IMPROVING CONTENT INTEROPERABILITY WITH THE DASH CONTENT PROTECTION EXCHANGE FORMAT STANDARD

L. Piron[1], K. Hughes[2], T. Inskip[3]

[1] Nagravision, Switzerland, [2] Microsoft, USA, and [3] Google, USA

ABSTRACT

Content Protection is one of the key success factors in the deployment of an OTT TV system. To enable various sustainable business models, Service Providers need to securely and efficiently implement the interoperability of DRM-protected content across multiple devices.

Secured software client integration is needed at the device level for retrieving keys and decrypting content in a controlled environment. There are many different implementation frameworks for executing this function, going from pure software to hardware-based solutions. Secured integration is also needed at the streaming platform head-end, so that the DRM system core elements such as content keys, needed for encrypting content and also for generating content usage licenses, can be used at the right place and at the right moment in the head-end system.

One key aspect of the DRM ecosystem is that it encompasses multiple DRM vendors with specific implementations across a broad and growing pool of devices. A service provider thus needs to ensure that the components in its head-end, often coming from multiple vendors, can also support multiple DRM vendors to ensure the interoperability of content across multiple devices.

To help address this challenge, DASH-IF has defined a set of supported use cases and a secure container for exchanging content keys between DRM systems and head-end components such as encoders and CMS systems. This allows for the seamless exchange of content keys between all components in the head-end. Content Security remains in the hand of the operator, as such interfaces and key exchanges are secured. Leveraging the DASH Common Encryption standard (CENC), the same piece of content is encrypted once and used on many different devices with the appropriate key.

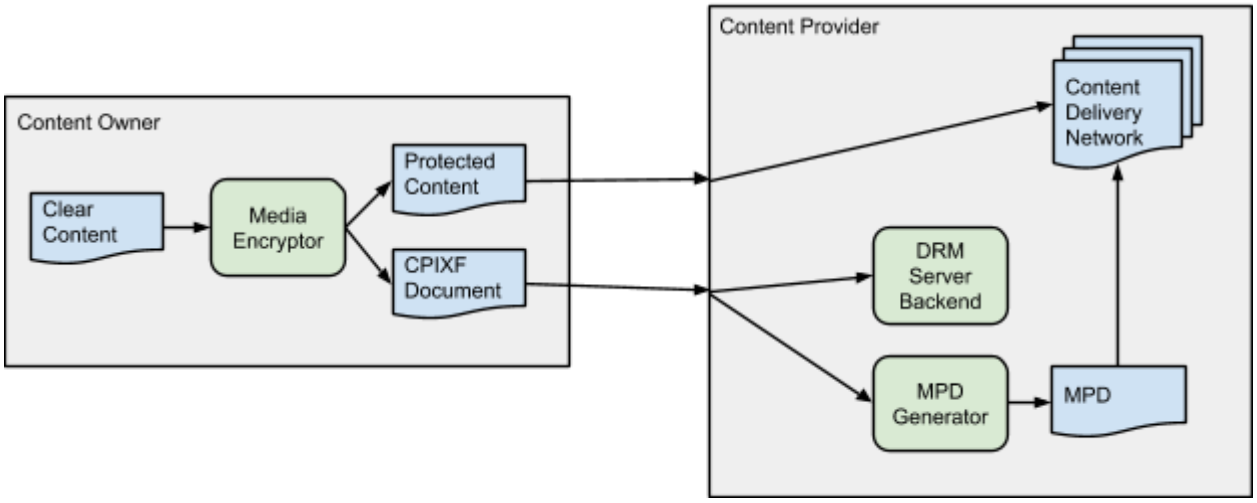
INTRODUCTION

The MPEG-DASH ecosystem is growing quickly, and a significant portion of the content being prepared and delivered is protected content. DASH profiles that have been deployed use MPEG Common Encryption for content protection in order to allow a single encoded and encrypted Representation to be played on multiple device types using multiple Digital Rights Management (DRM) systems. Common Encryption specifies standard content

protection information in ISO Media Representations and DASH manifests such as key identifiers, DRM system identifiers, etc. that can be shared throughout the DASH ecosystem.

