides HTML5 Media Element APIs for all media access.
- (b) CE/CPE describes support for all media MIME types with codecs and profiles via `canPlayType()` [HTML5][RFC 2045][RFC6381]
- (c) CE/CPE plays all supported unencrypted and all link encrypted media (e.g. DTCP-IP or HDCP) via HTML5 video and audio elements
- (d) CE/CPE plays all supported common encryption media (e.g. ISO Common Encryption) via EME API.
- (e) CE/CPE supports at least one DRM Content Decryption Module (CDM) capable of decrypting each common encryption format supported [EME].
- (f) CE/CPE supports MSE API for all adaptive video.
- (g) CE/CPE supports Web Crypto for application-based user authentication and for access to any platform certificates.

(3) Overall Requirements

The following describe overall requirements applying to MVPD/OVDs and CE/CPE platforms

(a) Following the practice of the IETF and W3C, the specific CDM/DRM, link protection, media format and common encryption technologies used are not mandated, allowing technology evolution, vendor interoperability, and marketplace competition.

(b) Following the practice of the IETF and W3C, all referenced specs will be considered to refer to the latest spec versions. For example, HTML5 may be replaced with HTML5.1, when published. Similarly, key IETF RFCs are updated over time.

(c) This usage of the HTML5 APIs is non-exclusive for both MVPD/OVDs and CE/CPE, because while HTML5 provides the best environment for portable, write-once, run-everywhere applications, there are still market requirements for non-portable applications that may not use these APIs for security system access. For example, applications on popular mobile platforms are often written in native code. Also, apps are sometimes written to non-portable APIs to access special platform capabilities (e.g. game platforms with gesticulation interfaces).

(d) Following the practice of the W3C, the HTML5, EME, MSE, and Web Crypto specifications were drafted under a royalty free patent license policy. IETF specifications are drafted under a RAND IPR policy, but in practice contributions are generally only accepted under royalty free terms.

(e) The software programs (applications and libraries) which call the HTML5, EME, MSE, and Web Crypto APIs, choose from available content protection technologies, resolutions and formats and also implement some security aspects, such as user authentication and certificate access. There is no restriction on authorship of these programs, which could be written by an MVPD, OVD or CE company.

b) Hardware components (if any)

There are no specific hardware requirements.

Some media may have generic hardware requirements. For example, UHD content may require a hardware root of trust. As another example, 3D video may require a hardware 3D display. But there are no specific hardware requirements, such as a particular CPU architecture, a particular hardware root of trust or a particular chip or chip component of any kind.

c) Operational description (download, startup, update, etc.)
The MVPD/OVD media is accessed over the well-understood HTTP(S) model. The CE/CPE HTML5, EME, MSE & Web Crypto APIs operate under the well-understood HTML runtime.

The software downloadable security system (DSS) runtime operations of discovery and key server communication are defined in the EME Content Decryption Module (CDM) abstraction, which standardizes this behavior across all supported DRMs.

All other DSS operations (downloading the DSS, installing the DSS, updating the DSS, DSS rollback, etc.) are not standardized in the HTML5 model. These operations may be defined by the DSS, the operating system, the user agent and/or the underlying hardware root of trust.

Each CDM or link level protection may be implemented in software or hardware or some combination of the two. The HTML5 and EME APIs are the same.

The CDM or link level protection system itself is downloadable and can be downloaded with an application, downloaded separately or pre-integrated in a hardware or software platform.

The combination of a common API with differing security operations provides for portable, write-once, run-everywhere applications while still preserving a competitive market of DSS systems and a competitive market of hardware roots of trust.

3. Benefits/Costs

a) Royalty Free: HTML5, EME, MSE, Web Crypto and all W3C APIs are available Royalty Free under the W3C Patent Policy [W3CPP] with Royalty-Free licensing commitments from over sixty companies [HTML5LIC]

b) Open source: HTML5, EME, MSE, Web Crypto software implementations are available at no cost from at least three open source libraries - Chromium, Gecko and WebKit - which have been integrated into hundreds of millions of devices.

c) Portable applications: The single HTML5 API, supported across all major CPU architectures, all major DRMs and on all types of devices from smart phones, tablets, PCs, Macs, smart TVs, set-tops and game systems, enable write-once, run everywhere applications.

- d) Competitive security systems: A common abstraction for both CA/DRM systems and link protection systems makes for a competitive market for security systems. Additionally, EME enables innovation in both hardware and software implementations that can advance ahead of, or in response to, the growing sophistication of attacks on these security systems. By not mandating a single security system, it avoids creating a single point of attack for hackers.
- e) Evolving functionality: By requiring usage of latest specification APIs, the architecture will evolve to meet new requirements rather than being stuck with the technology at the initial definition.
- f) Support TV and Internet merging: By basing the proposal on leading Web and Internet protocols, the proposal supports continued merging of TV and Internet media services.
- g) Field proven: This proposal is not unduly burdensome, as it has been implemented by all of the commercial browser vendors and is already being used by multiple content distributors, including Netflix, Google YouTube and Apple for premium content.
- h) Uniform API: HTML5, EME, MSE and Web Crypto provide a uniform architectural framework and provide uniform JavaScript APIs.
- i) Technology- and platform-neutral: The HTML5 architecture is technology- and platform-neutral as it does not mandate specific software or hardware technologies or platforms. Nor does it mandate a particular network technology or architecture.
- j) Software-based downloadable security systems: HTML5 and EME MIME and EME are clearly software-based solutions and provide access to downloadable security systems.
- k) CE/CPE choice: A device manufacturer can choose one or more link level protection technologies and/or one or more DRM/CA technologies from a competitive market of commercial content protection technologies to implement on their device. These technology choices can be updated or changed after the device is sold and in the market as a device manufacturer chooses to renew the security systems on its devices. A wide variety of CE devices support HTML5 including smart phones, tablets, PCs, Macs, smart TVs, set-tops and game systems.
- l) Security providers competition: Content protection providers can compete on the robustness of their implementation, their countermeasures, threat monitoring, etc. Content protection technologies can easily be updated or abandoned based on security breaches. As multiple CA/DRMs are abstracted and supported, no single point of attack is created.
- m) Chip manufacturer competition: Hardware chip manufacturers can continue to compete on the quality of their hardware roots of trust

and on their integration with DRM, CA and link level protection technologies and trust models.

n) MVPD/OVD choice: MVPD/OVDs can choose from a competitive content protection market which technologies to support on their network to secure their content. MVPD/OVDs can also add to or replace their content protection systems over time.

o) Minimizes proprietary code: From the EME spec: “The common API supports a simple set of content encryption capabilities, leaving application functions such as authentication and authorization to page authors. This is achieved by requiring content protection system-specific messaging to be mediated by the page rather than assuming out-of-band communication between the encryption system and a license or other server.” These security-related functions rely on apps and other means that are CDM/DRM/CA security-system independent.

p) Provides common IP abstraction to MVPD/OVD network security elements: By supporting IETF and W3C APIs for access to security elements for MVPD/OVD streams made available via IP, this proposal avoids the cost and complexity of building to and testing against each of the divergent MVPD/OVD access network security elements.

4. Requirements Analysis

The HTML5 Proposal is evaluated against the requirements outlined in section II.B Downloadable Security System – Common Requirements.

1) *Verifies the navigation device reports having the necessary components for receiving the media provider’s service, and it identifies if the device has been tampered with or compromised.*

This verification remains the responsibility of the security system. The related robustness and compliance rules govern the level of security provided by the implementation. CA/DRM providers typically leverage hardware components (e.g. root of trust and trusted execution environment) to perform this function (see section II.C Existing Downloadable Security System Solutions). In the case of link level protection, it is the robustness and compliance rules of the link protection that govern the implementation.

2) *Verifies the integrity of the software components that are downloaded and installed in the navigation device to ensure that those components have not been compromised at download, installation, boot, or runtime. This is typically done by code signature verification.*

A CA/DRM implementation can either be downloaded separately or as a part of the OS. In the case where it is a separate download, the download process (either provided by the OS or a separate application) validates the integrity of

the implementation. In the case where the CA/DRM is a part of the OS, it is the OS download process that performs this function. CA/DRM providers typically make use of proprietary protocols and leverage any hardware support (e.g. root of trust and trusted execution environment) to perform this function (see section II.C Existing Downloadable Security System Solutions). In the case of link level protection, it is the robustness and compliance rules of the link protection that govern this.

