DASH-IF IOP-1 V5.0.0 (2022-06)

DASH-IF Interoperability Points;
Part 1: Overview, Architecture and Interfaces

DASH Industry Forum

3855 SW 153rd Dr.
Beaverton, OR 97003 - USA

Email : admin@dashif.org

Important notice

The present document can be downloaded from:
http://www.dashif.org/guidelines

Contents

Intellectual Property Rights

Disclaimer

This is a document made available by DASH-IF. The technology embodied in this document may involve the use of intellectual property rights, including patents and patent applications owned or controlled by any of the authors or developers of this document. No patent license, either implied or express, is granted to you by this document. DASH-IF has made no search or investigation for such rights and DASH-IF disclaims any duty to do so. The rights and obligations which apply to DASH-IF documents, as such rights and obligations are set forth and defined in the DASH-IF Bylaws and IPR Policy including, but not limited to, patent and other intellectual property license rights and obligations. A copy of the DASH-IF Bylaws and IPR Policy can be obtained at http://dashif.org/.

The material contained herein is provided on an "AS IS" basis and to the maximum extent pe mitted by applicable law, this material is provided AS IS, and the authors and developers of this material and DASH-IF hereby disclaim all other warranties and conditions, either express, implied or statutory, including, but not limited to, any (if any) implied warranties, duties or conditions of merchantability, of fitness for a particular purpose, of accuracy or completeness of responses, of workmanlike effort, and of lack of negligence.

In addition, this document may include references to documents and/or technologies controlled by third parties. Those third-party documents and technologies may be subject to third party rules and licensing terms. No intellectual property license, either implied or express, to any third-party material is granted to you by this document or DASH-IF. DASH-IF makes no warranty whatsoever for such third-party material.

Note that technologies included in this document and for which no test and conformance material is provided, are only published as candidate technologies, and may be removed if no test material is provided before releasing a new version of this guidelines document. For the availability of test material, please check https://www.dashif.org.

Foreword

This Technical Specification (TS) has been produced by the DASH-IF Technical Working Group.

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in deliverables except when used in direct citation.

Executive summary

This part of DASH-IF Guidelines provides an overview of DASH services, the architecture and introduces interfaces. It also provides an overview of basic functions and introduces the remaining parts of DASH-IF Guidelines.

Introduction

The present document is Part 1 of a multipart set of documents, collectively called “DASH-IF Interoperability Points, V5.0” (IOP V5). Version 5 of the DASH-IF IOP is defined for usage with the MPEG DASH specification (ISO/IEC 23009-1 [1]) and further constrained to deliver media formatted according to the MPEG CMAF Specification (ISO/IEC 2300-19 [3].

The goal of the DASH-IF IOP specifications is facilitating a common interoperability of media and media services at key points of the delivery chain from the server to the client.

The following is a list of the parts of IOP V5 at the time of publication of the present document:

1. Overview, architecture and interfaces (this document)

2. Core principles and CMAF mapping
3. On-demand services
4. Live and low-latency live services
5. Ad insertion
6. Content protection
7. Video
8. Audio
9. Text
10. Events
11. Additional functionalities
12. Conformance and reference tools

1 Scope

The present document provides an overview of the different features in DASH-IF Interoperability Guidelines. In particular, this document provides a reference architecture together with relevant interfaces and functional blocks.

Any identified bugs or missing features may be submitted through the DASH-IF issue tracker at https://github.com/Dash-Industry-Forum/DASH-IF-IOP/issues.

2 References

2.1 Normative 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, DASH-IF cannot guarantee their long-term validity.

The following referenced documents are necessary for the application of the present document.

