Commercial Requirements for DVB-I

Enhanced DRM, Service & Service List Protection, Customisation for Service Discovery, Accessibility Services and Application support

DVB Bluebook C108

November 2023

Intellectual Property Rights

Please refer to the IPR policy of DVB Project available at: https://dvb.org/about/policies-procedures/

Foreword

DVB is an industry-led consortium of broadcasters, manufacturers, network operators, software developers, regulators and others from around the world committed to designing open, interoperable technical specifications for the global delivery of digital media and broadcast services. DVB specifications cover all aspects of digital television from transmission through interfacing, conditional access and interactivity for digital video, audio and data. DVB dominates the digital broadcasting environment with thousands of broadcast services around the world using DVB specifications. There are hundreds of manufacturers offering DVB-compliant equipment. To date, there are over 1 billion DVB receivers shipped worldwide.

Executive summary

DVB published a new version of the DVB-I BlueBook Specification (A177r5), in June 2023.

On reflection by CM-I and TM-I, and with various new contributions suggested by DVB Members and DVB-I Users (via a public forum set up by DVB), a number of new topics are now being taken into consideration for a future revisions of the DVB-I Specification and DVB-I Implementers' Guidelines documents (A177 and A184 respectively).

These topics include various security requirements for 1) protection of Content, and 2) protection of DVB-I compliant devices, services and service lists, plus some additional miscellaneous requirements around Customisation of service lists, provision of new Accessiblity Services and enhanced support for Applications.

Use cases and commercial requirements for these features have been elaborated in this document, adhering to the guiding principle for this specification of the need to deliver the full linear television experience over IP networks, including high quality content with low latency coupled with program information for a complete service offering.

The intention is to inform the work required by TM-I working group to deliver a specification that can be easily implemented to protect the whole DVB-I ecosystem while maintaining a user experience at least equivalent to today's TV experience.

Due to the global nature of IP delivered TV, the specification should seek to avoid being too restrictive and therefore implies the need for a good, flexible, interoperable solution.

Contents

1. Introduction

This document specifies a set of commercial requirements enhancing DVB specifications including, but not restricted to, the DVB-I Service Discovery and Programme Metadata Specification (A177) and the DVB-I Implementation Guidelines (A184)

1.1. Scope

The scope of this document is Commercial Requirements for the enhancement of DVB-I, principally in the areas of Content (DRM) and Service related protection, Customisation and Accessibility Services, and Application support.

1.2. Overview of Commercial Requirements

The set of commercial requirements for enhancing the DVB-I system specifications covering the following areas:

- Improved support for the use of DRM systems with DVB-I. DVB-I already supports the use of DRM. These CRs aim to:
  - Optimise the use of DRM with DVB-I services based on feedback from trial deployments and experience in the field.
  - Improve the user experience, for example by avoiding multiple unnecessary logins and enabling the consistent selection of audio tracks and subtitles.
  - Improve scalability and performance.
  - Support additional use cases.
- Improved support for applications in DVB-I systems. DVB-I already supports the signalling and delivery of applications as part of DVB-I services. These CRs aim to:
  - Fulfil additional commercial use cases.
  - Improve the consistent selection of accessibility features between applications.
- Improved support for customisation of elements of DVB-I Service Discovery. These CRs aim to:
  - Allow customisation of DVB-I service offerings to individual users.
- Improved support for protection of services and service lists. These CRs aim to:
  - Prevent tampering with services and service lists through the use of various security measures.
- Support for non-standardised HTTP streaming of Icecast audio services. These CRs aim to:
  - Define requirements for Icecast Audio HTTP streaming.

2. References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, DVB cannot guarantee their long term validity.

[1]	ETSI TS 103 777	Digital Video Broadcasting (DVB); Service Discovery and Programme Metadata for DVB-I
[2]	A184	DVB-I Implementation Guidelines
[3]	W3C TR CSP	W3C Content Security Policy Level 2: https://www.w3.org/TR/CSP2/
[4]	RFC6797	HTTP Strict Transport Security (HSTS)
[5]		

3. Definitions and conventions

3.1. Terms

For the purposes of the present document, the following terms apply:

Type 1.2 application	An associated application that controls media presentation or has no media
DVB-I System	This term is used to represent the collective group of Specifications and Guidelines for the DVB-I System, including but not limited to the DVB-I Service Discovery specification (A177) and Guidelines (A184), the DVB-DASH specification (A168) plus any V&V specifications developed as a result of this work.
WebView	A browser engine contained within an application that allows programmers to write the bulk of their application using HTML, JavaScript and CSS, which are the standard Web programming tools
Persistent cookies	Cookies that remain on a user's device until the end of an expiration period, even after they close their browser, and are used to store information that can be accessed across multiple browsing sessions

3.2. Abbreviations

For the purposes of the present document, the following abbreviations apply:

