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

[Summary of STAC Report Scope goes here]

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 Description*s, 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 Description*s, 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 defining “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 downloaded and installed onto a navigation device to securely receive the services offered by the media provider. 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]

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.

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] http://csrc.nist.gov/projects/root-trust/

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.[2]
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.
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:

[2] 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.

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.)

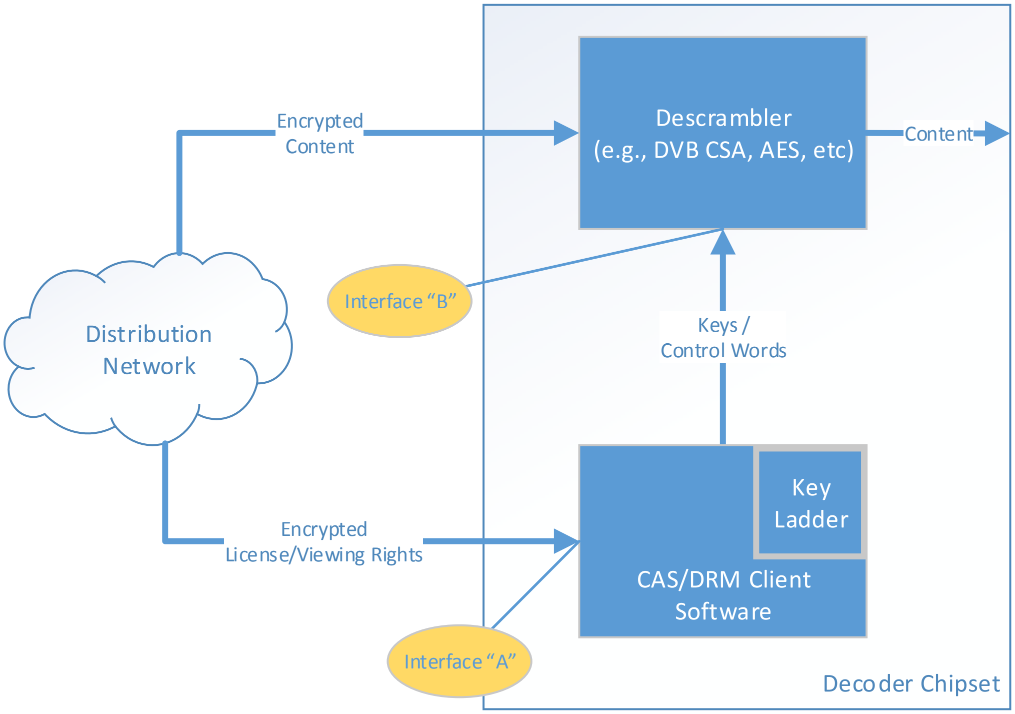
A DSS must support the ability to download sufficient code and data to renew the security system – to download different keys, certificates, code, configuration parameters, etc., such that the renewed system is secure.

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.



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) Interfaces Standards

[a mere stab at this – pending finalization of (b) above]

The secured software execution environment/platform (such that a CA vendor can implement the CA Client to run in it)

The secure download/secure boot process such that a CA Client can be downloaded, installed, verified, and booted.

The communications between the CA Client and the non-secured-environment.

[likely others]

d) 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.

e) 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.

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, revel 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.

f) (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 adjunct IP connectivity 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 must 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.

g) 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.

h) 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.

An example of how device and system testing processes work today is described in Section VIII.

i) 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 [Example MVPD Trust Infrastructure March 27, 2015 (part of WG2 process)].

j) 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 and meet the required testing for each MVPD.

k) 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.

To accomplish this, the Device and DSS must support recovery of outstanding purchase information, e.g. Pay-Per-View events from the device upon termination of service, as well as clearing any remaining entitlements to the service from the device.

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

[brainstormed list:

the system should be fast enough to support the requirements (above, elsewhere) in a way that works good, fast enough, cheap enough, for generally acceptable consumer usage

the system should be designed so that it is commercially viable for >10 years

the system should support content data rates of at least [N mbps]

Suggested by email (from WG2 requirements)
S13: Scalability: The system must scale such that there should be no limits on addressing many tens of millions of devices in a timely manner without undue latency in authorizing or de-authorizing a device.

