REPORT OF WORKING GROUP 1 TO DSTAC

"WG1 REPORT #1"

April 21, 2015

Introduction

Working Group 1 (WG1) was formed out of the larger DSTAC to address the topic of commercial requirements. This is in furtherance of the overall mission, 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 designed to promote the competitive availability of navigation devices in furtherance of section 629 of the Communications Act of 1934."

This report serves to represent a more formal summary of the activities of WG1 and also captures additional dialog and a few conclusions that have been reached by the group since the group issued its initial feedback in late March.

The first report from WG1 ("Talking points for WG1 Report v09") is included as Appendix 1, and thus this second report incorporates all read-outs from the team thus far.

To refresh, the group was chartered to identify the commercial requirements of content owners, multichannel video programming distributors (MVPDs), consumer electronics companies, system equipment manufacturers, and consumers. The group was to consider risks and threats, including, but not limited to: content piracy, brand protection, consumer privacy, device cloning, and device spoofing. The group split requirements into five primary areas: MVPDs; CE/device manufacturers; consumer; content providers; and security.

Since the initial "Talking points" summary was issued, the group has compiled a list of more specific requirements consisting of nearly 200 different line items. The list serves as a tool for working group participants to express their proposed requirements based on their areas of expertise and study. This list is based on current requirements and anticipated (future) requirements. However, this list is by no means comprehensive. That list is attached as Appendix 2.

The list continues to be subject to clarifications and additions. After the initial list was compiled, the group worked to identify major areas of alignment and non-alignment (conflicting language). Due to the volume of requirements in the list and the perceived areas of overlap, there was a recognition that we needed to focus on the key themes and areas. Some classes of items are obviously more important than others. These important item classes came to be referred to as "tenets". Some of these tenets were discussed – see below – but others were not (e.g., privacy). With more time to discuss requirements, other tenets would have been discussed as well.

Tenets

Generally WG1 recognizes that programming and content has value, and mechanisms need to be put in place to protect intellectual property rights in such content. At a fundamental level this involves encryption and the use of a secure system that can identify, authenticate, and protect content from all of the points that have access to this system.

The group did not have sufficient time to completely identify all of the tenets, but a few key ones did surface and received extensive discussion, and at times debate.

Tenet: User Interface

The tenet that received the most focus had to do with the presentation of a MVPD's service. Although more comprehensive than just the user interface, the "UI" was the term we used to frame the discussion. Should a MVPD's UI be allowed to exist as the only possible method through which an MVPD's customer consumes the MVPD service? Or should competitive devices have access to (or continue to in the case of cable MSOs) a MVPD's services (or "Service" as MVPD's like to refer to it), for instance licensed linear programming, and enable those services to be presented by a retail device with its own UI? This topic received fervent debate. MVPDs state that they have come a long way from the days of simply broadcasting video channels, and placing them up on a list or grid on a TV guide. MVPDs also assert that a profusion of additional features have been added to their offerings, with most being incorporated into their UI.[1]

Other participants, such as consumer advocates, retail device manufacturers, and other MVPDs, assert that a fundamental feature of a competitive navigation device is that it has the option to present its own unique UI to access the MVPD services. Without the ability to present a unique UI, such parties assert, retail devices would be denied some ability to innovate and present the consumer with a differentiated and competitive alternative to an operator-supplied device. As a counter-point to this argument, the MVPDs noted that they are simply trying to honor their programming agreements.

[1] Examples include Start Over & Look Back, recent tuning history across devices, Voice Control, Caller ID on the TV (integrated with an operator's telephone service), HD Auto-tune (the automatic selection of HD versus SD channels when detected that an HD television set is attached), and on-screen Instant Upgrade and/or Bill Pay.

Tenet: Guide Data

Another topic that received much deliberation and discussion related to intellectual property rights in guide data. Some group members advocate that MVPDs should be required to provide retail devices with MVPD guide data (program information).