[1] ISO/IEC 23009-1:2022 “Information technology -- Dynamic adaptive streaming over HTTP (DASH) – Part 1: Media presentation description and segment formats”

[2] ISO/IEC 14496-12:2021 “Information technology -- Coding of audio-visual objects -- Part 12: ISO base media file format”

[3] ISO/IEC 23000-19:2022 “Information technology -- Multimedia application format (MPEG-A) — Part 19: Common media application format (CMAF) for segmented media”

[4] DASH-IF IOP v5, Part 12 “DASH-IF IOP: Conformance and Test Tools”

[5] IETF RFC 5246 “The Transport Layer Security (TLS) Protocol, Version 1.2”

[6] IETF RFC 6265 “HTTP State Management Mechanism”

[7] IETF RFC 7230 “Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing”

[8] IETF RFC 7231 “Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content”

[9] IETF RFC 7232 “Hypertext Transfer Protocol (HTTP/1.1): Conditional Requests”

[10] IETF RFC 7233 “Hypertext Transfer Protocol (HTTP/1.1): Range Requests”

[11] IETF RFC 7234 “Hypertext Transfer Protocol (HTTP/1.1): Caching”

[12] DASH-IF IOP v5, Part 2 “DASH-IF IOP: Core Functionalities”

[13] DASH-IF IOP v5, Part 6 “DASH-IF IOP: Content Protection and Security”

2.2 Informative 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, ETSI cannot guarantee their long-term validity.

The following referenced documents are not necessary for the application of the present document, but they assist the user with regard to a particular subject area.

[i.1] CTA 5003 “Device Playback Capabilities Specification”
[i.2] DASH-IF: Content Protection Information Exchange (CPIX)
[i.3] DASH-IF Guidelines for Implementation: DASH-IF Interoperability Point for ATSC 3.0
[i.4] DASH-IF Guidelines for Implementation: DASH-IF SAND Interoperability
[i.5] DASH-IF Implementation Guidelines: Token-based Access Control for DASH (TAC)
[i.6] DASH-IF Live Media Ingest Protocol
[i.7] IETF RFC 2616 “Hypertext Transfer Protocol -- HTTP/1.1”
[i.8] 3GPP TS 26.346 "Multimedia Broadcast/Multicast Service (MBMS); Protocols and codecs"
[i.9] Guidelines for Implementation: DASH-IF Interoperability Point for ATSC 3.0
[i.10] ETSI TS 103769 "Adaptive media streaming over IP multicast."

3 Definition of terms, symbols and abbreviations

3.1 Terms

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

3.2 Symbols

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

3.3 Abbreviations

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

BMFF	Base Media File Format
DASH	Dynamic Adaptive Streaming over HTTP
DRM	Digital Rights Management
HTTP	HyperText Transport Protocol
IOP	InterOperability Point
ISO	International Standards Organization
MPEG	Moving Pictures Experts Group
RFC	Request for Comments
URL	Uniform Resource Locator
XML	eXtended Markup Language

4 Conformance and style

For more detailed guidance on conformance and additional interpretation of the conformance key words: “**shall**”, etc, please see DASH-IF IOP Part 12 [4] clause 4.

The following naming conventions apply in this document.

- Elements in an XML document are identified by an upper-case first letter and in bold face as **`Element`**. To express that an element **`Element1`** is contained in another element **`Element2`**, the following format is used: **`Element2.Element1`**. If an element's name consists of two or more combined words, camel-casing is typically used, e.g. **`ImportantElement`**. Elements may be present either exactly once, or the minimum and maximum occurrence is defined by `<minOccurs>` ... `<maxOccurs>`.

- Attributes in an XML document are identified by a lower-case first letter as well as they are preceded by an '@'-sign, e.g. `@attribute`. To point to a specific attribute `@attribute` contained in an element **`Element`**, one may write **`Elemen`**`t@attribute`. If an attribute's name consists of two or more combined words, camel-casing is typically used after the first word, e.g. `@veryImportantAttribute`. Attributes may have

assigned a status in the XML as mandatory (M), optional (O), optional with default value (OD) and conditionally mandatory (CM).

- Namespace qualification of elements and attributes is used as per XML standards, in the form of **`namespace:Element`** or `@namespace:attribute`. The fully qualified namespace is provided in the schema fragment associated with the declaration. External specifications extending the namespace of DASH are expected to document the element name in the semantic table with an extension namespace prefix.
- Variables defined in the context of this document are specifically highlighted with *italics*, e.g. *InternalVariable*.
- Structures that are defined as part of the hierarchical data model are identified by an upper-case first letter, e.g. Period, Adaptation Set, Representation, Segment, etc.