S14: Latency: The performance of the system must be fast enough to avoid adding to customer support issues and maintain subscriber satisfaction. A goal may be for instant or near instant authorization which greatly helps in customer satisfaction, acquisition, retention, self-provisioning etc. (Instant gratification makes for happy customers).

S15: Addressability: The system must be able to efficiently address all combinations of individually channel line ups, at the required Scale, and with the required Latency (these are often technically conflicting challenges)

]

a) What are the performance objectives on the system components and interfaces?

The CAS and DRM system have to be designed to support better scaling (i.e. avoid exponential scaling tendencies). The interfaces must support ______

b) (if you don’t assume IP connectivity): Bandwidth and Complexity

c) (if you don’t assume IP connectivity): System throughput for control messages

How long will this last? How will it evolve? (Survivability, longevity)

4. Technical Standards

a) 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		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 (ATTM); 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

b) Networking and Communication Standards

Standards relating to communication and transmission to and inside homes.

_802.11	Wireless LANS 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		?
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/
DVB-S, DVB-S2	Satellite broadcasting standard	https://www.dvb.org/standards/dvb-s2
Ethernet		802.3
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
UHD Alliance	documents (available in a few months hopefully)	tbd

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/

c) 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	
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 13818-1:2013	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=62074
MPEG-1,2, DASH, TS	MPEG Specifications	http://mpeg.chiariglione.org/standards
HTTP Live Streaming		https://tools.ietf.org/html/draft-pantos-http-live-streaming-13 (IETF Draft)

Microsoft		https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=4&ved=0CDgQFjADahUKEwjWn_HM-oXGAhWLEqwKHUiiAHU&url=http%3A%2F%2Fdownload.microsoft.com%2Fdownload%2F9%2F5%2FE%2F95EF66AF-9026-4BB0-A41D- A4F81802D92C%2F%5BMS-DLNHND%5D.pdf&ei=_5x4VZakKYulsAXIxIKoBw&usg=AFQjCNFQmVMjUDmTtPH3PJFZ3caSYq0r_A&sig2=CQzvwduuEnF9vMSFjaQVTw (Microsoft)

d) Service Standards

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

RRT	U.S. Region Rating Table (RRT)	CEA-766-B
ATSC A/72	Closed Captioning	http://atsc.org/standard/a72-parts-1-2-and-3/
CALM act	for audio levels	
CEA-608-E	Line 21 Data Services	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
CEA-766	Extended Data Services	https://www.ce.org/Standards/Standard-Listings/R4-3-Television-Data-Systems-Subcommittee/CEA-766-C-%28ANSI%29.aspx
EME	Encrypted Media Extensions	https://w3c.github.io/encrypted-media/
PSIP	ATSC A/65 Program and System Information Protocol (PSIP)	Atsc.org

e) 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

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 from MVPD
- Retail Whole Home DVR Ecosystem (e.g. TiVo)
- 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 is in Table 1 at the end of this section and the following section summarizes 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 technology mandates, either in hardware or software, as such mandates effectively halt innovation.
- 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

Survey Question	AltiCast	ARRIS	Broadcom	Cisco	DTA Security	Nagra	OMS	Verimatrix
1. Name of the solution and brief overview	AltiProtect	Encryptonite	Broadcom	VideoGuard™	DTA Security	NAGRA anyCAS	Open Media Security	VCAS
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 Many as prescribed by the marketing departments of all the worlds MVPS	Yes	Yes
2.a.ii. Does it provide DRM services (e.g. this content can be viewed for 90 days)?	Yes	Yes	Yes	Yes	No	YES Many as prescribed by the marketing departments of all the worlds MVPS	currently being developed in labs.	Yes

Survey Question	AltiCast	ARRIS	Broadcom	Cisco	DTA Security	Nagra	OMS	Verimatrix
2.a.iii. Does it provide link protection across digital interfaces between separate devices?	Yes	Yes	Yes	Yes	Passes CCI	YES, DRM, PRM, DTCP-IP and others	as defined by the MPVD's content and technology license	Yes
2.a.iv. Does it provide watermarking or fingerprinting, device and user authentication, or system renewability?	Yes	thrid party watermarking systems	HW or Firmware Based	Finger printing supported, work with 3rd-party watermarking	Device Auth & System Renewability - Yes, all others No	Watermarking is implemented mainly using outsourced technology however standards are not agreed and no one wants to pay. Yes to rest (they are not related or part of a CAS or DRM?)	no specific watermarking or fingerprinting	Yes
2.b. Network support:								

