Widevine DRM for HLS

version 1.1
# Revision History

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td>9/13/2017</td>
<td>Initial draft</td>
</tr>
<tr>
<td>0.2</td>
<td>10/12/2017</td>
<td>Expanded Attributes section with X-prefix tags. Remove changes</td>
</tr>
<tr>
<td>0.3</td>
<td>10/17/2017</td>
<td>Added Widevine PSSH.</td>
</tr>
<tr>
<td>0.4</td>
<td>11/1/2017</td>
<td>Restructured V1 and V2 formats, various edits and re-arrangements</td>
</tr>
<tr>
<td>0.5</td>
<td>11/28/2017</td>
<td>Updated SAMPLE-AES-CENC tag to SAMPLE-AES-CTR</td>
</tr>
<tr>
<td>0.6</td>
<td>12/1/2017</td>
<td>Additional corrections for SAMPLE-AES-CTR</td>
</tr>
<tr>
<td>0.7</td>
<td>12/13/2017</td>
<td>Removed overlap of V1/V2 signaling. Various corrections.</td>
</tr>
<tr>
<td>0.8</td>
<td>1/4/2018</td>
<td>Correction - content_id must be base64-decoded before copying to protobuf.</td>
</tr>
<tr>
<td>0.9</td>
<td>1/11/2018</td>
<td>Made V2 optional for legacy TS</td>
</tr>
<tr>
<td>1.0</td>
<td>4/17/2018</td>
<td>Updates to platform support for CMAF</td>
</tr>
<tr>
<td>1.1</td>
<td>1/24/2019</td>
<td>Updated supported platforms and PSSH proto</td>
</tr>
</tbody>
</table>
Overview

The purpose of this document is to specify a set of extensions to the base HTTP (HTTP Live Streaming) specification [1] to support the Widevine DRM system.

There are two versions of Widevine DRM signaling for HLS:

**Version 1** is the original working design applicable to Chromecast and the Android in-app library. This will continue to be needed for Widevine-protected content delivery to those devices for some time, but will be phased out. It is meant for signaling for HLS using MPEG-2 TS and Sample AES.

**Version 2** specifies the new extensions which are meant to be used for HLS in CMAF and be compatible and consistent with Widevine DRM signaling for MPEG-DASH.

References

- [1] HTTP Live Streaming Specification
HLS with CMAF support (V2)

This version of Widevine DRM signaling is required going forward for CMAF content. It may also be present for MPEG-2 TS presentations for forward compatibility.

Expected media format:
- Playlist: m3u8
- Container formats:
  - CMAF-branded MP4
  - Optional: MPEG-2 TS HLS

<table>
<thead>
<tr>
<th>Platform</th>
<th>Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>Android P</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Changes are around manifest parsing.</td>
</tr>
<tr>
<td></td>
<td>Encryption scheme is already supported.</td>
</tr>
<tr>
<td>Chrome Browser</td>
<td>68 or later</td>
</tr>
<tr>
<td>EME-based browsers with Widevine CDM</td>
<td>Chromium 68 or later</td>
</tr>
<tr>
<td>Shaka Player</td>
<td>Supported</td>
</tr>
<tr>
<td></td>
<td>* depends on browser</td>
</tr>
<tr>
<td>Chromecast</td>
<td>Supported</td>
</tr>
<tr>
<td>NexPlayer</td>
<td>Supported</td>
</tr>
</tbody>
</table>

Goal
- Add a new Widevine EXT-X-KEY tag in HLS playlists, that is similar to elements and attributes in DASH MPD.
- Additions that do not break spec-compliant players.

Non-Goals
- V2 specification has no intent to deprecate the V1 format, which still ought to be used for HLS with MPEG-2 transport streams.
New Format

EXT-X-KEY tag is used in HLS to signal encrypted media in the playlist. HLS mentions that “Two or more EXT-X-KEY tags with different KEYFORMAT attributes MAY apply to the same Media Segment if they ultimately produce the same decryption key”. So adding a new KEYFORMAT is spec compliant and existing Widevine HLS players that already handle Android format may ignore the new format.

