draft-pantos-hls-rfc8216bis-18.txt	draft-pantos-hls-rfc8216bis-19-prelim.txt
Informational R. Pantos, Ed.	Informational R. Pantos, Ed.
Internet-Draft Apple Inc.	Internet-Draft Apple Inc.
Obsoletes: 8216 (if approved) 20 August 2025	Obsoletes: 8216 (if approved) 18 December 2025
Intended status: Informational	Intended status: Informational
Expires: 21 February 2026	Expires: When draft-pantos-hls-rfc8216bis-19 is published
HTTP Live Streaming 2nd Edition	HTTP Live Streaming 2nd Edition
draft-pantos-hls-rfc8216bis-18	draft-pantos-hls-rfc8216bis-19-preliminary-v1
Abstract	Abstract
This document obsoletes RFC 8216. It describes a protocol for transferring unbounded streams of multimedia data. It specifies the data format of the files and the actions to be taken by the server (sender) and the clients (receivers) of the streams. It describes version 13 of this protocol.	This document obsoletes RFC 8216. It describes a protocol for transferring unbounded streams of multimedia data. It specifies the data format of the files and the actions to be taken by the server (sender) and the clients (receivers) of the streams. It describes version 13 of this protocol.
Status of This Memo	Status of This Memo

skipping to change at *page 1, line 35*	skipping to change at *page 1, line 35*
Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.	Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.
Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."	Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."
This Internet-Draft will expire on 21 February 2026.	This Internet-Draft will expire on 21 June 2026.
Copyright Notice	Copyright Notice
Copyright (c) 2025 IETF Trust and the persons identified as the document authors. All rights reserved.	Copyright (c) 2025 IETF Trust and the persons identified as the document authors. All rights reserved.
This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights	This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights

1. Introduction to HTTP Live Streaming	1. Introduction to HTTP Live Streaming
HTTP Live Streaming provides a reliable, cost-effective means of delivering continuous and long-form video over the Internet. It allows a receiver to adapt the bit rate of the media to the current network conditions in order to maintain uninterrupted playback at the best possible quality. It supports interstitial content boundaries. It provides a flexible framework for media encryption. It can efficiently offer multiple renditions of the same content, such as	HTTP Live Streaming provides a reliable, cost-effective means of delivering continuous and long-form video over the Internet. It allows a receiver to adapt the bit rate of the media to the current network conditions in order to maintain uninterrupted playback at the best possible quality. It supports interstitial content boundaries. It provides a flexible framework for media encryption. It can efficiently offer multiple renditions of the same content, such as

skipping to change at *page 5, line 34*	skipping to change at *page 5, line 34*
The purpose of this document is to facilitate interoperability between HTTP Live Streaming implementations by describing the media transmission protocol. Using this protocol, a client can receive a continuous stream of media from a server for concurrent presentation.	The purpose of this document is to facilitate interoperability between HTTP Live Streaming implementations by describing the media transmission protocol. Using this protocol, a client can receive a continuous stream of media from a server for concurrent presentation.
This document is not an Internet Standards Track specification; it is published for informational purposes. It is not an Internet Standard. It is the focus of the IETF hls-interest group, but has not been shown to have the consensus of the wider IETF community.	This document is not an Internet Standards Track specification; it is published for informational purposes. It is not an Internet Standard. It is the focus of the IETF hls-interest group, but has not been shown to have the consensus of the wider IETF community.
This document describes version 12 of the protocol.	This document describes version 13 of the protocol.
2. Overview	2. Overview
A multimedia presentation is specified by a Uniform Resource Identifier (URI) [RFC3986] to a Playlist.	A multimedia presentation is specified by a Uniform Resource Identifier (URI) [RFC3986] to a Playlist.
A Playlist is either a Media Playlist or a Multivariant Playlist. Both are UTF-8 text files containing URIs and descriptive tags.	A Playlist is either a Media Playlist or a Multivariant Playlist. Both are UTF-8 text files containing URIs and descriptive tags.
A Media Playlist contains a list of Media Segments, which, when	A Media Playlist contains a list of Media Segments, which, when