Survey Question	AltiCast	ARRIS	Broadcom	Cisco	DTA Security	Nagra	OMS	Verimatrix
2.b.i. What kinds of networks (DBS, HFC, FTTH) are supported?	1-way & 2-way	2-way	All types	all major MVPD delivery networks	1-way HFC only	ALL PLUS terrestrial ATSC M/H, DVB-H, DMB….	2-way	IPTV, FTTH, HFC/QAM, DVB-S, DVB-C, DVB-T, unmanaged IP (OTT).
2.c. Services and Device Functions:								
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	YES AND MANY MORE USE CASES	All	based on 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	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	YES TO ALL and Many more such as place shifting, download to go or sideloading ,	All	All types

Survey Question	AltiCast	ARRIS	Broadcom	Cisco	DTA Security	Nagra	OMS	Verimatrix
streaming of content)?						transcoding, expiration enforcement, Enforcement of number of streams or copies…		
2.d. Device support:								
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,	Various DTAs only	ALL DEVICES ,STB SMARTPHONE, TABLET PC , MAC, CONNECTED TV	OMS defines SoC and keying requirements	both operator-managed devices and consumer devices

Survey Question	AltiCast	ARRIS	Broadcom	Cisco	DTA Security	Nagra	OMS	Verimatrix
				PS3/4 and Xbox One				
2.e. Application support:								
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,	APIs to verify authorization and enable purchases	API's vary by system	support various APIs	APIs (e.g., authentication and authorization status) are available for integration of VG Everywhere with TV Applications	No APIs are presented from the system	YES TO ALL	OMS defines APIs that are required to deliver the service provider's service	CAS and DRM clients are downloadable in different forms

Survey Question	AltiCast	ARRIS	Broadcom	Cisco	DTA Security	Nagra	OMS	Verimatrix
copy control information?								
3. Components of the solution								
3.a. Software								
3.a.i. What parts of the solution are downloadable as software?	CAS and DRM client modules	Depends on platform	All other than first stage bootloader and loader	supports fully downloadable security solutions where both DRM and CA components are implemented as downloadable software	The conditional access client is downloaded as software	MUCH OF IT	software environment, HTML5 applications, and a CAS client	

Survey Question	AltiCast	ARRIS	Broadcom	Cisco	DTA Security	Nagra	OMS	Verimatrix
3.a.ii. What is the secure software execution environment (execution environment framework, OS, etc.)	a variety of Trusted Execution Environments	Work with whatever is available	a separate, self-contained, security processor is required to meet all the security requirements and robustness rules	iOS (5.1 and above), Android (4.X and above), Windows 8 RT, Windows XP SP3 and above (XP SP3 / 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.	secure portion of the SOC	VARIOUS DEPENDS ON DEVICE AND SOC	OMS does not define a full software environment	TrustZone/ TEE or dedicated security processors

Survey Question	AltiCast	ARRIS	Broadcom	Cisco	DTA Security	Nagra	OMS	Verimatrix
3.a.iii. How is code verified, updated? Structure of signing keys and of download images	using Application upgrade protocol	ESAM3 protocol	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 security	authenticated according to CAL and Cisco licensing materials	??	OMS defines the OTP hardware root of trust	SW is signed (and encrypted) and verified during secure boot process
3.a.iv. Software Roll back support? Roll back management	Yes	Yes	Security processor is used	Software download and rollback infrastructure are dictated by the specific application download environment	Yes	YES	Not currently	Yes
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 specification/tools	SDKs are available for application integration partners.	APIs are defined by the SOC vendor	HTML, JAVASCRIPT OTHER	set of APIs that allow support of the MVPD HTML5 application	C/C++ APIs on the client side; SOAP and HTTPS

Survey Question	AltiCast	ARRIS	Broadcom	Cisco	DTA Security	Nagra	OMS	Verimatrix
								server interfaces.
3.b. Hardware								
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.	ALL ARE PREFERRED	OMS requires the implementation of a SoC with a secure processer that conforms to robustness rules defined by OMS	Depends on device type