MVPDs pointed out that some of this data is provided under commercial terms that only allow a B-to-C (business to consumer) distribution, not a B-to-B (business to business) type arrangement. Consumer advocates and retail device manufacturers point out that certain guide data, such as VOD, is not subject to such constraints and is only available from the MVPDs.

Tenet: Technology Licensing

Additionally, CE manufacturers assert that technology required by the MVPD's architecture to implement their conditional access solution needs to be available through particular licensing terms (*i.e.,* be fair, reasonable, and non-discriminatory, or FRAND) to enable a competitive retail market. Some MVPDs have made clear that many such technologies are owned and controlled by third parties, with terms not under the control of the MVPD. Consumer advocates and retail manufacturers have made clear that they believe the FCC has the authority to require such licensing.[2]

[2] For example, see 47 CFR 76.1204(c), "No multichannel video programming distributor shall by contract, agreement, patent, intellectual property right or otherwise preclude the addition of features or functions to the equipment made available pursuant to this section that are not designed, intended or function to defeat the conditional access controls of such devices or to provide unauthorized access to service."

General Topics of Discussion

This section discusses other important areas of interest that were discussed amongst the WG1 members.

Scope of Work

Some group members expressed concern that several of the proposed requirements and tenets go beyond recommendations for downloadable security, and could conflict with contractual agreements (including licensing terms), intellectual property rights, and copyright law. Other group members state that the purpose of the working group is to help the FCC determine technical solutions in furtherance of Section 629 of the Communications Act which directs the FCC to assure the development of a market for retail navigation devices.

Technological Differences

An additional topic that received a lot of attention was the fact that a DBS system is essentially a one-way system while others are two-way.

Given that the statutory requirement calls for a “uniform, and technology- and platform-neutral” system, some think that this presents an immediate paradox: either two separate systems are described, bifurcated into one-way and two-way (thus no longer honoring the requirement), or the system must be treated solely as a one-way system, which is an objectionable compromise to some group members. Those members still think the requirements can be uniformly met, but we did not get into details.

Others do not believe there is any such paradox, and believe that “uniform, and technology- and platform-neutral” can be met without making two separate systems. Indeed, those WG1 members state that there are no particularly insurmountable issues to meeting the statutory requirement.

Appendix 1

REPORT OF WORKING GROUP 1 TO DSTAC

March 24, 2015

Introduction

Working Group 1 has collected a set of commercial requirements through presentations from five perspectives: MVPDs; CE/device manufacturers; consumer; content providers; and security.

The working group has not yet tried to reconcile the requirements presented.

The primary points that have been raised are summarized below.

MVPD Requirements

Jay Rolls, Charter, John Card, DISH and Steve Dulac, DIRECTV, presented requirements for MVPDs. Common elements include:

Security and Content Protection. Security and content protection for MVPD services includes support for the conditional access systems' (CAS) and Digital Rights Management (DRM) systems' trust infrastructure and model. MVPDs must follow compliance and robustness rules that help control how resistant devices must be to attack and how they manage content and related copy, retransmission, or use restrictions in order to prevent piracy and to protect content holders' rights. Protection also requires meeting content provider requirements that are part of negotiated licenses that give each party defined rights and obligations. For example, the content provider may define a geographic area, give larger in-home rights than out-of-home rights, require a hardware root of trust for high value content, limit what content is available to less trusted devices, and require other terms that rely on an unbroken chain of trust. Licenses may also include terms to protect the content providers' brand, such as acceptable advertising, channel position and neighborhood, and subscription tier placement.

Consumer Protection Obligations. MVPDs design their service to meet regulatory requirements, such as emergency alerts (EAS), closed captions, and limits on the web links shown to children. Cable and satellite providers have privacy obligations to protect personally identifiable information, including subscriber viewing habits. Proposed recommendation: A downloadable security solution must comply with these legal requirements placed on service providers.

Execution of Video Provider's Service Offering. Each MVPD assembles, markets and delivers a branded service that includes programming, integrated data, interactive features, a guide, and software that enforces content provider requirements. MVPDs continue to enhance their service. A poor consumer experience caused by either an MVPD or third party device adversely impacts the MVPD customer relationship. MVPDs protect and promote their brand and marketing to customers through their service.