CM-I	Commercial Module for Internet based Specifications
CR	Commercial Requirement (per DVB definition)
DASH	Dynamic Adaptive Streaming over HTTP
DRM	Digital Rights Management
DTT	Digital Terrestrial Television
DVB	Digital Video Broadcasting
DVB CM	Digital Video Broadcasting
DVB TM	Digital Video Broadcasting
DVB-DASH	Digital Video Broadcasting - DASH
DVB-I	Digital Video Broadcasting - Internet
EPG	Electronic Program Guide
FTV	Free to View
HbbTV	Hybrid Broadcast Broadband Television
HTML5	HyperText Markup Language
Icecast	Non standardised HTTP streaming for audio: https://www.icecast.org/
IRD	Integrated Receiver Device
MPD	Media Presentation Description
RF	Radio Frequency
SSO	Single Sign-On
TM-I	Technical Module for Internet based Specifications
UI	User Interface
UX	User Experience

3.3. Conventions

Commercial Requirement tagging scheme:

Req x. [y].z.	Name	Status	Priority	Use case
Numeric requirement ref. x = section y = subsection(s) z = sequence number This is a unique id within the document that could be used to refer to a requirement within a specific version of this document. Note that this id. is not strictly coupled to the particular requirement, could vary across different versions of this document		This status field can have the following states: **Draft** = work in progress **Review** = believed to be at the stage where it is ready for review by the group **Complete** = completed and agreed in task force **Agreed** = agreed within CM-I **Accepted** = accepted by CM	This field is the associated priority set by the CM to the requirement. 1➔ Must have 2➔ Recommended to have 3➔ Nice to have	Identifies the use cases that relate to this commercial requirement, if applicable. [UC]

For the purpose of this document, the following normative conventions are used in the Commercial Requirements text:

Convention	Meaning
shall enable	The functionality shall be specified but its support is optional.
shall support	The functionality shall be specified and its support is mandatory.
should enable	The functionality is recommended to be specified and its support is optional.
should support	The functionality is recommended to be specified and supported.
may enable	The functionality may be specified and if it is then its support is optional, and it shall not have any weight in the selection or exclusion of any particular solution.
may support	The functionality may be specified and if it is then its support is recommended but it shall not have any weight in the selection or exclusion of any particular solution.
shall not preclude	The functionality shall not be prevented.
should not preclude	It is recommended not to prevent the functionality.

4. Commercial requirements

4.1. Content Protection and DRM related requirements (consolidated)

Req 4.1-1	Single Sign-on for groups of channels	Agreed	1	UC6.3, UC6.4, UC6.20
The DVB-I System shall enable use of a common subscription mechanism/sign-on to avoid users having to sign-in to each individual service provider/channel (or group of channels). NOTE: this CR may be met by existing DVB specifications.				

Req 4.1-2	Persistent sign-on and consent	Agreed	1	UC6.2, UC6.3, UC6.4, UC6.20
The DVB-I System shall support persistent storage of consent status information of Broadcasters. Note: When single sign-on is managed by Platform Operators, each Broadcaster / Service Provider has to obtain user's consent on the first occasion the user selects a service from that Broadcaster / Service Provider.				

Req 4.1-3	Licence Acquisition	Agreed	1	UC6.2, UC6.20
The DVB-I System shall allow users to acquire rights for broadband delivered content that is compatible with DVB-DASH and is protected by supported DRM schemes. Existing widely deployed DRM schemes shall be supported and new DRM schemes shall not be precluded. NOTE: 1. as this implies that a given service list may contain content protected by n different DRM protection schemes, the solution should support multi-DRM capability with fully interoperable DRM schemes. 2. as content provision may vary over time it should be possible to add, modify or remove protection of content from a service list without interrupting the service. 3. the term 'widely deployed' is used to avoid naming specific DRM schemes.				

Req 4.1-4	License Persistence/User Experience	Agreed	1	UC6.20

Service providers should be given at least the following options for protecting DVB-I services delivered by DVB-DASH:

- persistence of licences to be configurable.
- cost of provisioning DRM licenses to be minimised (including minimising the number of licenses requested).

NOTE: The technical module should address this as best they can within the limitations of confidentiality for documentation of DRM schemes.

Req 4.1-5	Content Encryption	Agreed	1	UC6.20

The DVB-I System shall enable the content or service to be encrypted once, while supporting decryption by multiple DRM schemes.

NOTE: this CR may be met by existing DVB specifications.

Req 4.1-6	Device Support	Agreed	1	UC6.20

The DVB-I System shall support basic DRM functionality i.e. license acquisition, to let devices natively decrypt and present the content without a web browser environment.

The TM is asked to identify what might be realistically practical within DVB and validate this with the CM before starting any detailed technical work. Examples to fullfill the CRs could be: guidelines / example architectures and potentially ‘hooks’ to facilitate such deployment.

Req 4.1-7	Channel protection and blocking	Agreed	1	UC6.2

Service providers shall be given at least the following options for protecting DVB-I services delivered by DVB-DASH;

- where all users are able to decrypt the service.
- where selected programmes can be blocked for selected users (e.g. where the service provider does not have rights for some programmes in some markets).

NOTE: this CR may be met by existing DVB specifications.