5 Architecture and interfaces

5.1 DASH-IF baseline architecture

A baseline architecture for DASH content distribution is provided in Figure 1. Content is provided in any format and then assumed to be encoded and prepared following the DASH Segment Formats as defined in ISO/IEC 23009-1 [1], in particular based on ISO BMFF as defined in ISO/IEC 14496-12 [2] and CMAF as defined ISO/IEC 23000-19 [3].

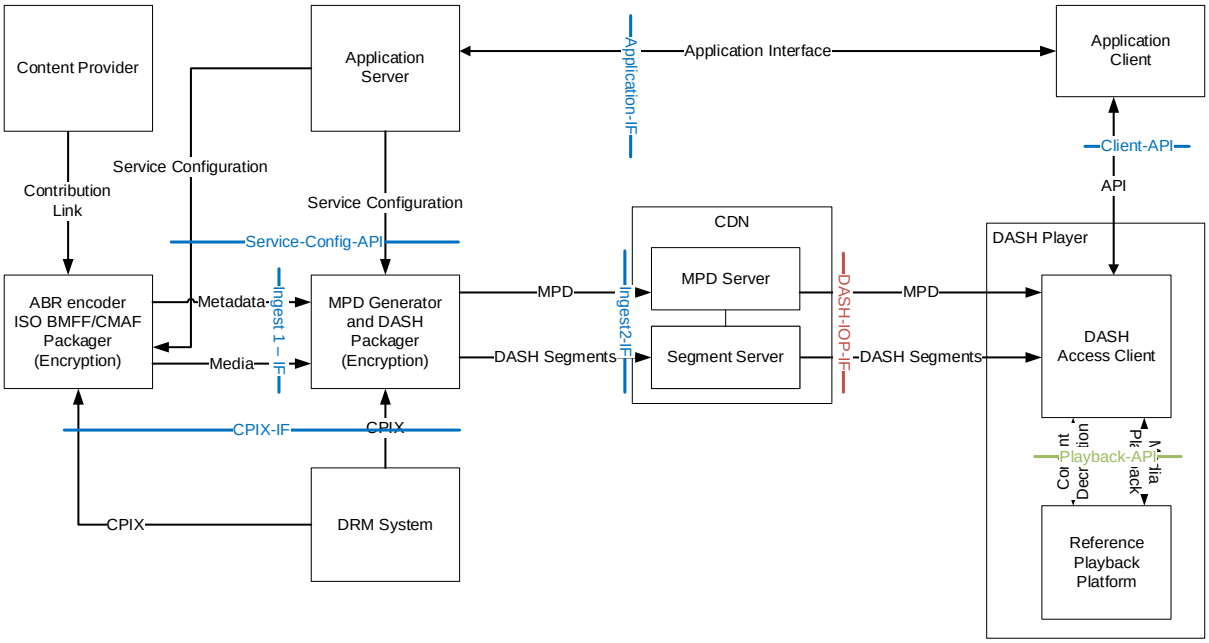

Figure 1 DASH-based distribution architecture

The following major components are identified:

- *ABR Encoder*: Adaptive Bitrate Encoder providing multiple equivalent versions of the same content in different qualities.
- *ISO BMFF/CMAF Packager*: An encapsulation and packaging that creates segmented media content that can be distributed through DASH and can be played back on a reference platform through well-defined APIs. In the content of the specification, and ISO BMFF/CMAF Packager is assumed. For details, refer to clause 5.2.
- *DASH Packager* and *MPD Generator*: An operation to add DASH formats and MPD signaling to create a DASH Media Presentation.
- *CDN*: A scalable distribution network supporting the delivery and caching DASH Resources.
- *DASH Access Client*: A client uses the MPD and the referenced resources to create a streaming experience to a user by using a reference playback platform

- *Application*: An application that controls the DASH access client by a set of well-defined APIs.

5.2 Interfaces

Figure 1 provides a set of interfaces which are explained in more details in Table 1.