Preparation of protected media content for delivery may involve multiple entities and processing steps. For example, a content owner may encrypt some premium content and deliver it to multiple content providers, which in turn may generate their own DASH Media Presentation Descriptions (MPDs), and make the media decryption keys available to end users via their DRM server(s). Without a common interchange format for the copy protection information, each content owner, provider, and/or DRM system might specify their own, non-interoperable means of importing and exporting copy protection related data. The Copy Protection Information Exchange Format (CPIXF) specification aims to provide interoperability for these functions by standardizing the way in which entities and media processors exchange content keys and associated copy protection metadata.

The following diagram illustrates the example described above



The Copy Protection Information Format specification fulfills the following requirements:

- Interoperability. This is the main goal of the specification; to allow the exchange of copy protection related data using a well-defined, specified and public mechanism.
- Flexibility. The CPIXF documents may be used in simple one-to-one exchanges, or in more complex workflows.
- Security. All security-sensitive information in the exchange (e.g. content keys) is encrypted in a manner such that only the intended recipient can decrypt it.

CONTENT PREPARATION WORKFLOWS

Content keys and DRM signalization need to be created and exchanged between some system entities when preparing content. The flows of information are of very different nature depending on where content keys are created and also depending on the type of content that can be either on-demand or live for example.

The following gives a general overview of the context in which content protection information made of keys and DRMs signalization needs to be exchanged between entities in the backend.

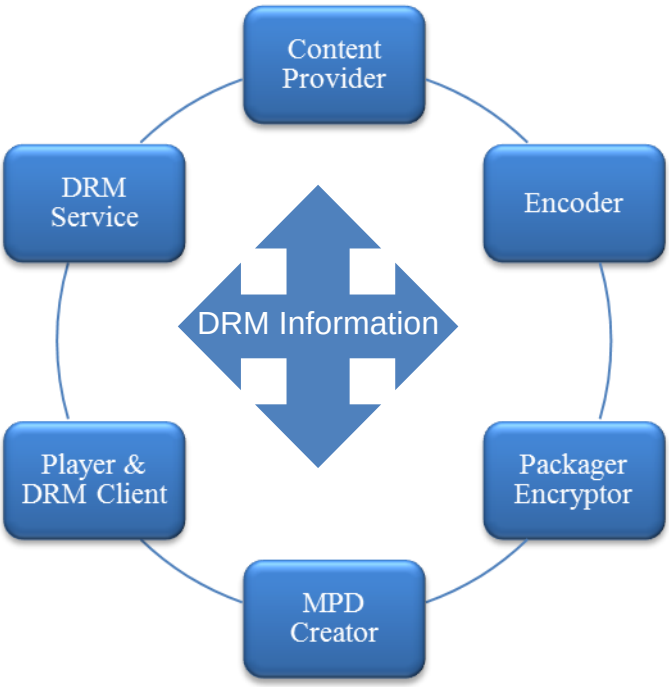


Figure 1: Logical roles that exchange DRM information and media.

Figure 1 shows logical entities that may send or receive DRM information such as content keys, asset identifiers, licenses, and license acquisition information. A physical entity may combine multiple logical roles, and the point of origin for information, such as content keys and asset identifiers, can differ; so various information flows are possible. This is an informative example of how the roles are distributed to facilitate the description of workflow and use cases. Alternative roles and functions can be applied to create conformant content. The different roles are:

Content Provider – A publisher who provides the rights and rules for delivering protected media, also possibly source media (mezzanine format, for transcoding), asset identifiers, key identifiers (KID), key values, encoding instructions, and content description metadata.

Encoder – A service provider who encodes in DASH format with specified media format, number of streams, range of bitrates and resolutions, seamless switching constraints, etc., possibly determined by the publisher. Each encoded track needs to be associated with a key identifier, a Representation element in an MPD, a possible 'pssh' box in the file header, and a DRM license separately downloaded.

Packager / Encryptor – A service provider who encrypts and packages media files, inserting default_KID in the file header 'tenc' box, initialization vectors and subsample byte ranges in track fragments indexed by 'saio' and 'saiz' boxes, and possibly packages 'pssh' boxes containing license acquisition information in the file header. Tracks that are partially encrypted or encrypted with multiple keys require sample to group boxes and sample group description boxes in each track fragment to associate different KIDs to groups of samples. The Packager could originate values for KIDs, content keys, encryption layout, etc., and then send that information to other entities that need it, including the DRM Provider and Streamer, and probably the Content Provider. Alternatively, the Packager could receive that information from another entity, such as the Content Provider or DRM Provider.