3) *Authenticates or supports the authentication of the user of the device as being authorized for receiving the media provider's service. This may be implicit when using a managed device assigned to a user.*

User authentication is the responsibility of the application. The Web Crypto library supports user authentication. In the case of a CA/DRM implementation, it is the responsibility of the security system to securely communicate the device entitlements or usage rights for this user. In the case of link level protection, the content source and destination are trusted based on mutual authentication.

4) *Provides to the navigation device secure and verifiable information on the authorized services available to the device and user.*

In the case of an EME implementation the JavaScript APIs are used to communicate to the application whether the service is available to the device and user. In a CA/DRM implementation the implementation provide APIs specific to that implementation to convey this information (see section II.C Existing Downloadable Security System Solutions). In the case of link level protection, it is the robustness and compliance rules of the link protection that govern the implementation.

5) *Enables descrambling of the authorized services available to the device.*

In the case of a CA/DRM implementation it is the implementation that is responsible for descrambling the authorized services available to the device. CA/DRM providers typically leverage hardware components (e.g. hardware decryption engines and trusted execution environment) to perform this function (see section II.C Existing Downloadable Security System Solutions for the types of scrambling algorithms supported). In the case of link level protection, the encryption on the link is specified by the link protection technology (e.g. DTCP-IP).

6) *Performs a secure download from the network to a client device, for either first time installation of content security software, or a software update.*

See (2) above.

7) *In the network, encrypts content for later consumption, either on a real time or pre-encrypted basis, packetized in accordance with the target delivery system.*

In the case of a CA/DRM implementation content encryption is performed in the network, either on a real time or pre-encrypted basis, packetized in accordance with the target delivery (see section II.C Existing Downloadable Security System Solutions for the types of scrambling algorithms supported). In the case of link level protection within the home network, the encryption/decryption is performed by endpoints and the content is packetized on the link as specified by the link protection technology.

8) *In the network, encrypts software to be downloaded, either on a per client device basis, or based on a parameter or set of parameters that enables a group of devices to be targeted for download as an ensemble.*

See (2) above.

9) *In the network, distributes entitlement information in various forms, using either one-way or two-way protocols, depending on the delivery network type.*

See (3) above and section II.C Existing Downloadable Security System Solutions.

From the EME spec: "The common API supports a simple set of content encryption capabilities, leaving application functions such as authentication and authorization to page authors. This is achieved by requiring content protection system-specific messaging to be mediated by the page rather than assuming out-of-band communication between the encryption system and a license or other server."

10) *The DSS fulfills the commercial and/or regulatory obligations of an MVPD to protect content from content sources/owners.*

In the case of a CA/DRM implementation it is the implementation that fulfills the commercial and/or regulatory obligations of an MVPD. The related robustness and compliance rules govern the level of security provided by the implementation. CA/DRM providers typically leverage hardware components (e.g. root of trust and trusted execution environment) to perform this function (see section II.C Existing Downloadable Security System Solutions). In the case of link level protection, it is the robustness and compliance rules of the link protection that govern the implementation.

5. Additional Specifications

HTML5	W3C HTML5	http://www.w3.org/TR/html5/
EME	W3C Encrypted Media Extensions	http://www.w3.org/TR/encrypted-media/
MSE	W3C Media Source Extensions	http://www.w3.org/TR/media-source/
WEBCRYPTO	W3C Web Cryptography API	http://www.w3.org/TR/WebCryptoAPI/
W3CMEMBERS	W3C Current Members	http://www.w3.org/Consortium/Member/List
RFC2045	IETF RFC 2045	https://tools.ietf.org/html/rfc2045
RFC6381	IETF RFC 6381	http://tools.ietf.org/html/rfc6381
W3CPP	W3C Patent Policy	http://www.w3.org/Consortium/Patent-Policy-20040205/
HTML5LIC	HTML5 Royalty Free License Commitments	http://www.w3.org/2004/01/pp-impl/40318/showCommitments
IETF IPR	IETF IPR Policy	http://tools.ietf.org/html/rfc3979

B. Proposal 2: Virtual Headend System

As is documented in the working group 2 and working group 4 reports, there is a wide variety of network architectures, delivery networks, and security systems in use by MVPDs today. These include both “mostly” one-way systems, like direct broadcast satellite, traditional cable HFC/QAM systems, IP-centric telco systems, and combinations thereof (e.g., Verizon FiOS). Within these, there are security systems rooted in Smartcard conditional access technologies, traditional embedded conditional access security technologies, and various permutations based on DRM-style security controls.

Each of these systems and permutations have specifics which make them different even from others of a similar type. For example, among direct broadcast satellite systems, there are different conditional access systems in use with different signaling protocols, and different content encryption mechanisms. Unless all MVPDs replace or upgrade these proprietary solutions with some common and interoperable means of network termination using a downloadable conditional access system (DCAS) or other technology however, only such devices as are designed for these proprietary systems and authorized by the specific MVPD can connect directly to the MVPD network to achieve full access. It should not be necessary to disturb the potentially multiple present and future DCAS and other network technology choices made by cable, DBS and IPTV systems, which leave in place several proprietary systems for delivering digital video programming and services across MVPDs, while still supporting competitive navigation devices.

Because there is such a wide variety of network technologies in use, the best solution which is both not technically burdensome, and supports retail devices which are both portable across MVPDs and geographically, is to create a technical solution that abstracts the network differences of MVPDs away. Such a solution will support the operation of commercial competitive devices to receive all MVPD content on all MVPD systems, as required by Section 629⁹ and as a congressionally directed task.¹⁰

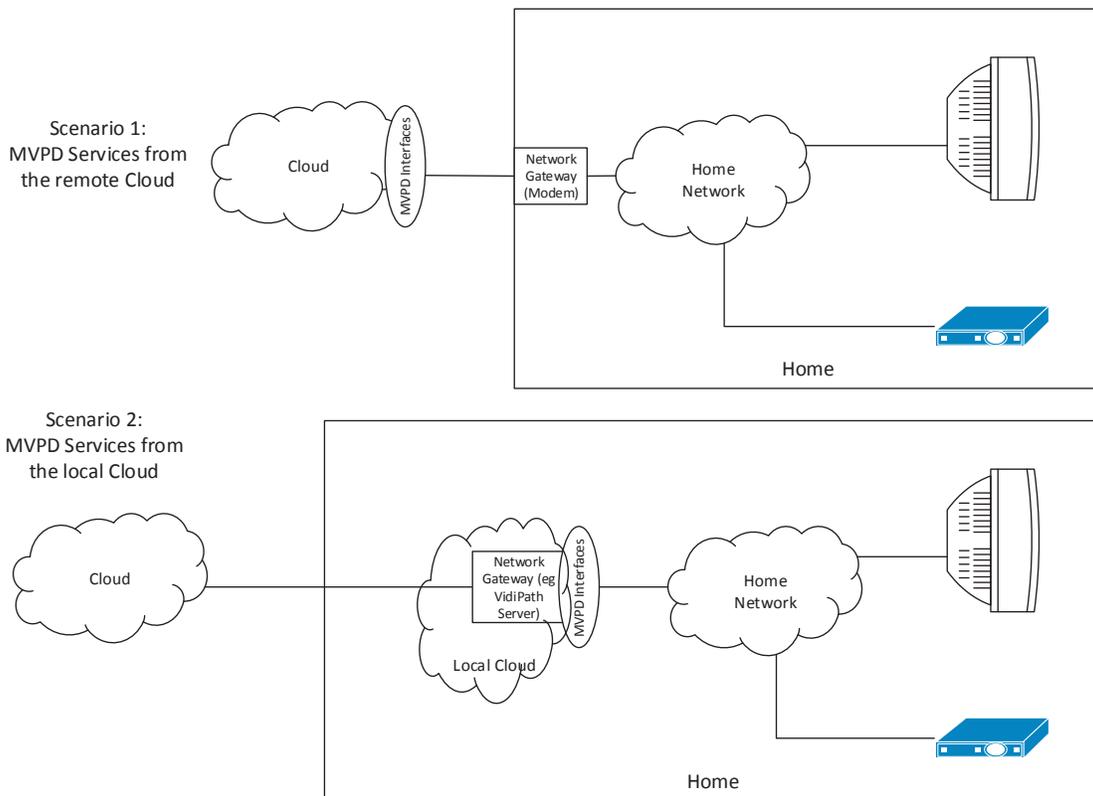
It would not be a step forward to return to an environment in which, to offer access comparable to that of MVPD-sourced devices, across all MVPD programs and services, a competitive manufacturer would have to equip a device with RF tuners for cable and satellite, varied semiconductor platforms to support the dozen-plus proprietary DCAS technologies that may be used, and IP connections for IPTV implementation, and provide for all associated application and field testing. Nor is it reasonable to expect that all operators will radically re-architect their networks, and converge on a common solution in order to avoid the obstacles to competitive solutions.