skipping to change at *page 26, line 46*	skipping to change at *page 26, line 46*
#EXT-X-KEY:<attribute-list>	#EXT-X-KEY:<attribute-list>
The following attributes are defined:	The following attributes are defined:
METHOD	METHOD
The value is an enumerated-string that specifies the encryption method. This attribute is REQUIRED.	The value is an enumerated-string that specifies the encryption method. This attribute is REQUIRED.
The required methods are: NONE, AES-128, and SAMPLE-AES. Clients MAY additionally support the SAMPLE-AES-CTR method.	The required methods are: NONE, AES-128, and SAMPLE-AES. Clients MAY additionally support the SAMPLE-AES-CTR and the AES-256-GCM methods.
An encryption method of NONE means that Media Segments are not encrypted. If the encryption method is NONE, other attributes MUST NOT be present.	An encryption method of NONE means that Media Segments are not encrypted. If the encryption method is NONE, other attributes MUST NOT be present.
An encryption method of AES-128 signals that Media Segments are completely encrypted using the Advanced Encryption Standard (AES) [AES_128] with a 128-bit key, Cipher Block Chaining (CBC), and Public-Key Cryptography Standards #7 (PKCS7) padding [RFC5652]. CBC is restarted on each segment boundary, using either the Initialization Vector (IV) attribute value or the Media Sequence Number as the IV; see Section 5.2.	An encryption method of AES-128 signals that Media Segments are completely encrypted using the Advanced Encryption Standard (AES) [AES] with a 128-bit key, Cipher Block Chaining (CBC), and Public-Key Cryptography Standards #7 (PKCS7) padding [RFC5652]. CBC is restarted on each segment boundary, using either the Initialization Vector (IV) attribute value or the Media Sequence Number as the IV; see Section 5.2.
	An encryption method of AES-256-GCM signals that Media Segments are completely encrypted using the Advanced Encryption Standard (AES) [AES] with a 256-bit key and the Galois/Counter Mode (GCM) [AES_GCM]. This mode uses a 128-bit IV, and produces a 128-bit GCM authentication tag in addition to the cipher-text. GCM is restarted on each segment boundary. Each encrypted segment starts with the 16-octet IV, followed by the AES cipher-text, and ending with the 16-octet GCM authentication tag. If an EXT-X-KEY tag uses the AES-256-GCM encryption method then it MUST NOT have an IV attribute.
An alternative to whole-segment encryption is Sample Encryption. With Sample Encryption, only media sample data - such as audio packets or video frames - is encrypted. The rest of the Media Segment is unencrypted. Sample Encryption allows parts of the Segment to be processed without (or before) decrypting the media itself.	An alternative to whole-segment encryption is Sample Encryption. With Sample Encryption, only media sample data - such as audio packets or video frames - is encrypted. The rest of the Media Segment is unencrypted. Sample Encryption allows parts of the Segment to be processed without (or before) decrypting the media itself.
An encryption method of SAMPLE-AES means that the Media Segments are Sample Encrypted using the Advanced Encryption Standard [AES_128]. How these media streams are encrypted and encapsulated in a segment depends on the media encoding and the media format of the segment. fMP4 Media Segments are encrypted using the 'cbcs' scheme of Common Encryption [COMMON_ENC]. Encryption of other Media Segment formats containing H.264 [H_264], AAC [ISO_14496], AC-3 [AC_3], and Enhanced AC-3 [AC_3] media streams is described in the HTTP Live Streaming (HLS) Sample Encryption specification [SampleEnc]. The IV attribute MAY be present; see Section 5.2.	An encryption method of SAMPLE-AES means that the Media Segments are Sample Encrypted using the Advanced Encryption Standard [AES]. How these media streams are encrypted and encapsulated in a segment depends on the media encoding and the media format of the segment. fMP4 Media Segments are encrypted using the 'cbcs' scheme of Common Encryption [COMMON_ENC]. Encryption of other Media Segment formats containing H.264 [H_264], AAC [ISO_14496], AC-3 [AC_3], and Enhanced AC-3 [AC_3] media streams is described in the HTTP Live Streaming (HLS) Sample Encryption specification [SampleEnc]. The IV attribute MAY be present; see Section 5.2.
An encryption method of SAMPLE-AES-CTR is similar to SAMPLE-AES. However, fMP4 Media Segments are encrypted using the 'cenc' scheme of Common Encryption [COMMON_ENC]. Encryption of other Media Segment formats is not defined for SAMPLE-AES-CTR. The IV attribute MUST NOT be present	An encryption method of SAMPLE-AES-CTR is similar to SAMPLE-AES. However, fMP4 Media Segments are encrypted using the 'cenc' scheme of Common Encryption [COMMON_ENC]. Encryption of other Media Segment formats is not defined for SAMPLE-AES-CTR. The IV attribute MUST NOT be present.
URI	URI
The value is a quoted-string containing a URI that specifies how to obtain the key. This attribute is REQUIRED unless the METHOD is NONE.	The value is a quoted-string containing a URI that specifies how to obtain the key. This attribute is REQUIRED unless the METHOD is NONE.
IV	IV
The value is a hexadecimal-sequence that specifies a 128-bit unsigned integer Initialization Vector to be used with the key. Use of the IV attribute REQUIRES a compatibility version number of 2 or greater. See Section 5.2 for when the IV attribute is used.	The value is a hexadecimal-sequence that specifies a 128-bit unsigned integer Initialization Vector to be used with the key. Use of the IV attribute REQUIRES a compatibility version number of 2 or greater. See Section 5.2 for when the IV attribute is used. This attribute is OPTIONAL; but may be disallowed depending on the encryption METHOD.
KEYFORMAT	KEYFORMAT
The value is a quoted-string that specifies how the key is represented in the resource identified by the URI; see Section 5 for more detail. This attribute is OPTIONAL; its absence indicates an implicit value of "identity". Use of the KEYFORMAT attribute REQUIRES a compatibility version number of 5 or greater.	The value is a quoted-string that specifies how the key is represented in the resource identified by the URI; see Section 5 for more detail. This attribute is OPTIONAL; its absence indicates an implicit value of "identity". Use of the KEYFORMAT attribute REQUIRES a compatibility version number of 5 or greater.
KEYFORMATVERSIONS	KEYFORMATVERSIONS
The value is a quoted-string containing one or more positive integers separated by the "/" character (for example, "1", "1/2",	The value is a quoted-string containing one or more positive integers separated by the "/" character (for example, "1", "1/2",