MPD Creator – The MPD Creator is assumed to create one or more types of DASH MPD. The MPD must include descriptors for Common Encryption and DRM key management systems, and should include identification of the default_KID for each AdaptationSet element, and sufficient information in UUID ContentProtection Descriptor elements to acquire a DRM license. The default_KID is available from the Packager and any other role that created it, and the DRM specific information is available from the DRM Provider.

DRM Client – A player typically relies on a native DRM client installed on a device that must receive information from different sources: MPD, Media files and DRM licenses.

DRM Service – The DRM Provider creates licenses containing a protected content key and playback rules that can only be decrypted by a trusted client.

The DRM Service needs to know the default_KID and DRM SystemID and possibly other information like asset ID and player domain ID in order to create and download one or more licenses required for a DASH presentation on a particular device. Each DRM system has different license acquisition information, a slightly different license acquisition protocol, and a different license format with different playback rules, output rules, revocation and renewal system, etc. The DRM Service typically must supply the Streamer and the Packager license acquisition information for each UUID ContentProtection Descriptor element or 'pssh' box, respectively.

The DRM Service may also provide logic to manage key rotation, DRM domain management, revocation and renewal and other content protection related features.

In such ecosystem, there can be different content preparation and information workflows, therefore CPIXF uses a container that is similar in structure to an MPD to allow secure exchange of all DRM information between any entities in any workflow.

DASH-IF has defined a container called the Content Protection Exchange Format (CPIXF) which has the following main properties. This is an XML file that is fully described in [DASH-CPIXF].

THE CONTENT PROTECTION EXCHANGE FORMAT

The structure is similar to the MPD structure defined in [DASH]. A Presentation is the root element of this schema and contains all information required for getting the common encryption keys which is used to encrypt all representations within all adaptation sets. It follows these principles:

- Following the constraints defined by [DASH-IOP], it is assumed that the same key is used for encrypting all Representations of a given Adaptation Set. For supporting key rotation, several Content Keys can be used for encrypting all Representations, each key with a validity period.
- The same XML file can be shared between several receiving entities; hence, each one must be able to decrypt the encrypted Common Encryption keys contained in the document by using public and private keys shared with the sender. The sharing of public key pairs is usually part of a contractual relationship between entities authorizing access to the content and keys, and is outside the scope of CPIXF.
- Taking this into account, the Presentation contains:

- DeliveryData: Each instance of the DeliveryData describes an entity that is permitted to decrypt common content key contained in the XML document. There is textual description and associated certificates for example.
- AdaptationSet: Each AdaptationSet contains the DefaultKey information (the common content key itself and all associated DRM Signalizations which is protection system specific information for every DRM.). Optionally, it can also contain ContentKey instances used when key rotation is enabled on this Adaptation Set.

The keys inside the DefaultKey and ContentKey entities can be encrypted inside the XML file using information provided in the DeliveryData element. The XML file also allows storing the content keys in the clear and then the protection of the delivery mechanism, such as IPSEC or TLS, is used for securely deliver the file.

The proposed schema relies on the Portable Symmetric Key Container (PSKC) defined by IETF [RFC-6030] for describing keys and the associated encryption. Necessary extensions are added for supporting DRM information and association of information with content.