Reference Point	Explanation
Ingest 1-IF	This interface is defined in the DASH-IF Live Media Ingest Specification. Ingest 1-IF present the first, interface 1, CMAF ingest, is based on fragmented MPEG-4 as defined in the common media application track format (CMAF). The interface uses the HTTP POST Method to transmit media objects from the ingest source to the receiving entity. Examples of live streaming workflows using these protocol interfaces are also presented. The protocol interfaces also support carriage of timed metadata and timed text. Guidelines for redundancy and failover are also included. For details, please check here: https://dashif.org/guidelines#dash-if-technical-specification-live-media-ingest
Ingest 2-IF	The second interface of the DASH-IF Live Media Ingest Specification is based on MPEG DASH and HLS as defined by ISO SC29 WG 11 and IETF. The interface uses the HTTP POST Method to transmit media objects from the ingest source to the receiving entity. Examples of live streaming workflows using these protocol interfaces are also presented. The protocol interfaces also support carriage of timed metadata and timed text. Guidelines for redundancy and failover are also included. For details, please check here: https://dashif.org/guidelines#dash-if-technical-specification-live-media-ingest
CPIX-IF	Details on the CPIX-IF are provided in a separate specification. The scope of this document is to define a Content Protection Information Exchange Format (CPIX). The CPIX document contains keys and DRM information used for encrypting and protecting content and can be used for exchanging this information among entities needing it in many possibly different workflows for preparing, for example DASH content or HLS content. The CPIX document itself can be encrypted, signed, and authenticated so that its receivers can be sure that its confidentiality, source, and integrity are also protected. For details, please check here: https://dashif.org/guidelines#dash-if-content-protection-information-exchange-format
DASH-IOP-IF	The main interface defined in the DASH-IF IOP guidelines in order to provide interoperability between a content provider offering DASH-based services on a CDN and a DASH client.
Application-IF	An interface typically available in an application that provides for example the entry point to the DASH service by providing a URL to an MPD.
Playback-IF	A reference interface between a DASH access client and a playback and decryption platform. This API is modelled against the HTML-5 video element and the Media Source Extensions with the restrictions in the CTA WAVE device playback API.
Service-Config-API	A network side API that allows an application provider to configure certain parameters of DASH-based streaming service. This configuration is used to statically and dynamically create the MPDs and updates thereof as well as manages the Segment data generation and distribution.
Client-API	An API between the application and the DASH client (both DASH access client and playback platform) in order to configure, control and monitor the service.

5.3 DASH reference client

In order to develop the interoperability guidelines, a reference client for playback is assumed as shown in Figure 2. The reference client is not a mandatory implementation, but is considered as a reference for developing the IOP guidelines as well as for service offerings.

The following basic workflow procedures are assumed:

- The DASH Reference client downloads, processes and presents a DASH Media Presentation by instruction of an application.
- The application can, in addition, configure the presentation of the media, can receive notifications on events, or can query the internal status of the DASH Player and Access Client.
- Several functions are provided in the DASH Access client that are typically necessary to process a DASH Media Presentation, including MPD processing, selection of Adaptation Sets and Download functions. More details are provided in the following
- A Media Playback Platform and content decryption module are used for secure decoding and presentation of the streamed media.