skipping to change at *page 57, line 50*	skipping to change at *page 58, line 5*
attribute is OPTIONAL.	attribute is OPTIONAL.
5. Key Files	5. Key Files
5.1. Structure of Key Files	5.1. Structure of Key Files
An EXT-X-KEY tag with a URI attribute identifies a Key file. A Key file contains a cipher key that can decrypt Media Segments in the Playlist.	An EXT-X-KEY tag with a URI attribute identifies a Key file. A Key file contains a cipher key that can decrypt Media Segments in the Playlist.
[AES_128] encryption uses 16-octet keys. If the KEYFORMAT of an EXT-X-KEY tag is "identity", the Key file is a single packed array of 16 octets in binary format.	[AES] encryption uses 16-octet keys (or 32-octet keys in the case of AES-256-GCM). If the KEYFORMAT of an EXT-X-KEY tag is "identity", the Key file is a single packed array of the key octets in binary format.
5.2. IV for AES-128	5.2. IV for AES encryption methods
[AES_128] REQUIRES the same 16-octet IV to be supplied when encrypting and decrypting. Varying this IV increases the strength of the cipher.	[AES] REQUIRES the same IV to be supplied when encrypting and decrypting. Varying this IV increases the strength of the cipher.
	An EXT-X-KEY tag with a KEYFORMAT of "identity" and a METHOD of AES-128 or SAMPLE-AES that does not have an IV attribute indicates that the Media Sequence Number is to be used as the IV when decrypting a Media Segment, by putting its big-endian binary representation into a 16-octet (128-bit) buffer and padding (on the left) with zeros. Note that this approach is not recommended, as simply incrementing the IV provides little variability.
An IV attribute on an EXT-X-KEY tag with a KEYFORMAT of "identity" specifies an IV that can be used when decrypting Media Segments encrypted with that Key file. IV values for AES-128 are 128-bit numbers.	An IV attribute on an EXT-X-KEY tag with a KEYFORMAT of "identity" and a METHOD of AES-128 or SAMPLE-AES specifies an IV that can be used when decrypting Media Segments encrypted with that Key file.
An EXT-X-KEY tag with a KEYFORMAT of "identity" that does not have an IV attribute indicates that the Media Sequence Number is to be used as the IV when decrypting a Media Segment, by putting its big-endian binary representation into a 16-octet (128-bit) buffer and padding (on the left) with zeros.	IV values for AES-128, SAMPLE-AES, and AES-256-GCM are 128-bit (16-octet) numbers. In the case of AES-256-GCM, an IV value is specified in the encrypted segment.
6. Client/Server Responsibilities	6. Client/Server Responsibilities
6.1. Introduction	6.1. Introduction
This section describes how the server generates the Playlist and Media Segments and how the client should download them for playback.	This section describes how the server generates the Playlist and Media Segments and how the client should download them for playback.
6.2. Server Responsibilities	6.2. Server Responsibilities