Survey Question	AltiCast	ARRIS	Broadcom	Cisco	DTA Security	Nagra	OMS	Verimatrix
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	1) Non-Modifiable OTP key/IDs 2) Root Key Derivation 3) Content key derivation/ Key ladder	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.	????	OMS allows for a Trust Authority to create keys	Verimatrix-provisioned /personalized SOCs using Verimatrix blackbox
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.	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
3.b.iv. What happens if some physical elements are not present?	A subset of services can be provided depending on	Dependent on content license	It will depend on the content protection policy	designed in a modular fashion to support and where necessary to	They may not receive certain content if they do not have certain	CAN BE EMULATED IN SECURE SW WITH SOME SECURITY CAVEATS	The full security chain is required for use of OMS solutions	Some critical security features must always be present

Survey Question	AltiCast	ARRIS	Broadcom	Cisco	DTA Security	Nagra	OMS	Verimatrix
	robustness of device.			compensate for varying degrees of physical hardware security.	capabilities.			
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 operational security (OpSec) are responsible for identifying threat criteria and dynamically updating Cisco's own internal robustness and compliance criteria for hardware, software, networks, and operating	The SOC and DTA device go through a validation process to ensure they comply with the license and robustness rules.	VERY STRINGENT. DEFINED BY NAGRA. RULES PRESCRIBE MEASURES TO BE TAKEN TO AVOID KNOWN AND LIKELY FUTURE ATTACK METHODS. Advice and input is also taken from studios and content owners.	OMS defines the Robustness and Compliance rules	Compliance and Robustness Rules are published by Verimatrix

Survey Question	AltiCast	ARRIS	Broadcom	Cisco	DTA Security	Nagra	OMS	Verimatrix
				environments.		AUDITED BY NAGRA AND BY THIRD PARTIES		
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 requirement.	Robustness rules are defined in the content license.	all SW/FW should be verified	Threats to security are not completely under the control of a downloadable security client and are dynamic.	This is covered under the CAL and Cisco licensing materials.	YES IF IN SAME PROCESSOR SPACE AS SECURITY CODE	OMS requires the validation of the CAS Client APIs as well as the Application APIs.	depends on the type of device

Survey Question	AltiCast	ARRIS	Broadcom	Cisco	DTA Security	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.	a secure scheme that can separate the trusted applications from the non-trusted applications should be required	The entity that controls or manages a device is responsible for certification of third-party applications downloaded to a device.	Independent, third-party applications are not supported.	DEPENDS ON PROCESSOR PARTITIONING AND SPECIFICATION	The full security chain is required for use of OMS solutions	Applications must abide by integration compliance and robustness rules.
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 evaluations, as requested or required by commercial agreement.	DTA SOCs and DTAs are validated by Arris/CCAD and Cisco/Itaas	YES	OMS validates solutions.	Yes, e.g. Riscure for SOCs. TEE certification by GlobalPlatform approved test labs, etc.

Survey Question	AltiCast	ARRIS	Broadcom	Cisco	DTA Security	Nagra	OMS	Verimatrix
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 on the network	The DTA's network identity is created at time of SOC manufacture as part of the keying process	YES	The OMS defined Root of Trust is a key residing on the SoC, and is accessible by the KLAD key ladder.	Immutable SOC IDs; MAC addresses and unique device certificates.
3.c.ii. Serial number/unique identification requirements	Yes	not required	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.	YES	OMS defines the specification for serialization and keying of SoCs.	Unique SOC IDs, typically programmed in OTP during the SOC personalization process.