Support for Business Operations. Any solution has to support the business operations of the service provider. For example, there are ordering processes for VOD and audit trails to handle billing disputes. Consumers may be provided the ability to upgrade their account from the application UI, which must then integrate with various billing systems.

Support for Distribution Architecture. Each MVPD also has unique and specific transport layers, codecs, control channels, etc., so the end-to-end delivery of service all the way to the consumer has to fit within that architecture.

Support for Service Installation and Configuration. Each MVPD also has requirements for how service is enabled or installed. For example, a satellite receiver (IRD) will not receive DBS service unless there is an Out Door Unit (ODU), Multiswitch and professional installation to point the ODU at the satellite; when service providers install wired networks, they test signal levels and use remote diagnostics to insure proper installation.

Advertising. MVPD operations are funded in part by advertising, so MVPDs operate advertising systems that: meet content provider restrictions; provide audit paths for advertisers; and enable a variety of more advanced types of advertising, such as zone advertising, local advertising using DVR technology, advertising targeted to election districts, advertising targeted to different interest groups, transactions and usage reporting, and interactive Request For Information (RFI) ads where the consumer can, for example, order a coupon with their remote.

Customer Support. MVPDs need built-in support for customer service, such as access to diagnostic tools that are often included in CPE. Customers may need to access information generated by these tools in conversations with Customer Service Reps to resolve customer problems.

Change. These systems change on a frequent, sometimes regular basis. There are regular updates, bug fixes and feature enhancements. MVPDs continually maintain and enhance security to protect consumers and content. Device robustness requirements can also change over time. On occasion, systems can change in a way that obsoletes older devices.

Intellectual Property. MVPDs operate within limits of intellectual property. They must: respect conditions of copyright licenses from commercial video content providers that are typically included in bilaterally negotiated affiliation and retransmission agreements; respect the intellectual property controlled by other licenses (e.g. guide data that Rovi or Tribune licenses for limited use); license or otherwise accommodate patents and intellectual property in their implementations.

Device Manufacturer Requirements

Brad Love, Hauppauge, presented device requirements that manufacturers would like to see in the future:

User Interface. The system must allow for, but not require, third-party manufacturers to supply their own user interfaces. Third-party user interfaces allow for unique consumer experiences and differing feature sets than offered by an MVPD, in addition to fostering meaningful competition. The third-party user interfaces must be allowed full access to all linear channels, VOD, and PPV. Remote presentation of user interface (RUI) must also be allowed, such as might be the case for 'headless' (non-HDMI) gateway devices.

Uniform Provider Terms. All content providers should ideally follow uniform terms of affiliation license, and use common copy control instructions. Signaling or embedding of copy control data is required for all programs. Recording must not be prohibited for non-premium programs, and fair use should apply for all recorded material.

Output Restrictions. A device must be able to output to any secure/licensed device. Recordings must be able to be exported to any licensed/secure device in approved formats, depending on copy control restriction. Secure network retransmission of programs via DTCP-IP or other secure methods must be allowed. In the case of 'copy free' programs network transmission in the clear must be allowed, as is the case currently.

Guide Data. A device should ideally receive guide data from MVPD's for at least 7 days. However, guide data for VOD and PPV must always be supplied by the MVPD in order to receive accurate and up to date information on dynamic content. A unified method of distribution must be chosen for guide data delivered from MVPD's.

EAS. A device must have some uniform way of receiving EAS data from MVPD's.

Security. Every MVPD should ideally use the same security methods and CAS, or at most, a limited number of permutations. There should be common reliance on security methods for the DCAS module. There must also remain a 'man machine interface' (MMI) to allow interaction with the DCAS module.

Terms. All required technology should be available under FRAND licenses (fair, reasonable, and non-discriminatory). A neutral organization should be responsible for initial certification and self certification should be allowed for subsequent re-testing.