Instead a Virtual Headend System is a cloud-based security system. Network security and conditional access are performed in the cloud, and the security between the cloud and retail

⁹ 47 U.S.C. § 549(a).

¹⁰ DSTAC Charter, Dec 2014.

navigation devices is a well-defined, widely used link protection mechanism such as DTCP-IP. A MVPD may choose a system architecture for a Virtual Headend System that includes a device located at a consumer's location (e.g., home), which provides a "local cloud" which has security system components downloaded to it as necessary, or the entire solution may be in their network "cloud" and offered as IP services directly to devices in the home. The downloaded security components of the Virtual Headend System do not need to be standardized to a particular hardware platform or CPU architecture, as these aspects remain in the MVPD's control. The Virtual Headend System's interface to the home network (and retail devices) is standardized across MVPDs and thereby enables nationally-portable retail navigation devices without imposing an undue burden on MVPDs or retail device manufacturers. Furthermore, this link-protection mechanism can be extended to account for end-to-end IP systems, providing a clear path to purely protocol-based service integration in modern MVPD networks.



DBS providers currently provide devices with functionally similar to a Virtual Headend solution with a "local cloud" device. Dish's Hopper and DirecTV's Genie are currently-distributed devices that serve as Virtual Headend Systems via mixes of standard and proprietary protocols, and provide services to a range of consumer devices connected to the home network "cloud". In order to provide a uniform mechanism for competitive navigation device integration, some form of gateway device will continue to remain a practical necessity for unidirectional distribution networks under any security scheme suggested that complies with the DSTAC's charter.

Comcast and other Cable MVPDs have announced both a “local cloud” solution using VidiPath enabled server devices¹¹, as well as a true virtual cloud solution such as “Comcast Stream.”¹² These solutions provide content services to unmanaged devices without requiring the implementation or download of MVPD network-specific technologies.

These current efforts from MVPDs demonstrate that operators are working towards Virtual Headend System technology that abstracts legacy network systems into common IP network protocols that serve non-proprietary navigation devices.

¹¹ “XFINITY for VidiPath enables customers with XFINITY on the X1 Entertainment Operating System to stream video content, including live TV and recorded DVR programs, directly to a VidiPath-compatible device (e.g., smart TV) without the need for an additional set-top box.”
<http://customer.xfinity.com/help-and-support/cable-tv/vidipath-overview/>

¹² “No extra device or additional equipment required...or even a TV. And it’s called Stream”,
<http://corporate.comcast.com/comcast-voices/a-new-streaming-tv-service-from-comcast>; “an IP-based cable service that offers live, on demand and cloud DVR delivered over our managed network in the home”, <http://www.engadget.com/2015/07/12/comcast-xfinity-internet-stream/>.

V. Annexes

A. MVPD Security System Validation Process

For traditional MVPD deployed set-tops, SoC and set-top box validation is normally done at the direction of the CAS or DRM provider, in response to requirements from content providers and MVPDs. This testing includes a validation of both the SoC and the set-top box that is built using the SoC.

SoC Validation Process

The following is a typical validation process for the SoC:

1. The technical requirements of the CAS or DRM provider derived from requirements from content providers and service providers are made available under license to the SoC vendor. These technical requirements have two parts:
 - a) Functional requirements – These are the capabilities and features of the SoC (e.g. cryptographic algorithms, codecs, graphics capabilities, etc.)
 - b) Robustness rules – These rules relate to characteristics of the SoC that are not testable by functional testing. They describe what level of security protection is required, rather than how the security functions are to be implemented.
2. Once the SoC vendor has implemented the technical requirements, the vendor will bring in its device to the CAS or DRM provider for validation. This validation has two parts:
 - a) Functional validation – This involves running functional tests on a reference or development platform that uses the SoC, to insure that it meets the functional requirements, e.g. properly process a video stream, clear appropriate registers when reset, properly implement cryptographic algorithms, etc. This testing is done independently of the SoC vendor, but will involve iterations with SoC vendor when issues are discovered.
 - b) Robustness validation – Since these requirements are not addressed through functional testing, the SoC vendor provides documentation describing how it has met the robustness requirements. This may involve a design review with the SoC vendor or may be done through a third-party review process, e.g. a common criteria evaluation.
3. Once the SoC has cleared this validation testing, a record of this is communicated to the SoC vendor, for example a letter to the SoC vendor confirming validation of the specific SoC version. Device manufacturers can use this as confirmation that the CAS or DRM provider has validated the SoC.
4. If the SoC vendor makes changes to the device, either hardware or software, the vendor is required to notify the CAS or DRM provider of the changes. The CAS or DRM provider will review the changes or contract with a third-party to review the changes and will determine if the SOC needs to be retested. In addition, the CAS or

DRM provider will often monitor which SoC versions are in the market to ensure that they are aware of any SoC revisions of which the vendor may have failed to notify them.

5. In order for a SoC to go through this process with the CAS or DRM provider, the SoC vendor signs a support agreement that obliges it to notify the CAS or DRM provider of any changes or revisions.
6. This process typically takes a number weeks or months for a new SoC, based on any issues that may be discovered through the process. The robustness review is typically the longest portion.
7. The SoC vendor needs to have a Black Box vendor approved by the CAS or DRM provider to inject the right keys into the SoCs at manufacture.
8. Set-top box manufacturers request from the SoC vendor a list of validated parts and the CAS or DRM provider can also verify this. Often the device manufacturers and SoC vendors work closely together through the validation process.
9. The SoC vendor will typically include countermeasures in its implementations, either of its own design or that of the CAS or DRM provider, to support renewability and upgrades in the field if necessary.

Set-top Box Validation Process

The set-top box validation process is very similar to the SoC validation process:

1. Set-top boxes must use a validated SoC before they can be submitted for validation.
2. The set-top box manufacturers must also license functional requirements and robustness rules from the CAS or DRM provider.
3. Devices have a similar process for SOC validation, e.g. functional testing and robustness design reviews.
4. To avoid cloned set-top boxes, the CAS or DRM provider may maintain a database of all the SoCs that could possibly be in the field. Service providers can use this database to validate devices as they attach to their network.
5. CAS or DRM providers monitor hacker sites and any unusual activity, such as the same device being installed in two different locations (cloning).

System and Device Testing Regimes

In addition to the set-top box validation described above, there are various regimes that are used for device and system testing. MVPDs will conduct system testing through a series of phases beginning with lab testing to validate that the system functions in a controlled environment. This is followed by limited field-testing, usually with employees, to validate that the system functions on a production network, and then followed by more expanded field-testing with paying subscribers to validate that the system functions in real customer use scenarios. This process ultimately leads to full deployment once all of the bugs have been worked out in the system, the set-top box, the installation process, provisioning, and customer support.

Device testing by itself can fall into one of a number of different testing regimes:

- 1) Device testing is done as part of system testing described above.

- a) Device testing is conducted through a third-party to test compliance with published specifications or standards; examples of third party testing organizations include DLNA, CableLabs, Wi-Fi Alliance, etc. The CableLabs certification process is an example of this type of test regime. The CableLabs certification is described through a set of publicly available guidelines (<http://www.cablelabs.com/wp-content/uploads/2014/01/CWGuidelines.pdf>). The test plans and test tools are available under NDA, and CableLabs offers development lab assistance under which device manufacturers can test their devices before certification submission. CableLabs staff conducts the device testing and reports test results to the device manufacturer. Test errors will be reproduced in the test lab if requested and there is a formal appeal process for pass/fail decisions.
- b) Devices are self tested or self certified by the device manufacturer to be in compliance with either published specifications or standards or even proprietary systems.