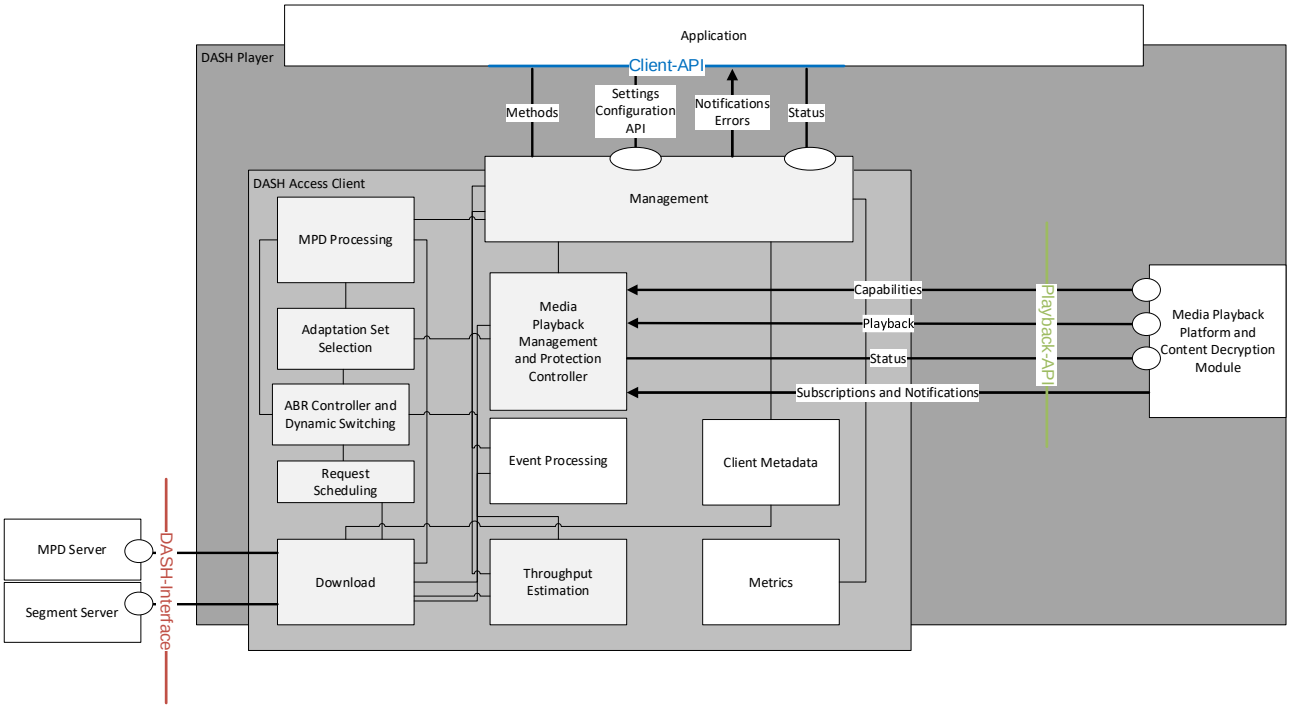

Figure 2 DASH reference client

The following functions are part of a reference client along with the key functionalities:

- *Application*: makes use of the DASH/Media Player to playback a DASH Media Presentation provided by an MPD. The application typically provides the MPD or a URL of the MPD to the DASH client.
- *DASH Player*: A complete player for the playback of a Media Presentation, including media playback platform and content decryption module.
- *DASH Access Client*: A part of the DASH Player that access and downloads the media from the network and makes use of Media Playback Platform and content decryption module for decoding and playback of DASH content.
- *Management*: Controls all internal processes and the communication with the application.
- *MPD Processing*: parses and processes the MPD and extracts the relevant information

- *Adaptation Set Selection*: selects the Adaptation Set based on user, environment and capability information
- *Dynamic Switching and Request Scheduling*: runs adaptive bitrate logic and triggers dynamic switching across Representations
- *Throughput Estimation*: estimates the throughput from a specific network/application server
- *Metrics Collection*: collects metrics in the streaming process and offers those to application in order to process and potentially also report to network entities.
- *Media Playback Management*: manages the media playback by moving downloaded information into media playback platform and also addresses handling of content protection and DRM related information
- *Media Playback Platform*: Plays back CMAF-based media content using well defined playback instructions.
- *Event Processing*: Processes DASH events and provides information to application.

Detailed APIs and methods to communicate with a DASH Reference client are implemented in the DASH-IF reference client. For a detailed description refer to part 12 of DASH-IF IOP [4].

Typically, DASH Players are not using specific media playback platforms, but rely on implementations of CMAF-capable playback platforms and decryption modules. More details on a CMAF capable playback platform are provided in DASH-IF IOP Part 2 [12]. Content security is accomplished in a device by two functions:

1. Key management by a digital rights management system (DRM), which authenticates a user or their device and authorizes decryption and playback of a media track on that device under control of the DRM client and under specific conditions, e.g. output protection, rental period, hardware root of trust, etc.
2. Decryption of an encrypted track using a specific decryption scheme.

Details on decryption functionalities are provided in DASH-IF IOP Part 6 [13].