Portability. The device must work uniformly across all MVPD's and be user friendly to activate. If upstream communication is required minimal restriction should be placed on the source of the connection.

Consumer Requirements

Adam Goldberg, Public Knowledge, presented a consumer view that included these requirements:

The system must allow unaffiliated third-party manufacturers to build navigation devices, and the system must allow those devices to be sold directly to consumers through unaffiliated (and unconstrained) retail channels.

Retail navigation devices must function properly on all MVPD’s networks, and must be portable to other networks (e.g., when a consumer changes MVPD or moves into another cable operator’s footprint).

Retail navigation devices must allow for a wide range of product prices, features, manufacturers, etc., and the system must impose only requirements necessary on retail navigation devices to enable the system.

The system must provide discovery of all available television services to retail navigation devices (what services are available on the network), and must provide a mechanism for identifying them in, e.g., an electronic program guide.

The system must allow (but need not require) a retail navigation device to provide its own user interface, and such user interface must be capable of enabling navigation to all available services (including services which require a commercial interaction, like PPV).

The system must enable retail navigation devices to provide EAS information, and closed captioning. The system must enable retail navigation devices to provide parental controls (v-chip).

Content Providers Requirements

John McCoskey, MPAA, presented requirements of content providers:

Authentication. The system must require and support basic authentication practices, including: subscriber validation, device authentication, subscription validation and service entitlement.

Content Protection. The system must meet at least the same content protection requirements that existing solutions meet today, with no decrease in content security due to downloadable security. The system must be upgradable. The MovieLabs *Specification for Enhanced Content Protection – Version 1.1* shall be the reference model for content protection.

Respect of Licensing Agreements. The system must support the technical requirements of content/service licenses. The solution must ensure content/service handoff is consistent with license terms with MVPDs.

No Disaggregation of Service. The solution must prevent disaggregation of retail content offerings licensed to MVPDs. Devices are to access the existing service provided by the content owner and MVPD, not to disaggregate service elements outside of contractual agreements.

Security Requirements

Robin Wilson, NAGRA, presented requirements for security that include:

Robustness. Robustness requirements establish different levels of resistance to different levels of resources applied by attackers, which can range from college student with little time and money to state actors. There are conventional breaking points for different levels of robustness, such as 480i (Standard Definition), 720p (low end of High Definition), 1080i and 1080p (high end of High Definition) and 4K (Ultra High Definition).

Encryption and key exchange. There are two complementary processes in CAS: encryption and key exchange. Encryption has advanced from DES to Triple DES to AES. The integrity is strong if you have strong keys. The second part of the process is key exchange and how you securely get the keys to the subs to decrypt content. Common encryption can support multiple key exchanges.

Certification. Certification or auditing is required to ensure that security is implemented to the level specified and required by the content owner.

Downloadable. The presentation also addressed some future issues associated with downloadable security:

- A key ladder attached to a root of trust
- The security downloader itself, and management of keys. The function has to trust the code to operate within a chain of trust.
- Need to address renewability
- Need to preserve room for innovation in rights management

- Need to evaluate balance between security implemented in secure software and one or more hardware roots of trust

Ban the term "Black Box." The term "black box" has specialized meaning in cryptography, and DSTAC should avoid the term.

Further Discussion

There is much room for further discussion. Because of the short period provided, the working group only had time to take an initial snapshot, and not to completely analyze these requirements or try to reconcile them.