Req 4.1-8	Channel Change Time/User Experience	Agreed	1	UC6.20
The DVB-I System shall support a channel change time to a protected DVB-DASH service which is comparable to protected broadcast channels, to allow an acceptable user experience when channel zapping. NOTE: The reference: https://nordig.org/wp-content/uploads/2016/03/NorDig-Unified-Requirements-ver.-3.2.pdf section 11.4 gives some order of magnitudes for zapping time.				

Req 4.1-9	Application Independent Operation	Agreed	1	UC6.3, UC6.4, UC6.6, UC6.20
The DVB-I System shall support authentication and playback of DRM-protected content for both HbbTV (e.g. TVs) and HTML5 (e.g. Phones/Tablets) devices.				

Req 4.1-10	Linked Applications	Agreed	1	UC6.2, UC6.19
The DVB-I System shall support simultaneous use of linked applications type 1.1 and 1.2. Note: there was another similar CR Req 4.1-12 (last seen in version r6 of this doc) which has now been removed as it is covered by this CR.				

4.2. Application related requirements

Req 4.2-1	Showing documents to end users – service providers	Agreed	1	UC6.8

The DVB-I System shall enable service providers to show documents to end-users, to obtain agreement and to remember that agreement (or lack of agreement).

- It shall be possible for the documents and the mechanism by which they are shown to the user and by which agreement is obtained to be branded by the service provider.
- It shall be possible for the documents shown to the user to include a login or sign-on to either that service provider's offering or some kind of single sign-on scheme where the service provider participates.
- It shall be possible for documents to be shown to the user on the first occasion a user selects a service from that service provider and/or every time the user selects a service from that service provider if they have not agreed to what is necessary.

NOTE: Such agreements may govern access to a service list, to one or more services, or to different content or content formats delivered by a service.

Req 4.2-2	Showing documents to end users – operators and platforms	Agreed	1	UC6.7

The same as immediately above except with service providers replaced by operators or platforms. It shall be possible for this to happen when the corresponding service list is installed and regions (etc) are configured.

NOTE: Such agreements may govern access to a service list, to one or more services, or to different content or content formats delivered by a service.

Req 4.2-3	Withdrawal of agreement	Agreed	2	UC6.7, UC6.8

The DVB-I System shall enable users to withdraw agreement to documents from service providers, operators or platforms.

NOTE: Such agreements may govern access to a service list, to one or more services, or to different content or content formats delivered by a service hence withdrawal of agreement may mean loss of access.

Req 4.2-4	Update of agreement	Agreed	2	UC6.7, UC6.8

The DVB-I System shall enable service providers, operators or platforms to update their documents and either require the user to agree again or provide a notification to the user of the update. This should support implementations where the prompt for agreements starts gently and progressively gets stronger over time and users are only denied access to content if all prompts so far have been ignored.

Req 4.2-5	User interaction on service list installation	Agreed	1	UC6.7

The DVB-I System shall enable user interaction to be defined that applies to all services in a service list. Specifically;

- It shall be possible to define user interaction that happens when the service list is installed (i.e. at the same time as target regions are configured).
    - It shall be possible to indicate that the user interaction resulted in a conclusion that the service list installation is not to continue (e.g. the user refused terms and conditions)
    - It shall be possible to remember a result from the user interaction (e.g. a token or identifier assigned by a network server).
- It shall be possible to define user interaction that the end-user is able to initiate should they wish to withdraw agreement or consent at some later time.
- There shall be a mechanism to allow re-triggering the installation user interaction if / when there are changes in terms and conditions or personal data processing statements such that previous agreement is no longer sufficient.
- The user interactions shall be able to include showing significant text from the service list provider to the user and obtaining agreement.
- The user interactions shall be able to be branded by the service list provider.
- The user interactions shall be able to include login / single sign-on without requiring the selection of specific protocols to be included in DVB-I clients.
- The user interactions shall be able to be realised by linked applications including but not limited to generic HTML5.

Req 4.2-6	User interaction before presenting media of a service	Agreed	1	UC6.8

The DVB-I System shall enable user interaction to be defined that happens before the media of a service is presented where the presentation is done by the native DASH player.

- It shall be possible to remember that the user interaction has happened and any result, and not repeat it. It shall be possible to time-limit this, e.g. so that the results of the interaction are not remembered more than 48 hours.
- It shall be possible to indicate that the user interaction resulted in a conclusion that the service presentation is not to continue (e.g. the user refused terms and conditions)
- It shall be possible to have the same user interaction on a set of related services within the service list with a common result and not repeat it once for each service within the set.
- The user interaction shall be able to be realised by linked applications including but not limited to generic HTML5.
- It shall be possible to combine this feature with the existing “application with media in parallel” such that a service has one linked application run before media is presented (if not already run) and a different linked application run once media is being presented.