skipping to change at *page 59, line 6*	skipping to change at *page 59, line 16*
support effective decode of individual Media Segments, such as on packet and key frame boundaries.	support effective decode of individual Media Segments, such as on packet and key frame boundaries.
The server MUST create a URI for every Media Segment that enables its clients to obtain the segment data. If a server supports partial loading of resources (e.g., via HTTP Range requests), it MAY specify segments as sub-ranges of larger resources using the EXT-X-BYTERANGE tag.	The server MUST create a URI for every Media Segment that enables its clients to obtain the segment data. If a server supports partial loading of resources (e.g., via HTTP Range requests), it MAY specify segments as sub-ranges of larger resources using the EXT-X-BYTERANGE tag.
The absence of media data (due to, for example, the temporary unavailability of an encoder) SHOULD be signaled by adding one or more Media Segments to the Playlist whose Segment durations add up to the duration of absent media; these Media Segments MUST have EXT-X-GAP tags applied to them. Similarly, such Partial Segments MUST have a GAP=YES attribute. Attempting to download these segments MAY produce an error, such as HTTP 404 or 410.	The absence of media data (due to, for example, the temporary unavailability of an encoder with no change in the encoding parameters) SHOULD be signaled by adding one or more Media Segments to the Playlist whose Segment durations add up to the duration of absent media; these Media Segments MUST have EXT-X-GAP tags applied to them. Similarly, such Partial Segments MUST have a GAP=YES attribute. Attempting to download these segments MAY produce an error, such as HTTP 404 or 410. Adding gap segments to the Playlist allows clients to detect and handle missing content while maintaining the continuity of the EXTINF timeline.
	Any changes in encoding parameters (such as, codec, resolution, file format, and tracks) or timing information MUST be signalled by the use of EXT-X-DISCONTINUITY. Format changes MAY require decoder initialization and MAY result in a noticeable playback transition.
A Media Segment MUST be available for immediate download at the full speed of the link to the Client when it is added to a Playlist unless it has been marked with an EXT-X-GAP tag; otherwise playback errors can occur. Once download starts, its transfer rate SHOULD NOT be constrained by the segment production process.	A Media Segment MUST be available for immediate download at the full speed of the link to the Client when it is added to a Playlist unless it has been marked with an EXT-X-GAP tag; otherwise playback errors can occur. Once download starts, its transfer rate SHOULD NOT be constrained by the segment production process.
A Partial Segment MUST be similarly available at the time it is added to a Playlist.	A Partial Segment MUST be similarly available at the time it is added to a Playlist.