As mentioned above, the stronger and more thorough the testing regime, the greater the level of confidence in the device's compliance with the functionality and robustness requirements. The testing regimes above move from strongest (device testing as part of system testing) to weakest (self testing). In the case of Uni-Directional Cable Products (UDCP), CableLabs permitted a process that moved from CableLabs validation to one of self-certification.

Testing in Existing Retail Systems

In existing retail systems that are supported by MVPDs today, there are several examples of how app/device testing is applied for these systems:

- a) MVPD TV Apps – MVPD TV Apps place much of the burden of testing onto the MVPD and relieve the retail manufacturer of testing their device with every MVPD. The Apps are made available through an App store supported by the retail device manufacturer or their platform partner. These App stores have license conditions, guidelines, and limitations on Apps. The App platform provider reviews these Apps before they are released. Retail manufacturers may also test MVPD TV Apps on their devices to insure they meet platform guidelines.
- b) HTML5 Web Apps – HTML5 implementations allow the retail manufacturer to self-test their browser or the browser vendor to self-test its browser on multiple devices. The MVPD can test its Web App on multiple devices. This approach splits the testing burden among all parties.
- c) VidiPath/RVU – These make use of third party compliance testing for devices through DLNA and RVU Alliance. The MVPD can test its devices and RUI Apps against certified devices.

Renewability in these systems is achieved through updates to the App, the platform, the Web browser, or the DRM system.

If a retail device connects directly to the MVPD network, it must be tested to assure compliance with requirements similar to those discussed above for MVPD set-top boxes in the sections on SoC and set-top box validation. This verification testing must initially be conducted through an MVPD-approved certification test process. It may be possible to design a self-certification test process for subsequent devices.

B. MVPD Entitlements within the existing MVPD Service

Conditional Access Systems and subscriber Entitlements have always been inextricably intertwined by design. Typical conditional access systems encrypt video content via a 64 or 128 bit number known as a control word (CW). The control word is delivered to a STB as part of the video stream, but in an encrypted form known as an Entitlement Control Message (ECM). It is the principle job of a conditional access system to create these ECMs in a manner such that they cannot be opened by anyone who is not authorized to use them, and to provide the set top with a process to open them when they are authorized. The STB has a mechanism to retrieve the ECM from the video stream, but the STB will still need special authorizations enabling that STB to decrypt the ECM and thus decrypt the MPEG video. For this, the CAS system creates a unique message known as an Entitlement Management Message (EMM) which is targeted to a specific STB and typically delivered outside of the video stream. Every STB in a video network will be sent EMMs that only that box can open and use to decrypt video that has been purchased by that subscriber. The generation of an EMM for a specific STB begins with an authorization delivered from the billing system when a service, such as 'Discovery Channel', is purchased by a subscriber. When an EMM is received by the STB, it will open the EMM using its hardware Root of Trust as a decryption key. That will produce the key to decrypt the ECM, which is opened by the STB. That produces the CW that is used to decrypt the video.

Video is often delivered with certain information denoting rights to copy. Most commonly, this is via a convention known as Copy Control Information, or CCI for short. The CCI is a one byte flag included in video streams that allows content owners as well as distributors to specify how content can be duplicated. Some of the common settings for the CCI field include copy freely (content is not copy protected), copy no more (no more copies permitted), copy once, and copy never (may be recorded but is not transferable). This provides a high level, albeit weak mechanism to convey certain embedded entitlements that go along with content. Typical DRM (digital rights management) systems have an ability to provide more advanced entitlement mechanisms and a rich rights expression language that can convey more extensive and variable access, copying, distribution, and usage rights.

For compatibility with a legacy video system that utilizes QAM transmission and distribution, CPE devices must contain SoCs (system on a chip) that embody certain embedded functions. This includes the notion of a hardware root of trust, which is a unique identifier that is placed in a 'one time programmable' (OTP) location on the SoC. The unique number for each STB is generated by a Trust Authority and injected into the OTP slot using a process jointly defined by the Trust Authority and the SoC Vendor. These SoCs must also implement the current decryption algorithms used by US cable operators, which include the DVB Common Scrambling Algorithm (DVB CSA 2) and SCTE-52 with a MediaCipher IV (Initialization Vector).

C. Technical Standards

1. Security Standards

Standards relating to encryption, hashes, and related items

AES	Advanced Encryption Standard	http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf
TLS	Transport Layer Security	https://tools.ietf.org/html/rfc5246
CSA	Common Scrambling Algorithm	http://www.etsi.org/deliver/etsi_TS/103100_103199/103127/01.01.01_60/ts_103127v010101p.pdf
DVB SimulCrypt	Digital Video Broadcasting (DVB);	http://www.etsi.org/deliver/etsi_ts/103100_103199/103197/01.05.01_60/ts_103197v010501p.pdf
FIPS 180-1	Secure Hash Standard	http://csrc.nist.gov/publications/PubsFIPS.html#fips180-4
RSA	Public Key Encryption	http://www.emc.com/emc-plus/rsa-labs/standards-initiatives/public-key-cryptography-standards.htm
SCTE 201	Open Media Security (OMS) Root Key Derivation Profiles and Test Vectors	http://www.scte.org/documents/pdf/Standards/ANSI_SCTE%20201%202013.pdf
SCTE 52	Data Encryption Standard – Cipher Block Chaining Packet Encryption Specification	https://www.scte.org/documents/pdf/Standards/ANSI_SCTE%2052%202013.pdf
DES	DES encryption standard	http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf
ETSI TS 103 162 V1.1.1 (2010-10)	Access, Terminals, Transmission and Multiplexing (ATM); Integrated Broadband Cable and Television Networks; K-LAD Functional Specification	http://www.etsi.org/deliver/etsi_TS/103100_103199/103162/01.01.01_60/ts_103162v010101p.pdf
DTCP/IP	DTCP/IP	http://www.dtcp.com/specifications.aspx

2. Networking and Communication Standards

Standards relating to communication and transmission to and inside homes.

_802.11	Wireless LAN Standards	http://standards.ieee.org/about/get/802/802.11.html
ATSC for OTA tune	Off the Air	http://atsc.org/standard/a72-parts-1-2-and-3/
Bluetooth	Bluetooth Core Version 4.2	https://www.bluetooth.org/DocMan/handlers/DownloadDoc.ashx?doc_id=286439 https://www.bluetooth.org/en-us/specification/adopted-specifications
DTCP CVP-2	DTCP CVP-2	http://www.dtcp.com/documents/dtcp/20150309-dtla-cpv2-v1-rev-1-1.pdf
DIRECTV (legacy DSS) transport	International Telecommunications Union, Recommendation ITU-R BO.1516, 2001, "Digital multiprogramme television systems for use by satellite operating in the 11/12 GHz frequency range, System B"	https://www.itu.int/dms_pubrec/itu-r/rec/bo/R-REC-BO.1516-0-200104-S!!PDF-E.pdf
DLNA	DLNA	http://www.dlna.org/guidelines/
DSG	DOCSIS Set-top box gateway	http://www.scte.org/documents/pdf/standards/ANSI_SCTE%20106%202010.pdf
DVB-S, DVB-S2	Satellite broadcasting standard	https://www.dvb.org/standards/dvb-s2
Ethernet	Ethernet networks standards	https://standards.ieee.org/about/get/802/802.3.html
HDMI	HDMI	http://www.hdmi.org/manufacturer/specification.aspx
MoCA	Multimedia over Coax	http://www.mocalliance.org/
RVU	RVU Alliance	http://rvualliance.org/specification-availability
SCTE-55	Legacy Out of Band (OOB) communications	http://www.scte.org/documents/pdf/standards/SCTE%2055-1%202009.pdf
UHD Alliance	documents (available in a few months)	http://www.uhdalliance.org/
UPnP	Universal Plug and Play	http://upnp.org/specs/arch/UPnP-arch-DeviceArchitecture-v1.1.pdf
USB	Universal Serial Bus	http://www.usb.org/developers/docs/