Attributes

- **KEYFORMATVERSIONS="1"**
  - This proposal defines key format version 1.
  - Version 1 defines the following attributes.
- **KEYFORMAT="urn:uuid:edef8ba9-79d6-4ace-a3c8-27dcd51d21ed"**
  - The UUID is the Widevine UUID from DASH IF IOP. The same exact string is used in MPD with Widevine encrypted streams.
  - Note that in section 6.3.6, the spec mentions that “A client MUST ignore any EXT-X-KEY tag with an unsupported or unrecognized KEYFORMAT attribute, to allow for cross-device addressability.” Which means a spec-compliant player should not prevent playback solely due to unrecognized this key format.
- **URI="data:text/plain;base64,<base64 encoded PSSH box>"**
- **METHOD** indicates the encryption cipher used when encrypting the content.
  - SAMPLE-AES signals that the content is encrypted using ‘cbc’s’.
  - SAMPLE-AES-CTR signals that the content is encrypted using one of the AES-CTR protections schemes, namely ‘cenc’.

Attributes mapped to DASH MPD

- **KEYFORMAT**
  - ContentProtection element’s schemeIdUri attribute.
- **URI**
  - The content of cenc:pssh element.
- **KEYID**
  - 16-byte hexadecimal string (0x---------------------------------) encoding the key ID which has the same role as the default_kid in MPEG DASH. That is, the key which is retrieved from a DRM server to decrypt the content, which may or may not be the same as the actual content key ID. If using a hierarchical key scheme, this would be the “root” key.
Example HLS Playlist with V2 Signaling

#EXTM3U
#EXT-X-VERSION:6
#EXT-X-TARGETDURATION:2
#EXT-X-PLAYLIST-TYPE:VOD
#EXT-X-MAP:URI="init_segment.mp4"
#EXTINF:1.001,
output_video-1.mp4
#EXT-X-DISCONTINUITY
#EXT-X-KEY:METHOD=SAMPLE-AES,URI="data:text/plain;base64,AAAAPXBzc2gA
AAAA7e+LgXnWSs6jyCfc1R0h7QAAABOaDXdpZGV2aW51X3Rlc3QiDHRlc3QgY29udGVud
A==",KEYID=0x112233445566778899001122334455,KEYFORMAT="urn:uuid:edef8
ba9-79d6-4ace-a3c8-27dcd51d21ed",KEYFORMATVERSION="1"
#EXTINF:1.001,
output_video-2.mp4
#EXTINF:0.734,
output_video-3.mp4
#EXT-X-ENDLIST
Appendix A: Widevine PSSH

The Widevine PSSH is encoded in a version 0 ProtectionSystemSpecificHeader (‘pssh’) with system ID edef8ba9-79d6-4ace-a3c8-27dcd51d21ed.
The latest Widevine PSSH can be referenced at https://github.com/google/shaka-packager/blob/master/packager/media/base/widevine_pssh_data.proto
The Data field contains a serialized protocol buffer defined as follows:

```protobuf
// Copyright 2016 Google Inc. All rights reserved.
//
// Use of this source code is governed by a BSD-style license that can be found in the LICENSE file or at
// https://developers.google.com/open-source/licenses/bsd
//
// This file defines Widevine Pssh Data proto format.

syntax = "proto2";

package shaka.media;

message WidevinePsshData {
  enum Algorithm {
    UNENCRYPTED = 0;
    AESCTR = 1;
  }
  optional Algorithm algorithm = 1;
  repeated bytes key_id = 2;

  // Content provider name.
  optional string provider = 3;

  // A content identifier, specified by content provider.
  optional bytes content_id = 4;

  // The name of a registered policy to be used for this asset.
  optional string policy = 6;

  // Crypto period index, for media using key rotation.
  optional uint32 crypto_period_index = 7;

  // Optional protected context for group content. The grouped_license is a
  // serialized SignedMessage.
  optional bytes grouped_license = 8;
}
```
Appendix B: Legacy Widevine HLS (V1)

This type of Widevine DRM signaling is meant for legacy devices, consuming media streams as MPEG-2 TS.

V1 is no longer recommended or advised for usage.

Expected media format for V1:
- Playlist: m3u8
- Container format: MPEG-TS
Media playlist information

HLS playlists contain EXT-X-KEY tags that specify how encrypted media segments may be decrypted. An attribute list is associated with each tag. The attribute list applies to the media segments seen until the next EXT-X-KEY tag with the same KEYFORMAT attribute. A summary of the attributes, relevant to this integration, is listed below. A more complete description can be found in the HLS specification. One or more EXT-X-KEY tags may be present in a media playlist, one for each DRM vendor.