skipping to change at *page 63, line 40*	skipping to change at *page 63, line 46*
tags, each with a different KEYFORMAT attribute value.	tags, each with a different KEYFORMAT attribute value.
The server MAY set the HTTP Expires header in the key response to indicate the duration for which the key can be cached.	The server MAY set the HTTP Expires header in the key response to indicate the duration for which the key can be cached.
Any unencrypted Media Segment in a Playlist MUST be in the scope of an EXT-X-KEY tag that specifies an encryption METHOD of NONE or precedes the first EXT-X-KEY tag. Otherwise, the client will misinterpret those segments as encrypted.	Any unencrypted Media Segment in a Playlist MUST be in the scope of an EXT-X-KEY tag that specifies an encryption METHOD of NONE or precedes the first EXT-X-KEY tag. Otherwise, the client will misinterpret those segments as encrypted.
If the encryption METHOD is AES-128 and the Playlist does not contain the EXT-X-I-FRAMES-ONLY tag, AES encryption as described in Section 4.4.4.4 SHALL be applied to individual Media Segments.	If the encryption METHOD is AES-128 or AES-256-GCM and the Playlist does not contain the EXT-X-I-FRAMES-ONLY tag, AES encryption as described in Section 4.4.4.4 SHALL be applied to individual Media Segments.
If the encryption METHOD is AES-128 and the Playlist contains an EXT-X-I-FRAMES-ONLY tag, the entire resource MUST be encrypted using AES-128 CBC with PKCS7 padding [RFC5652]. Encryption MAY be restarted on 16-byte block boundaries, unless the first block contains an I-frame. The IV used for encryption MUST be either the Media Sequence Number of the Media Segment or the value of the IV attribute of the EXT-X-KEY tag, as described in Section 5.2. These constraints allow a client to load and decrypt individual I-frames specified as sub-ranges of regular encrypted Media Segments, and	If the encryption METHOD is AES-128 and the Playlist contains an EXT-X-I-FRAMES-ONLY tag, the entire resource MUST be encrypted using AES-128 CBC with PKCS7 padding [RFC5652]. Encryption MAY be restarted on 16-byte block boundaries, unless the first block contains an I-frame. The IV used for encryption MUST be either the Media Sequence Number of the Media Segment or the value of the IV attribute of the EXT-X-KEY tag, as described in Section 5.2. These constraints allow a client to load and decrypt individual I-frames specified as sub-ranges of regular encrypted Media Segments, and

skipping to change at *page 74, line 14*	skipping to change at *page 74, line 14*
A client MUST ignore any EXT-X-KEY tag with an unsupported or unrecognized KEYFORMAT attribute, to allow for cross-device addressability. If the Playlist contains a Media Segment to which only EXT-X-KEY tags with unrecognized or unsupported KEYFORMAT attributes are applied, playback SHOULD fail.	A client MUST ignore any EXT-X-KEY tag with an unsupported or unrecognized KEYFORMAT attribute, to allow for cross-device addressability. If the Playlist contains a Media Segment to which only EXT-X-KEY tags with unrecognized or unsupported KEYFORMAT attributes are applied, playback SHOULD fail.
A client MUST NOT attempt to decrypt any segments whose EXT-X-KEY tag has a METHOD attribute that it does not recognize.	A client MUST NOT attempt to decrypt any segments whose EXT-X-KEY tag has a METHOD attribute that it does not recognize.
If the encryption METHOD is AES-128, AES-128 CBC decryption SHALL be applied to individual Media Segments, whose encryption format is described in Section 4.4.4.4.	If the encryption METHOD is AES-128, AES-128 CBC decryption MUST be applied to individual Media Segments, whose encryption format is described in Section 4.4.4.4.
	If the encryption METHOD is AES-256-GCM, AES-256 GCM [AES_GCM] decryption and authentication tag verification MUST be applied to individual Media Segments, whose encryption format is described in Section 4.4.4.4.
If the encryption METHOD is AES-128 and the Media Segment is part of an I-frame Playlist (Section 4.4.3.6) and it has an EXT-X-BYTERANGE tag applied to it, special care needs to be taken in loading and decrypting the segment, because the resource identified by the URI is encrypted in 16-byte blocks from the start of the resource.	If the encryption METHOD is AES-128 and the Media Segment is part of an I-frame Playlist (Section 4.4.3.6) and it has an EXT-X-BYTERANGE tag applied to it, special care needs to be taken in loading and decrypting the segment, because the resource identified by the URI is encrypted in 16-byte blocks from the start of the resource.
The decrypted I-frame can be recovered by first widening its byte range, as specified by the EXT-X-BYTERANGE tag, so that it starts and ends on 16-byte boundaries from the start of the resource.	The decrypted I-frame can be recovered by first widening its byte range, as specified by the EXT-X-BYTERANGE tag, so that it starts and ends on 16-byte boundaries from the start of the resource.