3. Encoding Standards

Standards used for digitally encoding audio and video

AAC	Information technology -- Generic coding of moving pictures and associated audio information -- Part 7: Advanced Audio Coding (AAC)	http://www.iso.org/iso/iso_catalogue/catalogue_ics/catalogue_detail_ics.htm?csnumber=25040
DASH	MPEG-DASH Profile for Transport of ISO BMFF Based DVB Services over IP Based Networks	https://www.dvb.org/resources/public/standards/a168_dvb-dash.pdf
Dolby Digital	Audio format	http://www.dolby.com/us/en/technologies/dolby-digital-plus.html
H.264/AVC	H.264	http://www.itu.int/rec/T-REC-H.264-201402-I/en
H.265/HEVC	HEVC	http://www.itu.int/rec/T-REC-H.265-201504-P/en
HLS	Apple adaptive bit rate streaming	https://github.com/winlinvip/simple-rtmp-server/blob/master/trunk/doc/hls-m3u8-draft-pantos-http-live-streaming-12.txt
ISO/IEC 13818-1:2015	Information technology, Generic coding of moving pictures and associated audio information: Systems	http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=67331
MPEG-1,2, DASH, TS	MPEG Specifications	http://mpeg.chiariglione.org/standards
MPEG-2 Transport	Specification for the MPEG Transport format	http://www.etsi.org/deliver/etsi_ts/103100_103199/103197/01.05.01_60/ts_103197v010501p.pdf
HTTP Live Streaming	HTTP Live Streaming, IETF Internet-Draft	https://tools.ietf.org/html/draft-pantos-http-live-streaming-16
Microsoft DLNA Extensions	Digital Living Network Alliance (DLNA) Networked Device Interoperability Guidelines: Microsoft Extensions	http://download.microsoft.com/download/9/5/E/95EF66AF-9026-4BB0-A41D-A4F81802D92C/[MS-DLNHND].pdf

4. Service Standards

Standards used for the delivery of MVPD services, and to comply with regulatory requirements

RRT	U.S. Region Rating Table (RRT)	https://www.ce.org/Standards/Standard-Listings/R4-3-Television-Data-Systems-Subcommittee/CEA-766-C-(ANSI).aspx
VBI Data	VBI Data in Cable Digital Transport Streams	http://www.scte.org/documents/pdf/Standards/ANSI_SCTE%2021%202012.pdf
CALM act	ATSC Recommended Practice: Techniques for Establishing and Maintaining Audio Loudness for Digital Television (A/85:2013)	http://atsc.org/wp-content/uploads/2015/03/Techniques-for-establishing-and-maintaining-audio-loudness.pdf
CEA-608-E	Line 21 Extended Data Services, Closed captioning	http://www.ce.org/Standards/Standard-Listings/R4-3-Television-Data-Systems-Subcommittee/Line-21-Data-Service.aspx
CEA-708-E	Digital Television (DTV) Closed Captioning	http://www.ce.org/Standards/Standard-Listings/R4-3-Television-Data-Systems-Subcommittee/CEA-708-D.aspx
EME	Encrypted Media Extensions	http://www.w3.org/TR/encrypted-media
PSIP	ATSC A/65 Program and System Information Protocol (PSIP) for Terrestrial Broadcast and Cable	http://atsc.org/wp-content/uploads/2015/03/Program-System-Information-Protocol-for-Terrestrial-Broadcast-and-Cable.pdf

5. Other

Miscellaneous Standards

OATC	“Open Authentication Technology Committee”	?
PNG	Portable Network Graphics (PNG) Specification	http://www.w3.org/TR/PNG/
RF4CE	ZigBee RF4CE Specification	https://docs.zigbee.org/zigbee-docs/dcn/09/docs-09-5262-01-0rsc-zigbee-rf4ce-specification-public.pdf

D. Existing Security Solutions Survey Results

Survey Question	AltiCast		ARRIS		Broadcom		Cisco		DTA Security		Intel		Nagra		OMS		Verimatrix	
	AltiProtect	SecureMedia™ Encryption Suite	Broadcom	VideoGuard™	DTA Security	Intel SGX Technology	NAGRA anyCAS	Open Media Security	VCAS									
1. Name of the solution and brief overview																		
2. Features/functions of the downloadable security solution:																		
2.a. Security functions:																		
2.a.i. Does the solution provide conditional access functions (e.g. this service not authorized for this user)?	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Survey Question	AltiCast	ARRIS	Broadcom	Cisco	DTA Security	Intel	Nagra	OMS	Verimatrix
2.a.ii. Does it provide DRM services (e.g. this content can be viewed for 90 days)?	Yes	Yes	Yes	Yes	No	Supports DRM systems but is not itself a DRM system.	Yes Supports complex Content Use Cases	currently being developed in labs.	Yes
2.a.iii. Does it provide link protection across digital interfaces between separate devices?	Yes	Yes	Yes	Yes	Passes CCI	Can support link protection technologies but does not itself provide link protection . iv. Does it provide watermarking or fingerprinting, device and user authentication, or system	Yes DRM, PRM, DTCP-IP and others	as defined by the MPVD's content and technology license	Yes

Survey Question	AltiCast	ARRIS	Broadcom	Cisco	DTA Security	Intel	Nagra	OMS	Verimatrix
2.a.iv. Does it provide watermarking or fingerprinting, device and user authentication, or system renewability?	Yes	third party watermarking systems	Yes	Fingerprinting supported, work with 3rd-party watermarking	Device Auth & System Renewability - Yes, all others No	ISVs can include these functions in their own applications.	Watermarking is implemented using outsourced technology however standards are not agreed and no one wants to pay. Nagra supports user authentication and	no specific watermarking or fingerprinting	Yes, Verimatrix is a pioneer in forensic watermarking; Verimatrix performs device authentication, supports user authentication by the MW or App, and supports

Survey Question	AltiCast	ARRIS	Broadcom	Cisco	DTA Security	Intel	Nagra	OMS	Verimatrix
							renewability		system renewability in a final integrated system
2.b. Network support:									
2.b.i. What kinds of networks (DBS, HFC, FTTH) are supported?	1-way & 2-way	2-way	support satellite, cable and IP	All major MVPD delivery networks	1-way HFC only	SGX is network agnostic.	All Plus terrestrial ATSC M/H, DVB-H, DMB....	2-way	All major networks and more (e.g., existing worldwide DBS, cable, and telco 1- & 2-way networks, unmanaged IP (OTT), and adaptable to new networks)
2.c. Services and Device Functions:									

Survey Question	AltiCast	ARRIS	Broadcom	Cisco	DTA Security	Intel	Nagra	OMS	Verimatrix
2.c.i. What content services are supported (e.g., live TV streams, file based VOD, progressive download VOD, pay per view, or download-rental)?	All	All	All types	All types	Linear only	Depends on the ISV application, but all can be supported.	Yes to all listed use cases and many more	All	All types (as specified by content distribution agreements)
2.c.ii. What consumer device features are supported (e.g., local recording, digital output control, whole-home streaming, out of home streaming of content)?	A full suite of consumer device features	NPVR, local PVR in home and out of home streaming	All types	All types	CCI and DTCP-IP only	Depends on the ISV application, but all can be supported.	Yes including secure removable storage, place shifting, download to go or sideloading, transcoding, expiration enforcement, Enforcement of	All	All types

Survey Question	Verimatrix	ARRIS	Broadcom	Cisco	DTA Security	Intel	Nagra	OMS	Verimatrix
2.d. Device support:							number of streams or copies...		
2.d.i. What are the target consumption devices? Does the system work only on special-purpose, operator managed devices like set-top boxes, or on generic consumer devices like tablets?	both operator-managed devices and consumer devices	both operator-managed devices and consumer devices	Broadcom chipsets have been designed so that they can technically serve a wide variety of devices	Popular devices including Windows PCs, Macs, Apple iOS devices, Android devices, Windows 8 RT/Phone devices, HDMI Dongles, Samsung Smart TV, Roku, PS3/4 and Xbox One	Various DTAs only	Devices with Intel processor including set top boxes, residential gateways, PCs, tablets, and smart phones.	All Devices: STB, Tablet, Phone, USB/HDMI dongles, SmartTV, Regular TV	OMS defines SoC and key requirements	All device types, including both operator-managed devices and consumer devices. MultiRight s approach provides full flexibility in this regard.
2.e. Application support:									