Req 4.2-7	Modifying media presentation based on results of user interaction	Agreed	1	UC6.7, UC6.8
The DVB-I System shall enable all necessary information resulting from a user interaction to be passed to the server returning the DASH MPD and should enable that information to be passed to the server returning the media segments. For example, the linked application includes a login. The results of a successful login are an identifier or token generated in the network and returned to the DVB-I client. The identifier is appended to the request for the DASH manifest such that the server responding to that request can match the request to a user that previously logged in. The solution should be as close to generic HTML5 as reasonably possible.				

Req 4.2-8	Signalling of Applications	Accepted	1	UC6.19
The DVB-I System shall enable the service provider's home page (such as a player app) to be launched through some user interaction, for example from the content guide or channel list. It shall be possible to include a name, a free text description and an icon that can be used in the receiver's UI.				

4.3. Customisation related requirements

Req 4.3-1	Service Discovery Customisation	Agreed	1	UC6.5
The DVB-I System shall enable customized queries and responses for elements of DVB-I Service Discovery (e.g., service list, playlist, content guide). Customized queries and responses serve for customization based on user/group (profile/ ID …) or based on specific properties (e.g., signing in case of object-based media) The specifications shall be written in a way that customized queries are only performed when interoperability is given between client and server in normal operation. NOTE: Properties referred to above include user settings / preference but how they are retrieved is out of scope of this CR.				

4.4. Accessibility related requirements

Req 4.4-1	Consistent component selection	Agreed	1	UC6.1
As far as it reasonably practical, the DVB-I System shall enable type 1.2 applications to invoke terminal / DVB-I client UI for component selection of accessibility features including but not limited to subtitles, audio language and accessible audio components. This covers the case of different services and different service instances within a service.				

4.5. Security of Service Lists

Req 4.5-1	Protecting the second level domain of a CSR	Agreed	1	UC6.9
The DVB-I System shall enable the use of mechanisms for authenticing Domain Name lookups for servers in DVB-I deployments, including but not limited to requests for Service List Discovery, Service Lists, Content Guide data and DVB-DASH MPDs and segments. Note: relevant technologies include DNSSEC.				

Req 4.5-2	Protecting the host of the CSR which is serving the ServiceListEntryPointsResponse	Agreed	1	UC6.10
The DVB-I System shall enable a Service List Registry to be available at multiple URLs. The DVB-I System shall also enable Service List Entry Points to be delivered using a CDN. Note: these requirements are intended to enable the deployment of mirror servers for redundancy, and scalability to support very large numbers of users. In addition to any specification updates required, the TM is also requested to consider writing guidelines around these topics.				

Req 4.5-3	Protecting the Servicelist host	Agreed	1	UC6.12
The DVB-I System shall enable the signalling of multiple URLs for each Service List in a list of Service List Entry Points returned by a Service List Registry. The DVB-I System shall also enable Service Lists to be delivered using a CDN. Notes: 1. these requirements are intended to enable the deployment of mirror servers for redundancy, and scalability to support very large numbers of users. In addition to any specification updates required, the TM is also requested to consider writing guidelines around these topics. 2. TM is requested to consider Caching issues.				

Req 4.5-4	Protecting the image service	Agreed	1	UC6.14
The DVB-I System shall enable DVB-I clients to authenticate images signalled in Service Lists and Content Guides. Note: this could be achieved by embedding images, or the signature of each image, in a Service List or Content Guide metadata, which is authenticated according to requirement 4.5-11.				

Req 4.5-5	Protecting the AIT signalling	Agreed	1	UC6.15
The DVB-I System shall enable DVB-I clients to authenticate AIT files signalled in Service Lists.				

Req 4.5-6	Protecting the XML Playlists and DASH manifests	Agreed	1	UC6.16
The DVB-I System shall enable DVB-I clients to authenticate XML Playlists and DASH manifests signalled in Service Lists.				

Req 4.5-7	Providing a content security policy	Agreed	1	UC6.17
The DVB-I System shall enable the use of techniques that detect and mitigate Cross-Site Scripting (XSS) and data injection attacks. Note: the TM is requested to consider the Content Security Policy [3] feature of HTML5 (https://content-security-policy.com/) as a possible solution for this requirement.				

Req 4.5-8	Providing Strict Transport security	Agreed	1	UC6.18
The DVB-I System shall enable servers to indicate that services should only be accessed over HTTPS. Note: the TM is requested to consider the HTTP Strict-Transport-Security [4] header as a possible solution for this requirement.				

Req 4.5-9	Authenticating service list entry points and service lists without encryption	Agreed	1	UC6.9, UC6.11, UC6.13
The DVB-I system shall enable authentication of service lists entry points and service lists without encryption, independent of how they are stored or distributed. It shall enable service list providers to operate in ways which ensure that, should an attacker compromise a service list registry or service list server and modify a service provider list or service list, it is possible for DVB-I clients to detect that modification. Within the limitations of XML, clients supporting earlier versions of the DVB-I specification should still be able to access such a service list registry or service list. EXAMPLE: A service list registry or service list provider chooses to ensure that all changes to their service list entry points or service list require physical involvement of one or more human beings. (I) Setting up any kind of PKI including generating and distributing certificates is outside the scope of this requirement and is outside the scope of DVB except if work on a CSR would be taken further. (I) The XML Digital Signature Specification adds signature elements in a different XML namespace that would be ignored by DVB-I clients using namespace aware XML parsers.				