Appendix 2

Number	Requirement
M 1	The system must support the Conditional Access System (CAS) and Digital Rights Management (DRM) trust model and infrastructure requirements in the service provider's system.
M 2	The system must follow the service provider's rules for compliance and robustness rules, for managing content and related copy, retransmission, or use restrictions.
M 3	The system must support each service provider's fundamental data and video delivery mechanisms: transport layers, codecs, control channels, return paths etc. as required to fit within the service provider's delivery architecture.
M 4	The system must preserve and present the branded service that represents the MVPD's offering, including but not limited to the programming, integrated data, interactive features, a guide, and software that enforces content provider requirements.
M 5	The system must meet content provider requirements that are part of negotiated licenses and retransmission agreements that give each party defined rights and obligations.
M 6	The system must support all of the service provider's regulatory requirements for content delivery, such as channel position, emergency alerts (EAS), closed captioning, and limits on web links shown to children.
M 7	The system must not allow relocating a channel to a different number or 'neighborhood' in the line up.
M 8	The system must support the service provider's obligation to protect all personally identifiable information of the customers, including subscriber and viewing habits
M 9	The system must support the service provider's protection of the privacy of video streams.
M 10	The system must not run advertisements, promotions or overlays over the service provider's video programs or over the guide.
M 11	The system must support the service provider's advertising systems that honor content provider rules and restrictions, and must prevent alteration of advertising as provided.
M 12	The system must support the service provider's audit paths for the tracking of advertising and viewership.
M 13	The system must support the service provider's requirements for service enablement and installation. The system must support the appropriate network connections or receivers (such as a satellite receiver), and wired networks with appropriate signal levels and diagnostics.
M 14	The system must support all business operations of the service provider, as required to support ordering, upgrading, billing, authorizing, and promoting services offered to customers.

M 15	The system must support the service provider's advanced advertising features, such as zone advertising, local advertising using DVR technology, advertising targeted to election districts, advertising targeted to different interest groups, transactions and usage reporting, and interactive Request For Information (RFI) ads.
M 16	The system must support diagnostic tools required by the service provider to install, upgrade and troubleshoot operation of the system. These tools must be accessible by customers and/or service provider customer service representatives to resolve customer problems.
M 17	The system must support the service provider's ability to be update service with feature enhancements and bug fixes required to maintain or enhance the security system that protects content and users.
M 18	The system must allow for updating of robustness requirements to match the current state of the art.
M 19	The system must respect the intellectual property controlled by other licenses, such as data and properties delivered by 3rd party EPG or content providers.
M 20	The system must not impose new patent or intellectual property obligations on the service provider.
M21	Guide and Program data will only be provided via the MVPD's integrated service environment. See M4.

B1	The system must protect linear channels and linear PPV.
B2	The system must support "pushed" (precached) VOD content delivered by DBS.
B3	The system must support "pulled" (on-demand) buffered content delivered by DBS or broadband.
B4	The system must support start over/look back content delivered by broadband to STB.
B5	The system must support linear streamed content to in-home devices in proximity to the STB.
B6	The system must support streaming linear channels to authenticated out-of-home devices via (native) app and (HTML5) website.
B7	The system must support streaming on-demand programming to authenticated out-of-home devices via (native) app and (HTML5) website. (Differs from B6 because of included search and possible purchase.)
B8	The system must support download of on-demand programming to authenticated out-of-home devices via (native) app and (HTML5) website.
B9	The system must support start over/look back content delivered by broadband to to authenticated in-home devices via (native) app and (HTML5) website.
B10	The system must support start over/look back content delivered by broadband to to authenticated out-of-home devices via (native) app and (HTML5) website.
B11	The system must support authenticated linear and/or on demand streaming and/or download, using content owner's app and/or website.