Survey Question	AltiCast	ARRIS	Broadcom	Cisco	DTA Security	Intel	Nagra	OMS	Verimatrix
2.e.i. Does the system present APIs to independent (i.e., not from or controlled by the security provider) applications, for example APIs for service information, authentication status, emergency alert messages, closed captioning information, copy control information?	APIs to verify authorization and enable purchases	API's vary by system	support various APIs	Open APIs (e.g., authentication and authorization copy control) are available for integration of Video Guard with TV Applications	No APIs are presented from the system	Can support whatever the ISV application presents.	Yes, many different API's depending on system and needs	OMS defines APIs that are required to deliver the service provider's service	Client and server-side APIs are published and licensable.
3. Components of the solution									
3.a. Software									

Survey Question	AltiCast	ARRIS	Broadcom	Cisco	DTA Security	Intel	Nagra	OMS	Verimatrix
3.a.i. What parts of the solution are downloadable as software?	CAS and DRM client modules	Entirely software solution	All other than first stage bootloader	Supports fully downloadable security solutions where both DRM and CA components are implemented as downloadable software	The conditional access client is downloaded as software	ISVs build their own SGX enabled applications using an SGX SDK.	All of the software components	software environment, HTML5 applications, and a CAS client	Both CAS and DRM clients are downloadable.
3.a.ii. What is the secure software execution environment (execution environment framework, OS, etc.)	a variety of Trusted Execution Environments, including TrustZone	Work with whatever is available	a separate, self-contained security processor is required to meet all the security requirements and	iOS (5.1 and above), Android (4.X and above), Windows 8 RT, Windows XP SP3 and above (XP SP3 /	secure portion of the SOC	SGX creates HW level robust trusted execution environment.	Various, Depends on device/processor and available resources	OMS does not define a full software environment	TrustZone/ TEE or dedicated security processors, or hardened OS.

Survey Question	AltiCast	ARRIS	Broadcom	Cisco	DTA Security	Intel	Nagra	OMS	Verimatrix
			robustness rules	Vista / 7 / 8 / 8.1), Windows 8, Mac OS 10.6 and above, IE 9.0 and above, Firefox 17.0 and above, Chrome 24.0 and above, Safari 5.1.7.					
3.a.iii. How is code verified, updated? Structure of signing keys and of download images	using Application upgrade protocol	Custom protocol makes use of a SW authentication key which is verified in the first steps of registration and	Security processor is used to verify and renew the SW and FW	All client device software is validated before being run using asymmetric cryptography for	authenticated according to CAL and Cisco licensing materials	Structure of signing keys and of download images SGX verifies the integrity of code to be	Code verified using classical authentication procedures	OMS defines the OTP hardware root of trust	SW is signed (and encrypted) and verified during secure boot process. OTA upgrades

Survey Question	AltiCast	ARRIS	Broadcom	Cisco	DTA Security	Intel	Nagra	OMS	Verimatrix
		authorisation. Additional code signing is employed on platforms where it is supported. As an example, iOS and Android products load images via their respective store in accordance with their required protocol		security		executed in its trusted execution environment and is able to attest to its validity to remote servers.			are also signed and optionally encrypted.
3.a.iv. Software Roll back support? Roll back	Yes	Yes	Security processor is used	Software download and rollback	Yes	This depends on the ISV application	Yes	Not currently	Yes. client-based or enforced

Survey Question	AltiCast	ARRIS	Broadcom	Cisco	DTA Security	Intel	Nagra	OMS	Verimatrix
management				infrastructure are dictated by the specific application download environment		n.			by the head-end.
3.a.v. In what format are Application interfaces provided?	APIs to verify authorization and enable purchases	http / XML or C or JNI or JAVA or objective C	provide specific information/tools to help the security partners and/or OEMs to verify, renew and revoke SW and FW	C, Java, JS, Objective C, http/JSON SDKs are available for application integration partners.	APIs are defined by the SOC vendor	Not applicable	XML, HTML, JAVA, C and other	set of APIs that allow support of the MVPD HTML5 application	C/C++ APIs on the client side; SOAP and HTTPS server interfaces.
3.b. Hardware									

Survey Question	AltiCast	ARRIS	Broadcom	Cisco	DTA Security	Intel	Nagra	OMS	Verimatrix
3.b.i. What is required on the physical platform (e.g. secure key bundle at manufacturing, Trusted Execution Environment, one-time programmable memory, cryptographic functions in hardware)?	dependent on target security requirements	No specific hardware or CPU architecture required	10 Specific HW features	The Key Ladder in the SoC forms the core of the content security system in the set-top box.	The SOC must support specified key ladders.	Intel processor with SGX support.	All listed are preferred by Nagra and typically mandated by most content owners for high value content. Also Secure Key Ladder	OMS requires the implementation of a SoC with a secure processor that conforms to robustness rules defined by OMS	Personalized SOCs (including 3 rd party Trust Authority), certified TEE, code/app signature verification, etc. (Depends on device type)
3.b.ii. Process description of how devices, SoCs, and CAS gain access to secure key elements	Access to secure elements is provided through low-level APIs.	implemented on a case by case basis, hw support where available	1) Non-Modifiable OTP key/IDs 2) Root Key Derivation 3) Content key derivation /Key	Leverages the standard OMS ecosystem for acquisition of all secure key elements.	Robustness rules and compliance requirements are specified in CAL and Cisco licensing materials.	See intel presentation	Via secure key ladder	OMS allows for a Trust Authority to create keys	Verimatrix-provisioned/personalized SOCs using Verimatrix or 3 rd party TA blackbox; or access to TEE keys.

Survey Question	AltiCast	ARRIS	Broadcom	Cisco	DTA Security	Intel	Nagra	OMS	Verimatrix
			ladder						
3.b.iii. Is there a specific CPU or CPU architecture required? If so, which one(s)?	No	No	No, should be left up to the SOC designers	DRM system works across a wide range of CPUs include x86 and ARM.	No specific CPU or CPU architecture is required.	Intel Architecture re.	MANY, DEPENDS ON DEVICE, The more secure the better but can be made to work at some level of security on most	No specific CPU or SoC architecture is defined by OMS	No specialized CPUs are required

Survey Question	AltiCast	ARRIS	Broadcom	Cisco	DTA Security	Intel	Nagra	OMS	Verimatrix
3.b.iv. What happens if some physical elements are not present?	A subset of services can be provided depending on robustness of device.	Dependent on content license	It will depend on the content protection policy	Designed in a modular fashion to support and where necessary to compensate for varying degrees of physical hardware security.	They may not receive certain content if they do not have certain capabilities.	Trusted Execution Environment using SGX is not possible.	Can be Emulated in SW, BUT may have significant reduction in security guarantees and may require waivers from content owners	The full security chain is required for use of OMS solutions	Some critical security features must always be present. Different levels of protection available depending on content type (e.g. HD vs. UHD).
3.b.v. How are robustness rules and compliance rules on hardware defined? Who defines them? What are these rules? How are they enforced?	dependent on service and content provider requirements	Robustness rules are defined in the content license.	defined by security architects, like CA/DRM vendors	Cisco security experts are responsible for identifying threat criteria and dynamically updating	The SOC and DTA device go through a validation process to ensure they comply with the license and robustness	SGX is a technology that ISVs use to meet various robustness rules. With respect to SGX itself, Intel defines	Very Stringent Defined by Nagra in conjunction with content owners Enforced by Nagra and third party	OMS defines the Robustness and Compliance rules	Compliance and Robustness Rules are published by Verimatrix in collaboration with content owners