- **METHOD (required):** SAMPLE-AES
- **URI (required):** A quoted string containing a "data" URL (RFC 2397) whose data item is a json formatted version of the CENC init data. The "data" URL shall specify a media-type text/plain and use the base64 option.
- **IV (optional):** hexadecimal sequence that specifies a 128-bit unsigned integer Initialization vector. If absent the media sequence number is used as IV when decrypting a media segment.
- **KEYFORMAT (required):** quoted string that specifies how the key is represented. As multiple EXT-X-KEY tags may be present in a media playlist, this attribute is used by DRM vendors to disambiguate attribute lists meant for them. Widevine use the CENC Key System "com.widevine" to identify its attribute list.
- **KEYFORMATVERSIONS (optional):** quoted strings containing one or more positive integers separated by the "/" character. If not present, its value is considered to be "1".

The optionality of the parameters above refers to whether they are needed in an attribute list for the Widevine CDM to work correctly. This is separate from requirements that the HLS specification imposes. Here is an example of what an EXT-X-KEY attribute list might look like for Widevine:

```plaintext
EXT-X-KEY: METHOD=SAMPLE-AES, \
URI="data:text/plain;base64,eyAKICAgInByb3ZpZGVyIjoibWxiYW1oYm8iYm8iLAoIGCAiY29udGV4dCBhd3NodHRwczovL2RzLW9tYW5hbmQvZG9iYWxzL2FwYXlcZ3JvZ2lcL2RlZmF1bHRcL2F1ZD0iMC4xNTZmMjUyZTQ0MjUxMjQzNDE4M2QwMzYyZGQ4NTI0Y2YyYmNiNTMzZWY5YjM0YjIiLAogICAiY29udGVyIjogIkpWcm9zcml0aWxlIiwgICAgICAgIjM3MWUxMzVlMWE5NjU3MzNmMzgwNjM0NTZhZDc2MDYzZjRmZjIyN2U2YjIwZTc5NGIwZjFmMThlN2IiLAogICAic2N5X2lkIjogICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgI
```

Google - Confidential
Page 10 of 12
Last Updated: 1/24/2019 v1.1
The init data specified in the URI will be a json formatted version of the WidevineCencHeader protobuf. Here is an example,

```
{
  "content_id": "MjAxNV9UZWFycw==",
  "key_ids": [
    "371e135e1a985d75d198a7f41020dc23"
  ]
}
```

The init data json string will consist of:
- provider: json string. Encoded with ASCII characters only.
- content_id: json string. Base64 encoded Content ID (as specified by RFC 4648). This value shall be consistent with the Content ID specified to the license server.
- key_ids: json array, whose individual values are a hexadecimal sequence, a string of 32 characters drawn from the set [0-9a-fA-F].

The data from the init data json string will be used to populate the fields of a serialized WidevineCencHeader proto. This protobuf will be included in the license request.
- The provider value shall be copied as is into the protobuf field.
- The content_id value shall be base64-decoded first then copied into the protobuf field.
- The Key ID should be converted, from a 32 character hex ASCII string to a 16 byte value. For KEYFORMATVERSION “1”, key_ids shall specify a single 16 byte key ID. If multiple key IDs are present, the first will be used to decrypt the media segments that follow, until the next media playlist is encountered.

Example HLS Playlist with V1 Signaling

```"EXTM3U
EXT-X-TARGETDURATION: 9
EXT-X-VERSION: 5
EXT-X-MEDIA-SEQUENCE: 0
EXT-X-PLAYLIST-TYPE: VOD
EXT-X-KEY: METHOD=SAMPLE-AES, KEYFORMAT="com.widevine", KEYFORMATVERSIONS="1", URI="data:text/plain;base64,ewogICAicHJvdmlkZXIiOiAiY2FzdCIsCiAgICJjb250ZW50X2lkIjogIlltbG5ZblZqYTJKMWJtNTUiLAogICAia2V5X2lkcyI6IjJlNzU5MDQwMzIxYTQwOGE1Yzc3NjhiNDUxMTI4N2E2IgogICBdCn0=" IV =0x75537a79fa41abc7b598ea72aba0c26f```