4.6. Icecast streaming requirements

Req 4.6-1	IceCast based streaming services	Agreed	2	UC6.21
The DVB-I System shall define an informative method to replay an Icecast livestream with OtherDeliveryParameters.				

4.7. Timeline requirements

Req 4.7-1	Timeline	Agreed	2	UC?
There are no specific timeline requirements, but if implementation of any Commercial Requirements are likely to significantly delay the publication of the enhanced Specification(s), TM is requested to discuss this with CM.				

4.8. V&V requirements

Req 4.8-1	Verification & Validation	Agreed	2	UC?
V&V requirements will be developed once the specification work has progressed significantly in TM.				

5. Expected technical work

5.1. Impact on existing specifications or need for new ones

It is expected that the following Specifications will need updates to fulfil these Commercial Requirements:

- DVB-I Service Discovery and Programme Metadata Specification, A177
- DVB-I Implementation Guidelines, A184
- DVB-DASH (MPEG-DASH Profile for Transport of ISO BMFF Based DVB Services over IP Based Networks), ETSI TS 103 285

Decisions about which Specification(s) will be updated is the responsibility of the DVB Technical Module.

6. Annex: Use cases and issues (informative)

6.1. Consistent Component Selection

Use Case Title	Consistent Component Selection
Description	Based on recent notes that many DVB-I services may need to be implemented as linked applications which are responsible for a number of functions (e.g., user privacy consent, login, subscriber and DRM management, …), including the A/V rendering of the service within the application (for type 1.2 applications). This presents an inconsistency between: Services delivered by IP using linked applications (type 1.2) and Services delivered by RF Service instances delivered by IP using linked applications (type 1.2) and the corresponding Services instances delivered by RF In both of these situations, the UI for control and selection of A/V components will be managed either by the terminal (for RF) or by the linked (type 1.2) application. At a minimum, the key sequences may be the same, and UI layout may be similar but likely the placement locations, colours, fonts etc. would be inconsistent. On some TV devices the divergence between the native TV UI for component selection would be very different from the applications. This inconsistency of UI is problematic for end users to understand: Some services will have one mechanism/UI for altering subtitles and audio/audio description (as presented by terminal), and others will have a variety of mechanisms/UI depending on the application authors intention. For services with mixed service instances, depending on the service instance being rendered at the time, different UI will be presented even within the same service. This is not ideal for consumers and should be addressed as far as is possible. As an observation, applications that can read the default component settings from the terminal are likely to be HbbTV applications, whereas pure HTML5 application environments are probably unable to surface the default terminal settings to an application.

6.2. DRM: License Acquisition

Use Case Title	DRM: License Acquisition
Description	A Broadcasters / Service Provider is providing one or several DVB-I Channel (s) as part of a “Broadcaster” service list, with user authentication (sign in) and DRM. Options are: • Licence acquisition done by a HbbTV application (type 1.2), which handles authentication and playback of DRM-protected content. • Licence acquisition done by a HTML5 application (type1.2), which handles authentication and playback of DRM-protected content.

- Licence acquisition done by a HbbTV application (type 1.2), which handles authentication, playback of DRM-protected content and the broadcaster application (red button)
- Licence acquisition (authentication and DRM licensing) should also be possible by “native DVB-I” without starting a linked application.

Notes:

a) b) c) have been tested in the German and Italian DVB-I Pilot Projects

relating to d.: the current specification does not provide a solution for a “native DVB-I” user authentication

the term “Licence acquisition” covers 1) user authentication (sign in) per Token activation plus 2) DRM licensing; however also use cases where DRM is needed without user authentication (sign in) might be considered by Broadcasters / Service Providers

User Journey: Once a DVB-I service list has been installed and the user selects a DRM protected service, on the first occasion a UI asks for authentication (sign in). If the user signs in, the service (s) from that service provider are activated by the service provider per token verification. If a user has not agreed to what is necessary, the same authentication UI will be shown every time the user selects a service from that service provider.

HbbTV service specific broadcaster applications (red button) shall be possible for HbbTV compliant devices. (note: based on the current specification, it is not possible to load a HbbTV broadcaster applications in addition to “DRM” apps type 1.2; uc 1a) and uc 1b))

In line with the EU portability regulation, which regulates the unrestricted access to (paid) subscribed online content, GEO-restrictions based on individual content rights may occur to the user (“blacking“ of individual programs/content in case the distribution is not authorized for specific countries). If a user is logged in and DRM is handled by a linked application - see use cases 1a) 1b) 1c) - Broadcasters / Service Providers can manage GEO-restrictions in the player, by running a license check (maybe followed by a license change) at each program start. If Licence acquisition is done by “native DVB-I” without starting a linked application - use case 1d) - alternative options for sign in and license checks must be considered. (note: the current specification does not provide a solution for a “native DVB-I” user authentication (sign in) – see above; a potential solution, to be added in the spec, could be: Service Instances of a DVB-I service list should additionally contain a link to a Service Operator license acquisition website, which then handles the Authentication process,)

As there might be different rights per consecutive content, licenses shall not be stored in a persistent way (License cache).