Survey Question	AltiCast	ARRIS	Broadcom	Cisco	DTA Security	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	YES	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		??	OMS defines a CAS Client API	Verimatrix-defined HW Key Ladder abstraction layer implemented by many SOC vendors
3.d. Key server/client communication path and network								

Survey Question	AltiCast	ARRIS	Broadcom	Cisco	DTA Security	Nagra	OMS	Verimatrix
3.d.i. Is a two-way communication path required? Does it need to be full-time connectivity?	Execution environment must meet robustness requirement.	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	NO BUT HELPS SECURITY	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)
3.d.ii. Must it be a secure channel or is an open unsecure 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	operates within completely managed as well as completely unmanaged networks	in-band proprietary messaging	OPEN	Defined by CAS provider	VCAS provides its own secure key management protocol
4. Technical Capabilities								

Survey Question	AltiCast	ARRIS	Broadcom	Cisco	DTA Security	Nagra	OMS	Verimatrix
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 Transport Streams, ABR/HLS, HSS and MPEG DASH	MPEG-2 and MPEG-4	ALL	OMS is agnostic to the transport stream	VCAS is as video encoding and file/transport format independent
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 BRCM STB chipsets can support satellite, cable and IP markets.	HFC QAM, DBS, IP unicast, IP multicast	Only HFC is supported.	ALL Plus Terrestrial Broadcast ATSC M/H, DVB-H, DMB	OMS can support any two way network	All of the above 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	ALL AND MORE	Yes	Minimal subset of SI information is required

Survey Question	AltiCast	ARRIS	Broadcom	Cisco	DTA Security	Nagra	OMS	Verimatrix
4.d. What encryption standards used (e.g., which ciphers, and is there support for legacy deployed systems such as DVB-CA, SCTE 55, etc.)?	A range of ciphers and key lengths are supported	System dependent	DVB- CSA2, DVB-CSA3, AES, 3DES and DES	including, but not limited to: DVB-CSA2, AES-CBC, DVB-CSA3, DVB-CPCM, ATIS-ISSA, ARIB, SCTE-55 and MPEG CENC	DES-CBC as defined in SCTE-52 or proprietary DES-CTS or DVB-CSA	ALL WE ARE AGNOSTIC AND DON'T FO THE ENCRYPTION, WE DO THE KEY EXCHSNGE AND RIGHTS MANAGEMENT, ALSO AES	OMS can be deployed on CSA and SCTE-52 networks	Specific content encryption is not 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	Basic APIs for requesting content decryption and querying entitlements	API's vary by system	ECM/EMM or DRM license filtering/parsing	MVPD is responsible for synchronizing user experience and content security services	The APIs to the CA client are supplied by the SOC vendor.	????	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	Nagra	OMS	Verimatrix
entitlements defining the associated content such as DVR recording, home streaming, and 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	???	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	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, and XCAS/iCAS	Pantos/AES for OTT, MPEG2-TS AES/CSA, TLS, RSA, SCTE-52	DTCP-IP, HDCP1.4, HDCP2.2, MPEG CAS	DVB SimulCrypt, DVB CSA and CPCM encryption ciphers, ATIS encryption ciphers, ETSI and SCTE OMS key ladder	• 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: firmware download	SCTE, DVB, ETSI, MPEG,	SCTE-52, DVB Simulcrypt, DVB CSA, KLAD (ETSI and SCTE 201)	MPEG, DVB, SCTE, ETSI, OIPF, EITF, W3C, DLNA, etc.

Survey Question	AltiCast	ARRIS	Broadcom	Cisco	DTA Security	Nagra	OMS	Verimatrix
5.b. Describe plans (if any) related to how the security system works with W3C Encrypted Media Extensions (EME).	Alticast HTML5 Browser supports EME.	Active program underway	PlayReady 2.5 and Widevine	working with a number of browser vendors to implement the VG Everywhere CDM (Content Decryption Module) in support of EME	There are no current plans to use DTA with W3C EME	PLANNED	No	W3C EME is supported where applicable.
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	EITHER	OMS is designed to work with legacy cable deployments that have been enhanced to support DVB Simulcrypt	Existing networks supported.

Survey Question	AltiCast	ARRIS	Broadcom	Cisco	DTA Security	Nagra	OMS	Verimatrix
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.	No special hardware necessary	N/A	cost of operating the new security solution alongside the legacy ones	The operator will have to modify or install new systems	???? SWAPING STB?	replacement or upgrade of all encryption devices, conversion to DOCSIS out-of-band, new CAS system and CAS controller, integration with legacy CAS Controllers, and integration with Billing	Verimatrix strives to provide standards-based solutions
6.c. Co-existence with legacy CAS systems, or modification required, or completely independent (simulcast) solution?	Simulcrypt	SimulCrypt	N/A	SimulCrypt and Simulcast modes, Sony Passage (partial encryption modes),	coexist with both the ARRIS and Cisco	EITHER	The OMS system can exist with legacy CAS Systems.	Simulcrypt with legacy CAS systems is supported