Survey Question	AltiCast	ARRIS	Broadcom	Cisco	DTA Security	Intel	Nagra	OMS	Verimatrix
3.b.vi. Are there any execution environment restrictions (e.g., any other applications must be tested and/or signed by the security solution or operator).	Execution environment must meet robustness requirements.	Robustness rules are defined in the content license.	all SW/FW should be verified. All platform and 3 rd party code should be HW isolated from critical security code, and	Downloadable CA should be signed by Cisco or operator	This is covered under the CAL and Cisco licensing materials.	There are some memory usage limitations in the current version of SGX.	Yes, Code run in TEE or secure processor is fully vetted. Depending on processor architecture other processes may need to be	OMS requires the validation of the CAS Client APIs as well as the Application APIs.	Dependent on client device type, a certified TEE is desirable.
				Cisco's own internal robustness and compliance criteria for hardware, software, networks, and operating environments.	Rules for keeping secrets. They are enforced through bilateral contracts.	audit			

Survey Question	AltiCast	ARRIS	Broadcom	Cisco	DTA Security	Intel	Nagra	OMS	Verimatrix
3.b.vii. Are independent third-party applications supported, that don't require verifications/certification from the CAS supplier?	Yes	Platform specific.	not rely on SW isolation mechanisms	The entity that controls or manages a device is responsible for certification of third-party applications should be required based on fully isolated hardware	Independent, third-party applications are not supported.	YES	Depends on processor architecture and partitioning	The full security chain is required for use of OMS solutions	Applications must abide by integration compliance and robustness rules or must be completely sandboxed away from CA/DRM.

Survey Question	AltiCast	ARRIS	Broadcom	Cisco	DTA Security	Intel	Nagra	OMS	Verimatrix
3.b.viii. Are there third party, independent lab testing and certification options?	No	Yes	Yes	Technology is periodically subject to third-party audits and evaluation, as requested or required by commercial agreement.	DTA SOCs and DTAs are validated by Arris/CCAD and Cisco/Itaas	Not applicable.	Yes	OMS validates solutions.	Yes, e.g. Riscure for SOCs and TEE certification by GlobalPlatform or approved test labs.
3.c. Device identification and Keying									
3.c.i. Secure mechanisms for identification of devices in the network.	Yes	Platform dependent	This is a MUST for anti-cloning.	Utilizes a common secure channel for identification of all VideoGuard clients	The DTA's network identity is created at time of SOC manufacture as part of the	SGX uses provisioning and attestation (see presentation) to verify genuine	Yes Essential	The OMS defined Root of Trust is a key residing on the SoC, and is	Immutable SOC IDs; MAC addresses, device ID, HW fingerprint, and unique device

Survey Question	AltiCast	ARRIS	Broadcom	Cisco	DTA Security	Intel	Nagra	OMS	Verimatrix
				on the network	keying process	Intel processor and SGX enclave.		accessible by the KLAD key ladder.	certificates .
3.c.ii. Serial number/unique identification requirements	Yes	not required, but may be used if present	Non-Modifiable OTP IDs can be readable by host ACPU	There are no specific identification requirements dictated by VideoGuard	Serial number is added at device manufacture time.	Requires genuine Intel processor with SGX technology. These properties are remotely attestable .	Yes	OMS defines the specification for serialization and keying of SoCs.	Unique SOC IDs, typically programmed during the SOC personalization process, or unique device ID (and optionally keys) accessible in TEE.

Survey Question	AltiCast	ARRIS	Broadcom	Cisco	DTA Security	Intel	Nagra	OMS	Verimatrix
3.c.iii. Keys, key storage capabilities	Yes	WBC or secure storage or simply encrypted storage if secure environment	Non-Modifiable OTP keys cannot be readable by host ACPU.	Downloadable clients work with device OS to ensure reliable access to persistent memory	APIs are provided by the SOC vendor	SGX can securely store an Application's keys by cryptographically sealing them to the processor.	Yes Essential	OMS defines OTP keys to use with the KLAD mechanism	Asymmetric verification keys (secure boot); Device unique symmetric OTP keys
3.c.iv. Is there a standardized mechanism for communication with SoC and other hardware elements?	Yes	No	We are not aware of any standardized scheme.	ETSI, SCTE and OMS all provide standards		SGX uses provisioning and attestation to enable ISV application to set up trusted execution environment.	No Only frameworks	OMS defines a CAS Client API	Verimatrix-defined HW Key Ladder abstraction layer implemented by many SOC vendors; or OMS/KLAD APIs.
3.d. Key server/client communication path and network									

Survey Question	AltiCast	ARRIS	Broadcom	Cisco	DTA Security	Intel	Nagra	OMS	Verimatrix
3.d.i. Is a two-way communication path required? Does it need to be full-time connectivity?	Two-way comm path required, but full-time connectivity not mandatory	Intermittent 2 way connectivity required	Certain STB features may require bi-directional communication	Provides multiple solutions for one-way and two-way environments	The DTA is a one-way device per FCC requirements	Setting up a trusted execution environment using SGX requires provisioning and attestation, which can be performed one time using bi-directional communication with a server via the Internet.	No, Helps security of present	OMS requires two-way connectivity at any time that a digital device is attached to the network	No, adapted to network type (1-way or 2-way)

Survey Question	AltiCast	ARRIS	Broadcom	Cisco	DTA Security	Intel	Nagra	OMS	Verimatrix
3.d.ii. Must it be a secure channel or is an open insecure channel supported (e.g., by encryption that is part of the system)? Does the channel use IP or proprietary protocols? DSG or other network specific technologies?	Secure channel is needed and is used on IP or proprietary network protocols.	ESAM protocol is application level protocol	Require secure channel to perform authentication and key exchange, defined by CAS/DRM vendor	Operates within completely managed as well as completely unmanaged networks	in-band proprietary messaging	This is up to the ISV application. SGX provisioning and attestation requires an internet connection set up.	The channel runs over a potentially open network using well known IP and RF protocols. Where necessary the messaging is secured	Defined by CAS provider	VCAS provides its own secure key management protocol based on standards such as TLS and X.509.
4. Technical Capabilities									
4.a. What media transport formats supported (e.g., MPEG-2 Transport Streams, ABR/HLS, ISO BMFF)?	All	MPEG2-TS for IPTV, HLS for OTT, mp4 offline playback, ISO-BMFF being added	can support a lot of container formats and codecs	MPEG-2 Streams, ABR/HLS, HSS and MPEG DASH	MPEG-2 and MPEG-4	SGX is format agnostic. Intel graphics support a wide range of media formats.	All	OMS is agnostic to the transport stream	All; VCAS is as video encoding and file/transport format independent

Survey Question	AltiCast	ARRIS	Broadcom	Cisco	DTA Security	Intel	Nagra	OMS	Verimatrix
4.b. What content delivery networks are supported (e.g., HFC QAM, DBS, IP unicast, IP multicast)?	1-way & 2-way	All two way networks.	Different BRCCM STB chipsets can support satellite, cable and IP markets.	HFC QAM, DBS, IP unicast, IP multicast	Only HFC is supported.	Network agnostic.	ALL Plus Terrestrial Broadcast ATSC M/H, DVB-H, DMB etc	OMS can support any two way network	All are supported.
4.c. Is Network information conveyed and required (e.g. DVB-SI, SCTE 65, etc.)?	Yes	Not for decrypt	STB chipsets can filter different network information	Network and System information are not conveyed or required	SCTE-65 on the in-band channel	Not required. Depends on specific ISV application.	DVB-SI and SCTE 65 helpful on broadcast networks. Not needed for DRM use cases	Yes	Yes, a minimal subset of SI information is required for use by VCAS
4.d. What encryption standards used (e.g., which ciphers, and is there support for legacy deployed systems such as DVB-CA, SCTE	A range of ciphers and key lengths are supported	System dependent	DVB-CA, DVB-CSA2, DVB-CSA3, AES, 3DES and DES	including, but not limited to: DVB-CSA2, AES-CBC, DVB-CSA3, DVB-CPCM,	DES-CBC as defined in SCTE-52 or proprietary DES-CTS or DVB-CSA	SGX is not an encryption technology. Can support whatever the ISV application	All, Relatively agnostic - encryption and decryption typically done by secure processor	OMS can be deployed on CSA and SCTE-52 networks	All can be used; typically AES128 is used, however, specific content encryption is not

Survey Question	Alticast	ARRIS	Broadcom	Cisco	DTA Security	Intel	Nagra	OMS	Verimatrix
55, etc.)?				ATIS-ISSA, ARIB, SCTE-55 and MPEG CENC		in supports.	in CAS and some DRM deployments		required by VCAS
4.e. What are the application APIs to the CAS/DRM client? (e.g., what are the API interfaces between the device software and the CAS/DRM software for requesting content decryption, and querying entitlements defining the associated content such as DVR recording, home streaming, and	Basic APIs for requesting content decryption and querying entitlements	API's vary by system	ECM/EMM or DRM license filtering/parsing	Open APIs for querying viewer rights and activation content decryption	The APIs to the CA client are supplied by the SOC vendor.	These are determined by the application.	Many	OMS APIs define the interfaces used by the CAS client	Verimatrix publishes a CAS/DRM client API for 3rd party middleware/application/player integrations.