Tokens for authentication can be cached, so that the user does not have to sign in again each time he selects the same DRM protected service.

While private Broadcasters / Service Provider need the options for user authentication (sign in) and DRM as described above, Public Broadcasters usually prefer streaming their services as “native DVB-I”, without using an application.

6.3. DRM: Single Sign On (single platform operator)

Use Case Title	DRM: Single Sign On (single platform operator)
Description	A Platform operator is managing single sign in for some Broadcasters / Service Providers of a "Broadcaster" DVB-I Service List, while DRM is handled by the Broadcasters / Service Providers: User Journey: Once a DVB-I service list has been installed and the user selects a DRM protected service from a particular Broadcaster*, on the first occasion a UI asks for authentication (sign in). This happens for every participating Broadcaster. If a user has not agreed to what is necessary, the same authentication UI will be shown every time the user selects a service from a Broadcaster. The backend of the platform operator communicates with the backend of the Broadcaster(s) to assure a single sign in. HbbTV service specific broadcaster applications (red button) shall be possible for HbbTV compliant devices. (see above) *2nd option: DVB-I UI during Service list installation asks for authentication (sign in). (note: the current specification does not provide a solution for a Platform operator user authentication)

6.4. DRM: Single Sign On (multiple platform operators)

Use Case Title	DRM: Single Sign On (multiple platform operators)
Description	One or more Platform operators are managing single sign in and DRM for one up to all Broadcasters / Service Providers of a "Platform operator" DVB-I Service List: **User Journey:** Once a DVB-I service list has been installed and the user selects a DRM protected service*, on the first occasion a UI asks for authentication (sign in). If the user signs in, the service (s) from that platform operator are activated by the platform operator per token verification. If a user has not agreed to what is necessary, the same authentication UI will be shown every time the user selects a service from that platform operator. HbbTV service specific broadcaster applications (red button) shall be possible for HbbTV compliant devices. (see above) *2nd option: DVB-I UI during Service list installation asks for authentication (sign in). (note: the current specification does not provide a solution for a Platform operator user authentication)

6.5. Service Discovery Customisation

Use Case Title	Customisation
Description	Background: The following describes examples of user journeys, whereas it is understood that the user journey is left to the IRD manufacturers. **User journey A:** Customisation is based on "profile_id" / "id" / "uuid" etc. Client submits request with profile id as query, device id and receives a customized response (see FAST submission CM-I 273) 1) Installation of IRD or mobile app (out of scope of DVB-I) which may include: a. Acceptance of terms and conditions b. Registration c. Generation or obtention of "profile" / "id" / "uuid" in case there is none preinstalled 2) When requesting elements of DVB-I Service Discovery, the IRD/mobile client sends his "profile" / "id" / "uuid" as argument for the request. Request only takes place where server is interoperable (no "trial and error"). 3) Review on terms & conditions may occur subsequently NOTES: • No application and WebView is required and as the above could be embedded in a lightweight implementation using a native UI, but it is not excluded. • there may be a combination of arguments Another example is when a sessiontoken is generated. After 1) is completed, an IRD initiates a session (out of scope of DVB) based on credentials and obtains a sessiontoken. This sessiontoken is used throughout the complete viewing session (based on profile and credentials). **User journey B:** Customisation based on profile, personal, etc. Client submits query with properties according to device or customer preference (e.g. visually impaired content) and receives corresponding response. 1) When requesting elements, the client sends one or several properties as argument for the request. Customized Requests only take place where server is interoperable (no "trial and error"). 2) The use of customized arguments is left to the IRD. There may be multiple conditions where the IRD initiates customized queries. Examples for signing or maturity: a. An accessibility menu that prioritizes services with signing b. A filter on the program guide that can be set on signing programs. c. An IRD based on maturity level that is set (on the personal profile or the default profile) will only request programs and a service list that contains corresponding services. NOTES: • No application, any application and WebView is required and could be embedded in a lightweight implementation using a native UI, but it is not excluded.

	• A combination of several arguments is possible. For example: signing and maturity level query. • Some operators / authorities require that specific adult programs do not appear in the program guides

6.6. DRM without an application

Use Case Title	DRM without an application
Description	User is capable to access to such FTV services that are DRM protected with the same user-experience as in DTT, i.e. without any need to load an application first, with no need to eventually perform user authentication, with a universal reach on any device which is DVB-I compliant.