B12	The system must support place-shifted content , streaming and/or download in-home and/or out-of-home and/or streaming via STB (or an external transcoder device) to devices (on service provider's app or website).
B13	The system must support delivery of content that is restricted by exclusivity deals managed by the content owner.
B14	The system must support delivery of content that is restricted by the service provider because of rational reasons. (Expected future discussion)
B15	3rd party devices should by default present all content available from the service provider.
B16	The system must support channels assigned to discrete packages. Packages must have unambiguous definition; contain enough channels; and there must be enough packages available to manage current and foreseeable operations. (Design requirement both inside the CAS and for security API)
B17	The system must allow different resolutions of content to be managed by different entitlements.
B18	Rights managed by the system must have different availability windows with defined start and end times.
B19	The system must support restricting the availability windows (times and dates) for features and content to the broadcast time of events.
B20	The system must support expiration dates and times (possibly never) for content.
B21	The system must support the addition and deletion of channels in one or many packages.
B22	Same as B15.
B23	The system must support different packages and channels between DBS and broadband delivery.
B24	The system must support different event lineups on a channel simultaneously received by DBS and broadband.
B25	The system must support timely deletion (removal, "take down") of events and channels.
B26	The system must respond to deletion (removal, "take down") events and channels within one hour. (3rd party device accuracy implications)
B27	The system must support simultaneous delivery of the same channel on DBS and broadband.
B28	The system must distinguish between instances of a channel delivered on DBS and broadband.
B29	The system must distinguish between instances of content delivered over different IP networks. (For DBS when additional carriage agreements are in place)
B30	The system must support delivery to single family homes.
B31	The system must support delivery to multi-dwelling units.
B32	The system must support delivery to restaurants and hotels.
B33	The system must support delivery to hospitals.
B34	The system must support delivery to schools.
B35	The system must support delivery to business offices.

B36	The system must support delivery to malls and commercial shopping establishments.
B37	The system must support delivery to aircraft and other vehicles.
B38	The system must support limiting delivery of content to within or excluded from one or more disjoint, adjacent, and/or overlapping geographic territories.
B39	The system must support limiting delivery to a subscriber account billing address within a territory.
B40	The system must support use of geofiltering technology.
B41	The system must support use of Content Delivery Networks for broadband distribution.
B42	The system must support blackouts of particular programs.
B43	The system must distinguish between and blackout specific instances of particular programs.
	The system must support real-time updates to blackouts.
B45	Same as B15.
B46	The system must allow content to be restricted to "in-home" use.
B47	The system should support an authenticated communications path with a 3rd party device.
B48	The system must support different rights for different devices.
B49	The system must distinguish among different other CAS and DRM systems, and allow reasonable treatment of differences.
B50	The system must support delivery of SD and/or HD to particular devices.
B51	The system must not interfere with viewing measurement technologies.
B52	The system must not interfere with watermark technologies.
B53	The system must support content-owner approved content protection (output) technologies.
B54	The system must support the pass-through and generation of CCI on outputs.
B55	The system must support CCI settings agreed to between content owners and service providers.
B56	Content owners must approve the system.
B57	The system must support content-owner approved DRM systems.
B58	The system must support a range of robust solutions.
B59	The system must support a requirement that devices must be registered to a subscriber account.
B60	The system must support a requirement that no more than X devices may be registered to a subscriber account at any given time.
B61	The system must support a requirement that no more than X concurrent streams of a content owner’s programs might be allowed to devices registered to one subscriber account .
B62	The system must support a requirement that no more than X downloads of a content owner’s programs might be allowed to devices registered to one subscriber account.
B63	The system must support AES-128.
B64	The system must support different behaviors with "jailbroken" devices.

B65	The system must support restrictions on user authentication methods (e.g. user ID and passwords of sufficient complexity).
B66	same as B55
B67	same as B40
B68	The system must support 3rd party security audits.
B69	same as B52
B70	The system must allow appropriate response to security threats of varying magnitudes.
B71	The system must support monitoring live operations.
B72	The system must support reasonable withholding of content to particular devices or subscribers.
B73	The system must support reinstatement of service after security issues are resolved.
B74	The system must support "channel neighborhoods".
B75	The system must allow particular programs not be listed with other programs.
B76	The system must support reasonable restrictions on foreign content overlays.
B77	The system must support use of service provider provisioned logos on 3rd party devices.
B78	The system must support updates to service provider provisioned logos.
B79	The system must support presentation of pre-roll information.
B80	The system must support Disabling the “Fast Forward” remote control feature during advertising for services (e.g. Start Over / Look Back).
B81	The system must preclude automatic deletion of ads from DVR recordings of linear services.
B82	The system must support use of DVR recording space for dynamic ad insertion.
B83	The system must support dynamic ad insertion for content distributed by CDN.
B84	The system must support "blind" ad sales.
B85	The system must support pre-order of PPV content.
B86	The system must support instant purchase of PPV content.
B87	The system must allow a subscriber to manage features of their subscription packages in online and offline operation.
B88	The system must support timely purchase reports.
B89	The system must operate in accordance with privacy regulations and user agreements.
B90	The system must support collection of information about the viewing of DBS distributed programs by its subscribers.
B91	The system must support report of usage/viewership of broadband delivered content and downloaded content.
B92	The system must support communication of a Listing Service ID.
B93	The system must support controlled announcement of a program or channel availability.
B94	The system must support start and stop dates for program availability and start dates for certain features like DVR recording and customer directed commercial skips.