skipping to change at *page 91, line 11*	skipping to change at *page 91, line 11*
(formerly SSL) in conjunction with a secure realm or a session token.	(formerly SSL) in conjunction with a secure realm or a session token.
13. References	13. References
13.1. Normative References	13.1. Normative References
[AC_3] Advanced Television Systems Committee, "Digital Audio Compression (AC-3) (E-AC-3)", ATSC Standard A/52:2010, 22 November 2010, <http://atsc.org/wp-content/uploads/2015/03/A52-201212-17.pdf>.	[AC_3] Advanced Television Systems Committee, "Digital Audio Compression (AC-3) (E-AC-3)", ATSC Standard A/52:2010, 22 November 2010, <http://atsc.org/wp-content/uploads/2015/03/A52-201212-17.pdf>.
[AES_128] National Institute of Standards and Technology, "Advanced Encryption Standard (AES)", Federal Information Processing Standards Publication (FIPS) NIST FIPS 197-upd1, May 2023, <https://doi.org/10.6028/NIST.FIPS.197-upd1>.	[AES] National Institute of Standards and Technology, "Advanced Encryption Standard (AES)", Federal Information Processing Standards Publication (FIPS) NIST FIPS 197-upd1, May 2023, <https://doi.org/10.6028/NIST.FIPS.197-upd1>.
	[AES_GCM] National Institute of Standards and Technology, "Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC", NIST Special Publication 800-38D, November 2007, <https://csrc.nist.gov/pubs/sp/800/38/d/final>.
[CEA608] Consumer Technology Association, "Line 21 Data Services", ANSI/CTA Standard 608-E, April 2008, <https://standards.cta.tech/kwspub/published_docs/ANSI-CTA-608-E-R-2014-Preview.pdf>.	[CEA608] Consumer Technology Association, "Line 21 Data Services", ANSI/CTA Standard 608-E, April 2008, <https://standards.cta.tech/kwspub/published_docs/ANSI-CTA-608-E-R-2014-Preview.pdf>.
[CEA708] Consumer Technology Association, "Digital Television (DTV) Closed Captioning", ANSI/CTA Standard CEA-708-E, August 2013, <https://standards.cta.tech/kwspub/published_docs/ANSI-CTA-708-E-Preview.pdf>.	[CEA708] Consumer Technology Association, "Digital Television (DTV) Closed Captioning", ANSI/CTA Standard CEA-708-E, August 2013, <https://standards.cta.tech/kwspub/published_docs/ANSI-CTA-708-E-Preview.pdf>.

skipping to change at *page 92, line 8*	skipping to change at *page 92, line 8*
International Organization for Standardization, "Information technology -- MPEG systems technologies -- Part 7: Common encryption in ISO base media file format files", ISO/IEC International Standard 23001-7:2016, February 2016, <http://www.iso.org/iso/catalogue_detail.htm?csnumber=68042>.	International Organization for Standardization, "Information technology -- MPEG systems technologies -- Part 7: Common encryption in ISO base media file format files", ISO/IEC International Standard 23001-7:2016, February 2016, <http://www.iso.org/iso/catalogue_detail.htm?csnumber=68042>.
[Content-Steering] Pantos, R., Ed. and E. Vershen, "Content Steering", Work in Progress, Internet-Draft, draft-pantos-content-steering-00, 17 February 2025, <https://datatracker.ietf.org/doc/html/draft-pantos-content-steering-00>.	[Content-Steering] Pantos, R., Ed. and E. Vershen, "Content Steering", Work in Progress, Internet-Draft, draft-pantos-content-steering-00, 20 August 2025, <https://datatracker.ietf.org/doc/html/draft-pantos-content-steering-01>.
[HDCP] Digital Content Protection LLC, "High-bandwidth Digital Content Protection System - Mapping HDCP to HDMI", February 2013, <http://www.digital-cp.com/sites/default/files/specifications/HDCP%20on%20HDMI%20Specification%20Rev2_2_Final1.pdf>.	[HDCP] Digital Content Protection LLC, "High-bandwidth Digital Content Protection System - Mapping HDCP to HDMI", February 2013, <http://www.digital-cp.com/sites/default/files/specifications/HDCP%20on%20HDMI%20Specification%20Rev2_2_Final1.pdf>.
[H_264] International Telecommunications Union, "Advanced video coding for generic audiovisual services", January 2012, <http://www.itu.int/rec/T-REC-H.264>.	[H_264] International Telecommunications Union, "Advanced video coding for generic audiovisual services", January 2012, <http://www.itu.int/rec/T-REC-H.264>.