6.7. User interaction on service list installation

Use Case Title	User interaction on service list installation
Description	A service list provider (e.g. a platform or operator) needs to obtain one or more of the following before any services from their service list are made available to users. The user's agreement to terms and conditions Consent from the user for processing personal data as defined in GDPR User login / authentication potentially single-sign on (SSO) Some form of subscription or payments from the user The text of the terms and conditions and/or description of personal data processing would be provided by the service list provider. The UI around the text would be provided by the service list provider, would use their terminology and be branded by them. If the user does not agree or give consent then service list provider is able to abort the process of installing the service list. If the user does agree or give consent, they are able to withdraw this if they so wish at any later time. When the terms and conditions change, the service list provider is able to re-trigger the process of obtaining agreement. Similarly, if the description of personal data processing changes. The service provider is able to start this sometime in advance of when it's really needed and progressively increase the strength of the request to the user as the time when it's really needed gets closer. The service list provider is able to create some kind of token following a successful login which, when the user selects a service from that service list, would be passed to the network servers involved in offering the selected service.

6.8. User interaction before presenting media of a service

Use Case Title	User interaction before presenting media of a service
Description	The reasons listed for user interaction on "User interaction on service list installation" also apply for a single service or a set of related services within the service list. e.g. a set of services from the same organisation.

6.9. Protecting the second level domain of a CSR

Use Case Title	Protecting the second level domain of a CSR
Description	An attacker can use DNS poisoning to redirect the DNS requests to the service list registrar's domain to his own and thus gain control over which service lists are made available to the client.

6.10. Protecting the host of the CSR which is serving the ServiceListEntryPointsResponse

Use Case Title	Protecting the host of the CSR which is serving the ServiceListEntryPointsResponse
Description	For example, if an attacker carries out a DDoS attack on the service list registrar's servers and the service list registrar cannot be reached, it must be ensured that it has a redundant structure and can deal with such attacks. If this is not the case, DVB-I clients may not be able to perform service discovery and will not receive any service list information.

6.11. Protecting the ServiceListEntryPoints Response against compromise

Use Case Title	Protecting the ServiceListEntryPoints Response against compromise
Description	There must be a trust relationship between the DVB-I client and the service list registrar. This can be achieved using different means, for example through a hard-coded CSR URL in the client. However, if the ServicelistEntryPoints Response cannot be accessed via the Internet because it is transmitted as an asset via DVB-NIP, for example, no trust relationship can be established.

6.12. Protecting the Servicelist host

Use Case Title	Protecting the Servicelist host
Description	For example, if an attacker carries out a DDoS attack on the service list host's servers and the service list cannot be reached, it must be ensured that it has a redundant structure and can deal with such attacks. If this is not the case, DVB-I clients will not receive any service list information and might stop working

6.13. Protecting the Servicelist against compromise

Use Case Title	Protecting the Servicelist against compromise
Description	If an attacker compromises the service list host, dangerous content would be served with the service list. URLs to DASH streams, for example, would point to the attacker's goals and the content guide would play out the attacker's EPG data.

6.14. Protecting the image service

Use Case Title	Protecting the image service
Description	If an attacker compromises the image service, dangerous content would be served with the service list and content guide. Incorrect image content (image defacement) or dangerous exploits could be delivered with the images.

6.15. Protecting the AIT signalling

Use Case Title	Protecting the AIT signalling
Description	If the AIT files are delivered separately and they are compromised, this allows an attacker to launch their own apps using application signaling if these URLs are compromised. This can happen to 1.1 and 1.2 signalled apps in the servicelist and also at the Boxset lists and Programinfo requests within the contentguide.

6.16. Protecting the XML Playlists and DASH manifests

Use Case Title	Protecting the XML Playlists and DASH manifests
Description	An attacker can propagate their own URLs in the XML playlist or content in DASH manifest if the are compromised. The DASH stream URLs or segments can point to content from the attacker.

6.17. Providing a content security policy

Use Case Title	Providing a content security policy
Description	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross-Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft, to site defacement, to malware distribution.

6.18. Providing Strict Transport security

Use Case Title	Providing Strict Transport security
Description	HTTP Strict Transport Security (HSTS) is a policy mechanism that helps to protect websites against man-in-the-middle attacks such as protocol downgrade attacks and cookie hijacking. It allows web servers to declare that web browsers (or other complying user agents) should automatically interact with it using only HTTPS connections, which provide Transport Layer Security (TLS/SSL), unlike the insecure HTTP used alone. HSTS is an IETF standards track protocol and is specified in RFC 6797.

6.19. Service App launch from EPG

Use Case Title	Service App launch from EPG
Description	**Purpose**: Add DVB-I metadata to signal the availability of Service App of content/service providers to enable options to directly **"launch service app/player"** from EPG (without deep-linking to a specific Programme) or from other menu interfaces such as channel list / mini-guide etc. **Scenario:** Viewer is browsing the EPG or mini-guide or Channel list and now would like to directly launch app/player of a service without selecting the service/channel and without deep-linking to any programme in the EPG. **Problem:** Currently it is **Not possible** to provide direct link/option to "launch service app/player" from EPG / mini-guide / channel list etc. due to the following limitations of current linked applications: Currently the linked applications (as type 1.1 / 1.2 or Type 2) which are signaled at the service level **are displayed/launched when that service is selected or in active state.** These linked applications **cannot be used to directly launch service apps/players from within EPG/mini-guide/Channel list** etc because: • **Type 1.1 -** App with media in parallel : An associated application to be started in parallel with commencing presentation of any A/V media. • It is like a Red button-type app and not the direct link to content provider's player page. Such links cannot be used in the EPG /min-

guide/Channel list to provide “launch player” option as the underlying service might not be selected so the red button-type application cannot be launched.