Events received in DASH media need to be processed for client consumptions. For details, refer to DASH-IF IOP Part 10 [13].

5.4 DASH-IF IOP Parts

5.4.1 Part 1: Overview, Architecture and Interfaces

Part 1 (this document) provides an overview of the different features in DASH-IF Interoperability Guidelines. In particular, it provides a reference architecture together with relevant interfaces and functional blocks.

5.4.2 Part 2: Core principles and CMAF mapping

Part 2 provides the core principles of DASH including the data and timing model, as well as the mapping of CMAF data structures to DASH Media Presentations.

5.4.3 Part 3: On-demand services

Part 3 provides relevant requirements and recommendations when using DASH for On-Demand services.

5.4.4 Part 4: Live and low-latency services

Part 4 provides details on live service offerings, including low-latency services.

5.4.5 Part 5: Ad insertion and content replacement

Part 5 of DASH-IF IOP v5 provides guidelines for advertisement insertion in a MPEG CMAF based content serving workflow utilizing MPEG DASH as the delivery protocol. This part details the general architecture of an ad enabled content serving workflow along with the conditioning, packaging, and signalling requirements to enable both SSAI and SGAI insertion forms. This part defines guidelines for the creation, storage, and serving of ad content. In addition, this part provides informative references and recommendations for auxiliary content and ad systems involved in the ad insertion architecture.

5.4.6 Part 6: Content protection and security

Part 6 provides guidelines for encrypted content delivered in MPEG CMAF format protected by MPEG CENC. As MPEG DASH is used as the delivery protocol, this part makes the links between signaling that is within content and within the MPD. In addition, to this, this part describes mechanisms for supporting key rotation. It defines the Enhanced Clear Key Content Protection (ECCP), a content protection mechanism for DASH content which provides greater protection than TLS delivery, token authentication or Clear Key used individually. It also defines the DASH-IF XML schema with elements related to content protection.

5.4.7 Part 7: Video

Part 7 defines the CMAF Media Profiles and the DASH signalling for video tracks.

5.4.8 Part 8: Audio

Part 8 of DASH-IOP v5 describes the audio interoperability points for the DASH-IF ecosystem. Audio coding profiles, ISOBMFF packaging and MPD parameters are defined for these points of interoperability. Also defined is the application of audio Preselections as applied to object-based audio. Preselections may include audio components from one or more streams.

5.4.9 Part 9: Text

The present document defines the CMAF Media Profiles and the DASH signalling for text tracks, including subtitles and captions as well as open captions and subtitles in video tracks. This work was derived from IOP v4.3 but does not contain non-CMAF profiles. The use of “sidecar” files is not covered in the present document.

5.4.10 Part 10: Events

Part 10 includes requirements and guidelines for Event stream offerings and processing.

5.4.11 Part 11: Additional Functionalities

Part 11 includes additional functionalities relevant for interoperability, among others:

- Thumbnail tracks
- Query and Token Mechanisms
- Metadata Tracks

5.4.12 Part 12: Conformance and reference tools

Part 12 provides an overview of DASH-IF Reference and Conformance Tools. In particular the conformance software to verify service offerings, the dash.js reference client and the DASH-IF test assets are introduced.

5.5 Protocols

5.5.1 General

Servers and clients operating on the DASH interface defined in this document shall support the normative parts of HTTP/1.1 as defined in IETF RFC 7230 [7], IETF RFC 7231 [8], IETF RFC 7232 [9], IETF RFC 7233 [10], and IETF RFC 7234 [11].

Specific requirements and recommendations are provided in the clauses that follow.

Note: IETF recently obsoleted RFC 2616 [i.7] and replaced it with the five RFCs referred above. The changes are generally text clarifications, but in some cases additional constraints to address security or interoperability issues. Each new RFC contains details of the changes compared to RFC 2616. The IETF strongly recommends to reference and use the new RFCs that collectively replace RFC 2616. This version of DASH-IF IOP addresses this aspect.

MPEG-DASH explicitly permits the use of HTTPS as a scheme and hence, HTTP over TLS as a transport protocol as defined in RFC 5246 [5]. For more details refer to DASH-IF IOP Part 6 [13].