skipping to change at *page 107, line 29*	skipping to change at *page 107, line 29*
If present, the duration (or planned duration) of the Date Range SHOULD be the duration of the interstitial asset(s), even if a CUE attribute allows the interstitial to start at some time other than the START-DATE.	If present, the duration (or planned duration) of the Date Range SHOULD be the duration of the interstitial asset(s), even if a CUE attribute allows the interstitial to start at some time other than the START-DATE.
A Server MAY add a Preload EXT-X-DATERANGE tag to indicate that the client SHOULD preload the URI specified by the X-ASSET-URI or X-ASSET-LIST attribute of an existing or upcoming Interstitial EXT-X-DATERANGE tag. See Appendix F for more information.	A Server MAY add a Preload EXT-X-DATERANGE tag to indicate that the client SHOULD preload the URI specified by the X-ASSET-URI or X-ASSET-LIST attribute of an existing or upcoming Interstitial EXT-X-DATERANGE tag. See Appendix F for more information.
	The server SHOULD specify a preload range that ends at or shortly before the interstitial is expected to be scheduled. The duration of the period SHOULD be as long as the preload could be considered valid before that point (even if practically the client will not be able to issue it that far in advance).
The client SHOULD choose a random point inside the Preload Date Range and preload the URI when the current playhead position passes that point. A client SHOULD NOT load an Interstitial any later than it would have in the absence of the Preload EXT-X-DATERANGE tag.	The client SHOULD choose a random point inside the Preload Date Range and preload the URI when the current playhead position passes that point. A client SHOULD NOT load an Interstitial any later than it would have in the absence of the Preload EXT-X-DATERANGE tag.
	After obtaining the preload date range but before selecting a random point within it, the client SHOULD:
	A. Ensure that the effective start of the preload range is greater than or equal to the current playhead position, to avoid selecting a preload time in the past.
	B. Ensure that the effective end of the preload range occurs before the client expects to normally resolve the interstitial.
	1. If the START-DATE of the interstitial is already known, the client SHOULD predict how long it would wait before resolving the interstitial if it were not preloaded, and ensure that the end of the preload range is no greater than the current playhead position plus that wait time.
	2. In the case where the START-DATE of the interstitial is not yet known, the client SHOULD assume that it will appear the next time that the Playlist is reloaded, with the same date as the end of the preload range, and then proceed as in the first case.
Clients SHOULD ignore Preload EXT-X-DATERANGE tags if the Playlist contains an EXT-X-ENDLIST tag.	Clients SHOULD ignore Preload EXT-X-DATERANGE tags if the Playlist contains an EXT-X-ENDLIST tag.
	If the X-RESUME-OFFSET is not present and X-PLAYOUT-LIMIT specifies a value less than the total duration of the Interstitial, then the value of the resumption offset will be the playout limit.
D.3. Skip button control for an Interstitial	D.3. Skip button control for an Interstitial
Content producers can allow clients to skip an Interstitial. This section describes how to configure a Skip button. The following attributes are defined to help control the skip button behavior.	Content producers can allow clients to skip an Interstitial. This section describes how to configure a Skip button. The following attributes are defined to help control the skip button behavior.
X-SKIP-CONTROL-OFFSET	X-SKIP-CONTROL-OFFSET
The value of the X-SKIP-CONTROL-OFFSET is a decimal-integer of seconds of an interstitial content that should be played until a	The value of the X-SKIP-CONTROL-OFFSET is a decimal-integer of seconds of an interstitial content that should be played until a