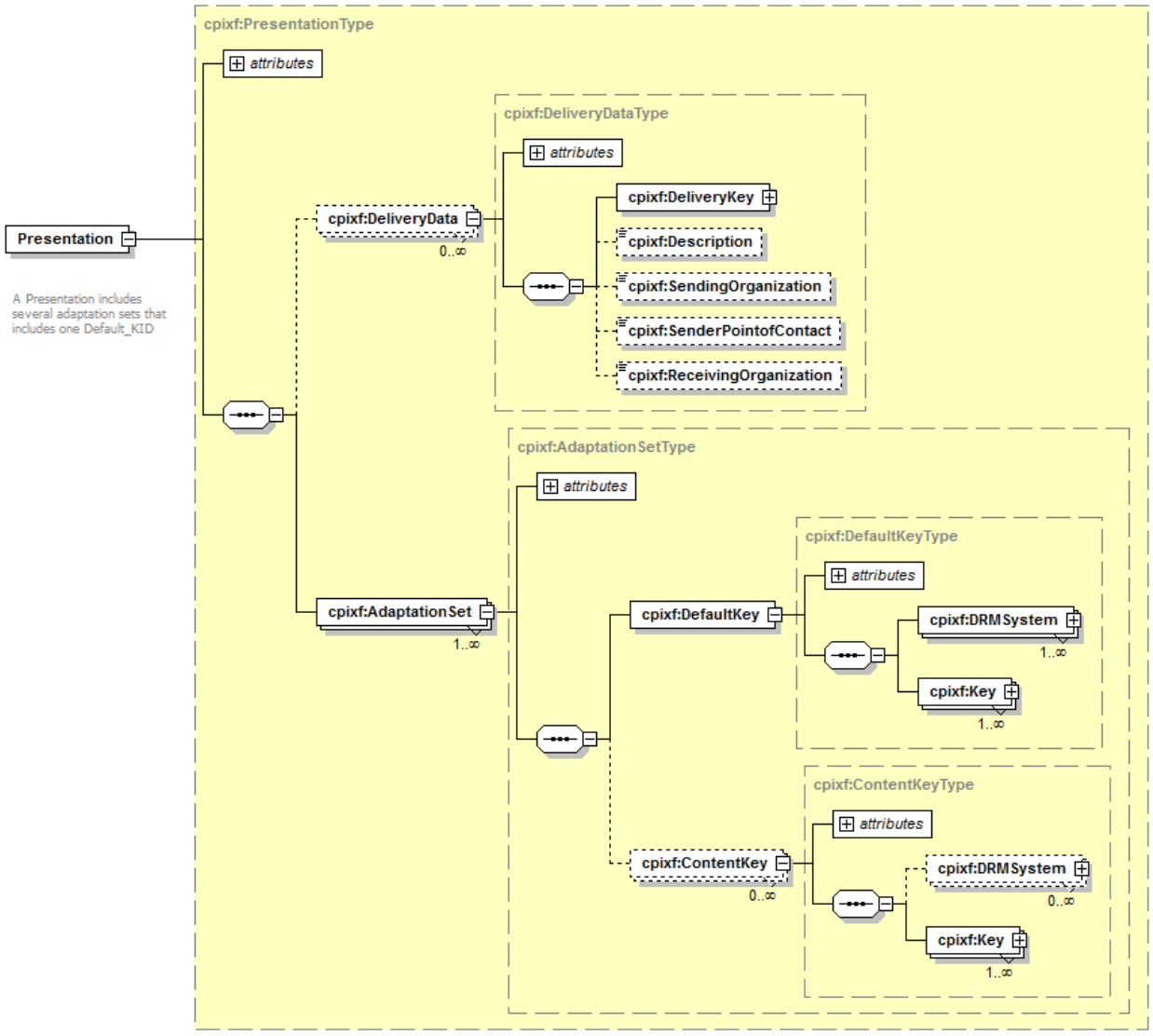


Figure 2: The CPIXF high level view.

USE CASES

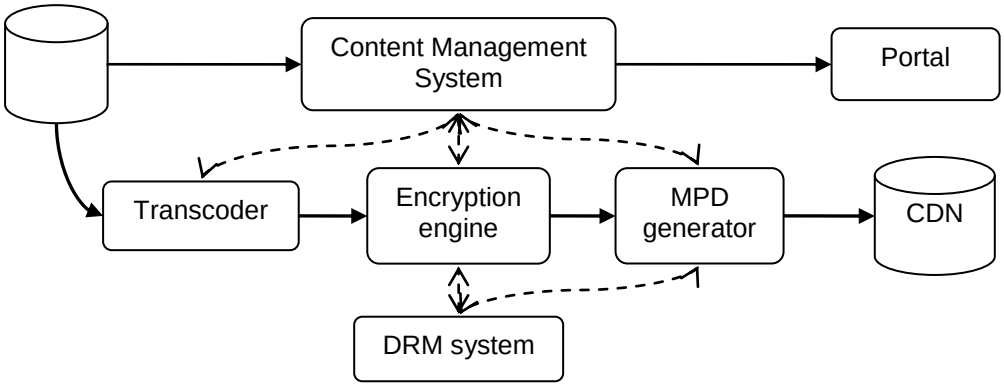
The following describes two classical cases where the CPIXF helps the overall workflow implementation. For on-demand content and live content,

Content on Demand

The flow for preparing Content on Demand requires that a file is available non-encrypted, ideally in the maximum resolution so that DASH content can be prepared.