B95	The system must support the delivery of trigger information for collecting programs from DBS distribtion or broadband.
B96	The system must support different lead times for service and program related metadata.
B97	The system must operate in accordance with applicable regulations and laws.
B98	The system must allow a service provider to respond to market requirements and customer needs
B99	The system must allow a service provider to define a competitive product – "The Service"
B100	The system must allow a service provider to offer a competitive product – "The Service"
B101	The system must allow the service to be maintained (throughput and scale)
B102	The system must allow a service provider to control its costs of doing business
B103	The system must not interfere with the measurement of the effectiveness of other deployed systems
B104	The system must not interfere with the measurement of the effectiveness of existing business processes
B105	The system must allow changes to other deployed systems
B106	The system must allow changes to existing business processes
B107	The system must allow the service provider to specify systems used to deliver the service
B108	The system must allow the service provider to manage systems used to deliver the service
B109	The system must allow a service provider to stop support for obsolete features that are no longer cost effective
B110	The system must allow for delivery system and component testing and qualification
B111	The system must secure the signal
B112	The system must secure the content
B113	The system must itself be secure
B114	The system must allow a service provider to maintain existing customer relationships
B115	The system must allow a service provider to negotiate for the best deal with vendors, suppliers, and 3rd party partners
B116	The system must support management of expected events (DST)
B117	The system must support management of unexpected events (system failure)
B118	The system must allow a service provider's business to grow
B119	The system must allow a service provider to add new customers
B120	The system must allow a service provider to increase revenue from existing customers
B121	The system must respond to changes in content owner requirements
B122	The system must allow the service provider to develop new features and new services
B123	The system must allow the service provider to deploy more efficient technology and processes

B124	The system must enforce agreements customers make with the service provider.
B125	The system must not leak unpaid-for content.
B126	The system must enforce agreements service providers make with the customer.
B127	The system must support the communication of clear terms and pricing.
B128	The system must communicate the subscriber's clear acceptance of an offer.
B129	The system must support the service provider to resolve customer issues.
B130	Same as B97

C1	The system must allow unaffiliated third-party manufacturers to build navigation devices, and the system must allow those devices to be sold directly to consumers through unaffiliated (and unconstrained) retail channels.
C2	Retail navigation devices must function properly on all MVPD's networks.
C3	Retail navigation devices must be portable to other networks (e.g., when a consumer changes MVPD or moves into another cable operator's footprint)
C4	Retail navigation devices must allow for a wide range of product prices, features, manufacturers, etc.
C5	The system must impose only (the minimal set of) requirements necessary on retail navigation devices to enable the system.
C6	The system must provide discovery of all available television services to retail navigation devices (what services are available on the network).
C7	The system must provide a mechanism for identifying all available television services in, e.g., an electronic program guide.
C8	The system must allow (but need not require) a retail navigation device to provide its own user interface, and such user interface must be capable of enabling navigation to all available services (including services which require a commercial interaction, like PPV).
C9	The system must enable retail navigation devices to provide EAS information, and closed captioning. The system must enable retail navigation devices to provide parental controls (v-chip).