skipping to change at *page 109, line 30*	skipping to change at *page 110, line 17*
interstitial with a resume offset of 0.	interstitial with a resume offset of 0.
If a request for the URI of a single asset within an asset list returns an error, the client SHOULD skip playback of that asset. When X-RESUME-OFFSET is determined by the duration of the interstitial you MAY ignore the duration of the skipped asset(s) in computing the duration of the interstitial.	If a request for the URI of a single asset within an asset list returns an error, the client SHOULD skip playback of that asset. When X-RESUME-OFFSET is determined by the duration of the interstitial you MAY ignore the duration of the skipped asset(s) in computing the duration of the interstitial.
If the JSON object returned by the asset list URI has an empty array as the value of the "ASSETS" key, the client SHOULD apply the resume offset without playing any interstitial content.	If the JSON object returned by the asset list URI has an empty array as the value of the "ASSETS" key, the client SHOULD apply the resume offset without playing any interstitial content. A resume offset of 0 SHOULD be used when no Interstitials are played, unless a value was specified with X-RESUME-OFFSET.
Clients SHOULD allow a generous amount of time (up to a minute) for a server to respond to requests for interstitial assets or asset lists, to enable the server to perform back-end decisioning. Servers MUST respond quickly enough to avoid playback disruptions on the client.	Clients SHOULD allow a generous amount of time (up to a minute) for a server to respond to requests for interstitial assets or asset lists, to enable the server to perform back-end decisioning. Servers MUST respond quickly enough to avoid playback disruptions on the client.
D.6. Example: Interstitial EXT-X-DATERANGE	D.6. Example: Interstitial EXT-X-DATERANGE
In this playlist an EXT-X-DATERANGE tag schedules a 15-second ad to play four seconds into a six-second primary asset. The client will	In this playlist an EXT-X-DATERANGE tag schedules a 15-second ad to play four seconds into a six-second primary asset. The client will

skipping to change at *page 117, line 4*	skipping to change at *page 117, line 48*
REQUIRED.	REQUIRED.
MEDIA-PRESENTATION-SETTINGS: This is an array of Presentation Selector objects. The array SHOULD be non-empty. This element is REQUIRED.	*MEDIA-PRESENTATION-SETTINGS*: This is an array of Presentation Selector objects. The array SHOULD be non-empty. This element is REQUIRED.
LANGUAGE-DISPLAY: This element is OPTIONAL. Language can be offered as a preference that's separate from all of the available Selectors. If this element is present and has the string value "NONE", then language SHOULD NOT be offered as a preference.	*LANGUAGE-DISPLAY*: This element is OPTIONAL. Language can be offered as a preference that's separate from all of the available Selectors. If this element is present and has the string value "NONE", then language SHOULD NOT be offered as a preference.
Otherwise, lnaguage SHOULD be offered as a preference. When offered, lanugage has the highest priority among the user's selected preferences.	Otherwise, lnaguage SHOULD be offered as a preference. When offered, lanugage has the highest priority among the user's selected preferences.
Each Presentation Selector object has these elements:	Each Presentation Selector object has these elements:
SELECTOR: The value is a UTF8 string which is a unique short namee for the Selector. This element is REQUIRED.	*SELECTOR*: The value is a UTF8 string which is a unique short name for the Selector. This element is REQUIRED.
DISPLAY-NAMES: The value is a set of name/value pairs, where each name is a primary language subtag [RFC5646] and each value is a UTF-8 string containing the name of the Selector localized in that language. This element is REQUIRED.	*DISPLAY-NAMES*: The value is a set of name/value pairs, where each name is a primary language subtag [RFC5646] and each value is a UTF-8 string containing the name of the Selector localized in that language. This element is REQUIRED.
SETTINGS: This is an array of Presentation Setting objects. The array SHOULD be non-empty. This element is REQUIRED.	*SETTINGS*: This is an array of Presentation Setting objects. The array SHOULD be non-empty. This element is REQUIRED.

End of changes. 40 change blocks.

62 lines changed or deleted	*135 lines changed or added*