- **Type 1.2** - App controlling media presentation: An associated application that controls media presentation or has no media.
    - App is presented as soon as the channel/service is selected. Therefore, not suitable for content providers/PSBs which have linear TV channels (broadcast and/or IP).
- **Type 2** - App for outside availability period: An associated application to be started outside the availability period of a service instance.
    - Time/availability bound.

Solution:

Create additional type of linked application metadata which can signal the availability of on-demand applications of content/service providers at the service level

- Additional HowRelated value to be created to signaling on-demand applications at RelatedMaterial level of a service

Such metadata can be used by the DVB-I client to provide menu options to the viewer to “launch” service apps/players of content providers directly from Channel List /EPG /mini-guide/other interfaces.

Benefits:

Enable the user to directly launch service app/player which is linked to the service without selecting/tuning to that service while being in DVB-I mode - this demonstrates the environment where hybrid and app world co-exist.

Advantages:

- ✓ Content provider apps/players can be accessed directly via EPG/Channel list/mini-guides etc
- ✓ Engagement with viewer is maintained
- ✓ Attracts more viewers to launch apps/players
- ✓ DVB-I client providers can use the functionality to create user-friendly interfaces to improve usability and provide seamless user experience

6.20. Security user experience

Use Case Title	Security user experience
Description	Currently the DVB-I specification A177r5 does not include consideration of any security requirements. It is intended that this be addressed in the next/future revision of A177. The first challenge will be to specify security requirements that can be easily implemented to protect the whole DVB-I ecosystem while maintaining the required user experience at least equivalent to today's TV experience. The second challenge relates to the global nature of the internet, particularly for IP delivered TV. The specification should therefore not be restrictive to support this diverse maket place. This will imply the need for a good, flexible, interoperable solution. Security could follow into four broad categories that are protection of: 1. Content (DRM) 2. Devices (RoT, Bode code authentication …) 3. Service infrastructure (signing of service registry etc.) 4. Applications (TEE, Code authentication …) Any of those categories that are breached could lead to a very negative market view of the DVB-I specification so getting this right is fundamental to the future success of DVB-I. This Use Case focuses mainly on the protection of Content, and this content might be from various providers that are a mix of Unencrypted (FTV – free to view) channels plus one of the following possible DRM encryption scenarios: 1. Channels that are DRM encrypted by one DRM provider i.e. single key source, single DRM scheme (e.g. ToPlay or PlayReady or Widevine or …) 2. Channels that are DRM encrypted with Common key for more than one DRM scheme i.e. a 'Service Aggregator' provides 'Retail Key' for consumption by more than one DRM provider (e.g. ToPlay and PlayReady and Widevine and FairPlay etc.) 3. Channels that are DRM encrypted with multiple DRM keys for multiple DRM schemes (e.g. one to one relationship between key owner + DRM scheme) Of course, Commercial DRM solutions already exist, prior to the creation of any DVB-I content protection CRs. There may be some limitations to integrating those solutions within a DVB-I framework. This could be satisfied by a well-defined solution that takes these limitations in to account as much as possible. Content encryption generally relies on a common encryption (CENC) scheme, however license acquisition methods (and the subsequent availability of a decryption key) vary from DRM system to DRM system Different business models are likely to have different considerations on license retention that need to be considered: ✓ In some situations, license persistence is important as you don't want to have keep acquiring licenses every time you zap away from a channel (or collection of channels) and come back again

	✓ In other situations, the license should be obtained each time the channel/service is acquired to ensure that the user still has the necessary rights to the programme. ✓ Most often, the license will identify an expiration time for the encryption key (generally every 24 hours) ✓ Replaying already aired programs (for example through DVB-I Box Set solution) may have a different license/key management approach. ✓ DVB-I has support for 'SubscriptionPackages' which may include multiple services and/or selected instances of services. At present there is no constraint or expectation placed on the subscription package structure, but this could be taken into consideration Another consideration is that a DVB-I solution is a collection of TV channels only curated through the service discovery system, there is no single point of aggregation of content and security. Content encryption and provisioning of keys is generally the responsibility of the service provider (but *may* be delegated to some 'downstream' entity)

6.21. Playback of non-standardised HTTP streaming for audio

Use Case Title	IceCast based streaming services
Description	The DVB-I client is to play back a radio live stream found in the service list. A service list includes several options for signalling additional formats for the delivery of media. The service instance for the Icecast service can: • include an OtherDeliveryParameters element with values indicating and referencing the Icecast stream for use by a native player function. Icecast delivered streams can co-exist to some extent as described in clause XX.4.

7. History

Reference	Month Year	Milestone
C108	November 2023	First BlueBook publication (Internal document CM2254r1 / CM-I0325r15 redacted for publication)