Survey Question	AltiCast	ARRIS	Broadcom	Cisco	DTA Security	Nagra	OMS	Verimatrix
				MultiCrypt modes				
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.	ALL MINUS RECOVERY LOGIC	Under development	Both server-side and client-side components are licensed to operators and device manufacturers.
7.b. What elements (if any) of the system are	None.	Not licensing IP separately	N/A		N/A	RECOVERY LOGIC		

Survey Question	AltiCast	ARRIS	Broadcom	Cisco	DTA Security	Nagra	OMS	Verimatrix
not currently licensed/licensable under FRAND terms?								
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	RECOVERY LOGIC and Countermeasure logic	Under development	Certain components should remain proprietary for reasons of diversifying security solutions
8. Porting Issues & Liability								
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	VARIES, MOSTLY NAGRA	device manufacturer	Verimatrix and SOC vendors

Survey Question	AltiCast	ARRIS	Broadcom	Cisco	DTA Security	Nagra	OMS	Verimatrix
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.	NAGRA	OMS will define validation procedures	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.	NAGRA to MVPD	business agreement between the CAS and Device vendors.	Indemnification is typically negotiated between operators and vendors

Table 1 - Summary of Survey Responses

III. Download Security System Threat Models

A Threat Model is 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 process to hide their track via actions such as deletion or editing of transaction logs, and 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 is 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.

E. DBS Input (Free-form)

[Placeholder]

IV. Download Security Systems

A. Example 1

1. Additional Definitions
2. Additional Requirements
   - *a) Technical Capabilities*
   - *b) System Requirements*
   - *c) Performance Objectives*
   - *d) Technical Standards*
   - *e) Target Devices*
3. System Description
   - *a) Hardware components (if any)*
   - *b) Software components (modules, APIs)*
   - *c) Operational description (download, startup, update, etc.)*
4. Benefits/Costs

Example Items to be Include in (some) Alternative(s)

1. Common Hardware Definition
   - *a) Execution engine*
   - *b) Descrambling capabilities*
   - *c) Encryption/Decryption capabilities*
   - *d) Content cypher selection*
   - *e) Network communications capabilities*
     - (1) Note: may vary for, e.g., satellite networks
   - *f) Serial number/unique identification requirements*
   - *g) Keys, key storage capabilities*
   - *h) Other Nonvolatile storage requirements*
2. Secure Boot Loader Definition
   - *a) Authentication requirements*
   - *b) Trust requirements*
   - *c) Encryption requirements*
   - *d) Vulnerability to/recovering from complete system failure*
   - *e) Vulnerability to/recovering from boot loader compromise*
3. Secure Downloader [input from Robin coming]
   - a) *Secure Downloader Definition:*
     - (1) Vulnerability to/recovering from complete system failure
     - (2) Vulnerability to/recovering from downloader compromise
     - (3) Consideration of immutability of secure downloader
   - *b) Authentication and Trust requirements:*

(1) Structure of signing keys and of download images: how to make sure that device ingests the right image, how to make sure that operators' devices do not accept foreign images

c) Functionality / Use cases:

(1) Roll back? Roll back management

(2) By module or complete image

(3) Background or offline mode

4.

5. Software Environment Definition

a) Performance requirements

b) Network identification, access and attachment requirements

c) Hardware API requirements

d) MVPD UI requirements

e) Third party UI requirements

f) MVPD service access requirements

g) CAS client rules/definition

6. Trust Model/Keying

a) Security key and serialization definition

b) Black box requirements

c) Distribution process of keys to CAS vendors

d) Distribution process of keys to MVPDs

e) Remediation and revocation requirements

f) Watermarking

g) [need different words: Bad actor] identification and responses – who is responsible for management?

7. Compliance and Robustness Rules

a) Hardware Robustness

b) Compliance

c) Output Rules

8. Renewability Scenario

a) Process for revocation/renewal of devices

b) Replacement of system

B. Example 2

V. Red/Blue Analysis

A. <placeholder>

VI. Conclusions

VII. References

VIII. 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.