Survey Question	AltiCast	ARRIS	Broadcom	Cisco	DTA Security	Intel	Nagra	OMS	Verimatrix
for how long or how many copies.)									
4.f. Network identification, access and attachment requirements APIs?	Authentication APIs are supported.	no dependence on network identification	Depend on each security partners.	Network attachment APIs are defined by the MVPD	Host requirements are via SOC-defined APIs	These are determined by the application.	-	OMS defines these	Provisioning APIs are provided by the CAS client.
5. Standards Used in the System									

Survey Question	AltiCast	ARRIS	Broadcom	Cisco	DTA Security	Intel	Nagra	OMS	Verimatrix
5.a. What standards (i.e., non-proprietary technical standards promulgated by government or private standards defining organizations) are used in the system?	JCAS, NCAS, XCAS/iCAS, and others	Pantos/AES for OTT, MPEG2-TS AES/CSA, TLS, RSA, SCTE-52	DTCP-IP, HDCP1.4, HDCP2.2, MPEG CAS, etc.	DVB SimulCrypt, DVB CSA and CPCM encryption ciphers, ATIS encryption ciphers, ETSI and SCTE OMS key ladder	<ul style="list-style-type: none"> • ATSC A/53, MPEG-2 and MPEG-4: Video Transport • SCTE-65: Network Information • SCTE-18: Emergency Alert Messages • SCTE-20, CEA-608 and CEA-708: Closed Captioning • OpenCable Common Download Specification: 	SGX is an Intel proprietary technology.	SCTE, DVB, ETSI, MPEG, ATSC, DLNA, AES	SCTE-52, DVB Simulcrypt, DVB CSA, KLAD (ETSI and SCTE 201)	MPEG, DVB, SCTE, ETSI, OIPF, EITF, W3C, DLNA, OMS, GlobalPlatform, DASH-IF, etc.

Survey Question	AltiCast	ARRIS	Broadcom	Cisco	DTA Security	Intel	Nagra	OMS	Verimatrix
5.b. Describe plans (if any) related to how the security system works with W3C	AltiCast HTML5 Browser supports EME.	Active program underway	Different DRM technologies with EME	Working with a number of browser vendors to	There are no current plans to use DTA with W3C EME	SGX can support any application, including	In Development	No	W3C EME is supported where applicable.

Survey Question	AltiCast	ARRIS	Broadcom	Cisco	DTA Security	Intel	Nagra	OMS	Verimatrix
Encrypted Media Extensions (EME).				implement the VG Everywhere CDM (Content Decryption Module) in support of EME	those with EME.				
6. Deployment Model									
6.a. Does the solution require the operator to deploy a new transmission network or leverage existing ones?	Leverage existing.	Use existing.	N/A	Should not require the deployment of new transmission networks	Existing HFC Networks	Up to the operator/SV. Can leverage existing ones.	EITHER	OMS is designed to work with legacy cable deployments that have been enhanced to support DVB Simulcrypt	Existing networks supported.

Survey Question	Verimatrix	OMS	Nagra	Intel	DTA Security	Cisco	Broadcom	ARRIS	AltiCast
6.b. What are the largest cost elements for an operator to deploy (new equipment, upgrades, network changes, swap out older equipment)	Highly operator dependent, however, Verimatrix strives to provide standards-based solutions to minimize such costs.	replacement or upgrade of all encryption devices, conversion to DOCSIS out-of-band, new CAS system and CAS controller, integration with legacy CAS Controller s, and integration with Billing	Deploying a new security system. This assumes existing STB 's can be re-used or continue to co-exist		The operator will have to modify or install new systems	Cost of operating the new security solution alongside the legacy ones	N/A	No special hardware necessary	Highly operator-dependent.
6.c. Co-existence with legacy CAS systems, or modification required, or	Simulcrypt with legacy CAS systems is supported. Simulcast	The OMS system can exist with legacy CAS Systems.	Either, Have deployed simulcast and simulcrypt	Can be whatever the ISV wants its application to be.	coexist with both the ARRIS and Cisco	SimulCrypt and Simulcast modes, Sony Passage	N/A	SimulCrypt	Completely independent, coexists with

Survey Question	AltiCast	ARRIS	Broadcom	Cisco	DTA Security	Intel	Nagra	OMS	Verimatrix
completely independent (simulcast) solution?	Legacy CAS (Simulcrypt)			(partial encryption modes), MultiCrypt modes					is also an option.
7. Intellectual property and licensing regime									
7.a. What elements of the system are currently licensed/licensable on Fair, Reasonable and Non-Discriminatory (FRAND) terms?	Proprietary license.	FRAND to service providers	N/A	Where IP Hooks are recommended for security reasons, such as use of DVB-CSA, intellectual property licenses are generally available from third-parties on FRAND terms.	negotiated between the licensors - CAL and Cisco -- and their licensees.	Intel will license SGX technology on FRAND terms.	All with exception of proprietary recovery logic used against persistent attack modes	Under development	Both server-side and client-side components are licensed to operators and device manufacturers.

Survey Question	AltiCast	ARRIS	Broadcom	Cisco	DTA Security	Intel	Nagra	OMS	Verimatrix
7.b. What elements (if any) of the system are not currently licensed/licensable under FRAND terms?	None.	Not licensing IP separately	N/A		N/A	SGX is an Intel microprocessor feature and is not licensed for implementation on non-Intel processors.	Recovery Logic included in Nagra NOCS3 key Ladder implementations		Specific elements that should be kept proprietary to diversify security.
7.b.i. Are there any elements that will never be licensed under FRAND terms?	Yes	Not licensing IP separately	N/A	Licensable to Cisco's MVPD customers as Cisco product licenses	N/A	Licensing is limited to applications for Intel processors.		Under development	Certain elements should remain proprietary to diversify security.
8. Porting Issues & Liability									

Survey Question	AltiCast	ARRIS	Broadcom	Cisco	DTA Security	Intel	Nagra	OMS	Verimatrix
8.a. Who does the port?	AltiCast.	ARRIS SecureMedia	Either security partner, OEM or Middleware vendor.	Cisco provides support for all ports of the VideoGuard Everywhere clients	The SOC vendor	ISVs license SGX and build their own SGX applications.	Varies Mostly Nagra	device manufacturer	Verimatrix and SOC vendors or 3 rd party integration labs.
8.b. How's the port validated?	Trusted Authority.	tested with over 150 different device and OS combinations	May require some forms of certification to validate the end-to-end system.	Cisco provides device and application certification services as dictated by MVPD commercial requirements.	CCAD and Cisco validate SOC requirements, then CCAD and Itaas validate DTA requirements.	Intel uses provisioning and attestation to validate creation of an SGX trusted execution environment.	By Nagra	OMS will define validation procedures	Verimatrix.

Survey Question	AltiCast	ARRIS	Broadcom	Cisco	DTA Security	Intel	Nagra	OMS	Verimatrix
8.c. Who provides indemnification for the ported implementation ?	Dependent on commercial contract terms.	Depends on business arrangement	Whoever is acting as an insurance company in the ecosystem .	Indemnification is a term that is governed by commercial agreement between entities	Indemnification terms are negotiated.	Intel does not indemnify ISVs for use of SGX.	Nagra to MVPD	business agreement between the CAS and Device vendors.	Indemnification is typically negotiated between operators and vendors

Table 24 - Summary of Survey Responses