A Content Management System (CMS) masters the creation flow. The CMS makes the file available to a transcoder. The transcoder outputs the segmented files that can be encrypted. The encryption engine either generates the content key(s) or requests them from a DRM system. The DRM system also provides any information to be added in the PSSH boxes. When the encrypted DASH content is ready, the MPD is generated by a MPD generator. It asks the DRM system the required DRM signalization to be added in the MPD. DASH content is then uploaded by the CMS on a CDN making it available to users. In parallel, editorial metadata is exported to the Portal, enabling access to users. DRM systems receive relevant metadata information that needs to be included in the license (output controls) when creating a license.

This flow is summarized in the following figure where arrows show the flow of information.



In this flow, the CPIXF finds its natural place in all exchanges between the DRM system and Encryption engine and between the DRM system and MPD generator.

Electronic Sell-through

In order to make available its content in a defined and controlled quality, a Content Provider is preparing it. Preparation includes transcoding to the desired format and encryption of the resulting segments. The content owner is generating also the content key(s). At the end of the process, DASH content is ready and stored along with the content key(s).

Later the content owner distributes the prepared content to multiple locations with the addition of metadata describing it. Content becomes then saleable on multiples Portals. In parallel, the Content Provider distributes the content key(s) to any authorized DRM system. A DRM system is authorized if it is one used by one of the Portal that has this content for sale.

In this flow, the CPIXF finds its natural place in all export of content key(s) from the Content Provider to the DRM systems. The Content Provider could also use the CPIXF for securely store content keys along with content.

SD, HD, AND UHD CONTENT

A Content Provider typically controls keys and license policy for a Presentation, and requires some type of client authentication (is playback requested by a subscriber?) and content authorization (does that subscriber have rights to the requested content and license?). For instance, a purchase or subscription might only include access to high definition content (HD), because ultra-high definition (UHD) content is sold at a higher price. Rights may also be limited by rental period, by location, by device, etc.

SD, HD, and UHD Adaptation Sets may require different keys and licenses because each requires a different security level and output controls. For instance, it is typical to allow SD content to be output over analog interfaces, but restrict HD content to protected digital outputs such as HDMI with HDCP. HD content may also require separate keys for audio and video because audio keys are typically less protected in devices. UHD content may require a hardware protected video path and HDCP 2.2 output protection.

A Content Provider can enable these scenarios by determining the mapping of KIDs to Adaptation Sets in CPIXF, then specifying the license policy required for each KID with DRM license Providers. Each player should determine in advance what content it is entitled to, and what level of content protection it supports; and then request the necessary licenses before attempting playback. A request will usually be authenticated and authorized by the service provider according to their business rules before providing the client an access token it can use to request the type of license authorized. The DRM license provides cryptographic enforcement of the entitlement authorized.

Separate from CPIXF, there is a contractual relationship of rights and responsibilities flowing from the copyright holder to each entity that handles the content and keys. Entities that handle unencrypted content or keys are contractually required to protect them, and are typically given cryptographic certificates containing the keys necessary to send and receive media keys protected by CPIXF key encryption.

CONCLUSION

This paper presented a secure mechanism for exchanging sensitive multimedia information when preparing value-added content. It makes no assumption on the overall trust framework and supports several use cases, from simple ones to more complex.

It provides an additional step in interoperability when enabling protected content with DRMs.

In next steps, the proponents will propose extensions allowing to fully supporting common use cases, such as on-demand content and live content. The first one is a quite straight forward use of the CPIXF while the latter requires the management of key rotation.

REFERENCES

1. [DASH-CPIXF] DASH-IF Implementation Guidelines: Content Protection Information Exchange Format, March 2015

2. [DASH] ISO/IEC 23009-2:2014 Information technology - Dynamic adaptive streaming over HTTP (DASH) - Part 1: Media presentation description and segment formats.
3. [DASH-IOP] DASH-IF Guidelines for Implementation: DASH264/AVC Interoperability Points, August 2014.
4. [RFC6030] IETF RFC 6030, “Portable Symmetric Key Container (PSKC)”, October 2010.

ACKNOWLEDGEMENTS

The authors would like to thanks the DASH-IF forum for its support in conducting this work and more specifically, all attendees to the DRM group who actively participated in the specification of this implementation guideline.