P1	The system must require and support basic authentication practices, including: subscriber validation, device authentication, subscription validation and service entitlement, and must include geolocation to support territorial and regionally restricted content distribution.
P2	The system must meet at least the same content protection requirements that existing solutions meet today, with no decrease in content security due to downloadable security. The system must be upgradable. The MovieLabs Specification for Enhanced Content Protection – Version 1.1 shall be the reference model for content protection.
P3	The system must support the technical requirements of content/service licenses. The solution must ensure content/service handoff is consistent with license terms with MVPDs.

P4	The solution must prevent disaggregation of retail content offerings licensed to MVPDs. Devices are to access the existing service provided by the content owner and MVPD, not to disaggregate service elements outside of contractual agreements.

D1	The system must support, but not require, third party user interfaces.
D2	Third party user interfaces must have access to all linear channels, VOD, and PPV.
D3	Remote presentation of user interface (RUI) must be supported, but not required.
D4	All content providers must have common copy control instructions.
D5	Signaling or embedding of copy control data must be required for all programs.
D6	Recording must not be prohibited for non-premium programs.
D7	Devices must be able to output content via any secure output to any secure device.
D8	Recordings must be exportable to any secure device, subject to copy control restrictions.
D9	Notably, DTCP-IP outputs must be supported.
D10	TO BE DISCUSSED: In the case of 'copy free' programs, network transmission in the clear must be allowed, as is the case currently.
D11	Retail devices should be provided with MVPD guide data by the MVPD's for at least the subsequent seven days.
D12	Guide data for VOD and PPV must be supplied by the MVPD to the retail device.
D13	Guide data, when provided, must be in a single standardized format.
D14	The system must have a uniform way of supplying EAS data from MVPD to retail devices.
D15	Retail devices must be supplied content secured by a uniform security method and CAS, or at most, a limited number of permutations.
D16	There should be a common reliance on security methods for the DCAS module.
D17	There must also remain a 'man machine interface' (MMI) to allow interaction with the DCAS module.
D18	All required technology must be available under FRAND licenses (fair, reasonable, and non-discriminatory).
D19	Neutral organization(s) must be responsible for initial certification of a device, and self-certification should be allowed for subsequent re-testing.
D20	The device must work uniformly across all MVPD's and must be user friendly to activate.
D21	If upstream communication is required, minimal restriction should be placed on the source of the connection.

S1	The system shall avoid common failure modes and careful consideration should be given to avoid selecting any single system or subsystem that could result in catastrophic failure to the whole system.

S2	In addition to downloading a CAS or DRM client, the system shall have a mechanism(s) to download countermeasures (SW patches) to fix security or other flaws without replacing the whole security application or SW stack.
S3	The additional security aspects and risks associated with the downloader needs to be tied to the security of the whole system and addressed.
S4	The scrambling or encryption algorithm used for the content should conform to open and fully disclosed industry standards such as AES 128 and defined in such a way (block size, key periodicity, etc...) that allows common encryption (key sharing / simulcrypt) across both CAS and DRM use cases.
S5	The security system shall allow different levels of robustness to match the license agreements requirements, content value, content resolution, and threat models while matching appropriate cost and complexity goals of rendering devices.
S6	Compatibility should be provided for browser or application environments using emerging standards such as EME.
S7	The system shall be designed such that CAS and DRM system can interoperate with common encryption (i.e. without trans-encryption).
S8	The system shall allow use cases that include linear/live broadcast/OTT, VOD and sideloading (redunant to other more verbose definitions).
S9	All SW components of the system shall be replaceable via download.
S10	The system shall support one or more HW roots of trust (more than one to avoid a potential single point of catastrophic failure.
S11	The system shall support a SW root of trust but only in devices where no HW root can be used and in addition, the robustness requirements can be met for the type of content processed.
S12	The system shall provide the necessary robustness to sustain the likely threat models.
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).
S16	One Way Network Use: If this mode is deemed within the scope, the system must have a mode of operation so that communications such as authorization and de-authorization must be able to be carried in the one-way data stream (DBS to land, DBS to aircraft....)

Letter	Section
M	MVPD - MSO
B	MVPD - DBS
C	Consumer
P	Content / Programming
S	Security
D	Device