While DASH is inherently designed to operate on top of an HTTP-based network connection, the distribution of DASH formats and DASH Media Presentations is not limited to HTTP/TCP connections.

For example, the delivery over HTTP3/QUIC/UDP has gained significant interest recently. Secondly, the delivery of DASH formats over multicast and broadcast networks is quite common nowadays. Examples include the delivery of DASH via ATSC3.0 broadcast networks [i.9], DASH over 3GPP MBMS [i.8], or DVB-DASH over multicast ABR [i.10].

5.5.2 Server requirements and guidelines

HTTP Servers serving segments should support suitable responses to byte range requests (partial GETs).

If an MPD is offered that contains Representations conforming to the ISO BMFF On-Demand profile, then the HTTP servers offering these Representations shall support suitable responses to byte range requests (partial GETs).

HTTP Servers may also support the syntax using Annex E of 23009-1 [1] using the syntax of the second example in Annex E.3,

BaseURL`@byteRange="$base$?$query$&range=$first$-$last$"`

5.5.3 Client requirements and guidelines

Clients shall support byte range requests, i.e. issue partial GETs to subsegments as defined in RFC 7233 [10]. Range requests may also be issued by using Annex E of 23009-1 using the syntax of the second example in Annex E.3,

BaseURL`@byteRange="$base$?$query$&range=$first$-$last$"`

Clients shall follow the reaction to HTTP status and error codes as defined in clause A.7 of ISO/IEC 23009-1 [1].

Clients should support the normative aspects of the HTTP state management mechanisms (also known as Cookies) as defined in IETF RFC 6265 [6] for first-party cookies.

5.5.4 Transforming proxies and other adaptation middleboxes

A number of video transcoding proxies (aka "middleboxes") are already deployed on the wider Internet may silently transcode Representations. Specifically: a middlebox may see a video/mp4 response, transcode that video into a different format (perhaps using a lower bitrate or a different codec), then forward the transcoded video to the DASH client. This will break MPD and/or Segment Index based byte range operations, as those ranges are generally not valid in the transcoded video.

If such a threat is possible, one of the following approaches may be considered in order to prevent proxies from transcoding DASH Representations:

1. serve Media Presentations using encryption (e.g., HTTP over TLS, segment encryption or content protection),
2. serve Representations with Cache-Control: “`no-transform`"

In all cases the operational impacts on caching and implementations should be considered when using any of the above technologies.

In order to prevent middleboxes to manipulate the MPD, e.g. removing certain Representations or Adaptation Sets, the MPD may be securely transported by appropriate means, e.g. HTTPS.

5.6 Features

MPEG-DASH is defined as an extensible framework to support different deployment scenarios. Over time, additional functionalities were added. In addition, MPEG-DASH defines optional functionalities that may be relevant only for certain deployment scenarios. Based on this, DASH permits different deployment features.

In the context of the DASH-IF Interoperability specifications, such features are introduced. A feature typically consists of different aspects:

- the feature description, i.e. what it is used for and how can it be used
- the signalling of the feature in the MPD, i.e. how can the feature be enabled

- the content authoring requirements, i.e. what needs to be provided by the content authoring such that the DASH media presentation conforms to the feature

- the requirements for the client to support the feature

Features in a DASH media presentation may be optional for the DASH client, for example it can ignore the feature if it does not support it. A typical example is, if the same media is provided with two different codecs, but the client only supports one of those, it can ignore the media provided with the other codec. There are other cases, for which the feature is mandatory to be supported by the DASH client in order to present the media presentation. Hence, it is expected that DASH clients support a certain set of features, if they want to consume a Media Presentation.

This logic leads to the definition of Interoperability Points, which presents a set of required features for the client in order to present a Media Presentation.

6 DASH-IF interoperability points

MPEG DASH defines formats for MPDs and Segments. In addition, MPEG provides the ability to further restrict the applied formats by the definition of *Profiles* as defined on clause 8 of ISO/IEC 23009-1 [1]. Profiles of DASH are defined to enable interoperability and the signaling of the use of features.

Such a profile can also be understood as permission for DASH clients that implement the features required by the profile to process the Media Presentation (MPD document and Segments).

Furthermore, ISO/IEC 23009-1 permits external organizations or individuals to define restrictions, permissions and extensions by using this profile mechanism. It is recommended that such external definitions be not referred to as profiles, but as *Interoperability Points*. Such an interoperability point may be signalled in the `@profiles` parameter once a URI is defined. The owner of the URI is responsible to provide sufficient semantics on the restrictions and permission of this interoperability point.

Earlier DASH-IF Interoperability specifications made use of this functionality and provided a set of Interoperability Points. Based on the interoperability point definition, DASH-IF interoperability points may have been understood in two ways:

- a collection of content conforming points, i.e. as long as the content conforms to the restrictions as specified by the IOP, clients implementing the features can consume the content.

- a client capability points that enable content and service providers for flexible service provisioning to clients conforming to these client capabilities.

DASH-IF Interoperability Points defined in earlier versions than v4.3 are maintained in Annex A.

However, in this version of the DASH-IF interoperability specifications, the concept of DASH-IF interoperability points is down-prioritized. The reason is that vertical client deployments are not in the scope of DASH-IF, but DASH-IF rather supports the introduction of features and provides interoperability for features.

Hence, the focus of this DASH-IF Interoperability specification is on features, the signalling of features and providing all relevant interoperability aspects for features. The definition of interoperability points is left to deployments and other organizations that may combine features for specific vertical deployments.

Newly defined Profiles and Interoperability Points are encouraged to be listed as part of the DASH-IF Identifiers as introduced in clause 7.

7 DASH-IF Identifiers

The DASH-IF hosts and manages an online cataloguing of identifiers for MPEG-DASH profiles, interoperability points, content protection metadata and other DASH related specific schemes. DASH-IF responsibilities include:

1. hosting the online catalogue on its website, listing all defined URIs along with short descriptions of their schemes and names of their owners,
2. providing a simple online mechanism to request the addition of new URIs and associated information, and finally
3. managing the administration and maintenance of the online catalogue.

It is believed that maintaining such a proper online catalogue helps the industry to increase the interoperability between various industry and consortia specifications, which are utilizing the MPEG-DASH standard.

DASH Identifiers for different categories can be found at http://dashif.org/identifiers/. DASH-IF supporters are encouraged to submit identifiers for documentation. In order to exploit synergies, individuals and organizations are encouraged to check the catalogue here prior to defining new identifiers. The DASH-IF will do its best to support individuals and organizations in this matter. Note also that DASH-IF typically tries to avoid defining identifiers. The website provides procedures how to request cataloguing the identifier in the DASH Identifier Repository and it defines a set of available descriptors and schemes identifiers.

Annex A:
DASH-IF Interoperability Points

This Annex defines the IOPs in Table A.1 and Extensions in A.2 from previous versions if DASH-IF IOP. The Implementation Guideline's version in which each IOP or Extension was added is also provided in the tables.

Note that all version 1 IOPs are also defined in version 2 and therefore referencing version 2 is sufficient.

Table 1 DASH-IF Interoperability Points

Interoperability Point	Identifier	Version
DASH-AVC/264	http://dashif.org/guidelines/dash264	1.0
DASH-AVC/264 SD	http://dashif.org/guidelines/dash264#sd	1.0
DASH-AVC/264 HD	http://dashif.org/guidelines/dash264#hd	2.0
DASH-AVC/264 main	http://dashif.org/guidelines/dash264main	3.0
DASH-AVC/264 high	http://dashif.org/guidelines/dash264high	3.0
DASH-IF IOP simple	http://dashif.org/guidelines/dash-if-simple	3.0
Error! Reference source not found.	http://dashif.org/guidelines/dash-if-main	3.0
DASH-IF IOP on-demand	http://dashif.org/guidelines/dash-if-ondemand	4.3
DASH-IF IOP mixed on-demand	http://dashif.org/guidelines/dash-if-mixed	4.3

Annex X (informative): Change History

Date	Version	Information about changes
2022-06-23	5.0.0	Initial version