ETSI TS 103 799 V1.1.1 (2021-04)

Publicly Available Specification (PAS); DASH-IF Content Protection Information Exchange Format

CAUTION

The present document has been submitted to ETSI as a PAS produced by DASH-IF and approved by the Joint Technical Committee (JTC) Broadcast of the European Broadcasting Union (EBU), Comité Européen de Normalisation ELECtrotechnique (CENELEC) and the European Telecommunications Standards Institute (ETSI).

DASH-IF is owner of the copyright of the document DASH-IF CPIX and/or had all relevant rights and had assigned said rights to ETSI on an "as is basis". Consequently, to the fullest extent permitted by law, ETSI disclaims all warranties whether express, implied, statutory or otherwise including but not limited to merchantability, non-infringement of any intellectual property rights of third parties. No warranty is given about the accuracy and the completeness of the content of the present document.

Reference

DTS/JTC-060

Keywords

DASH, encryption, internet, PAS, video

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

Copyright Notification

Contents

Intellectual Property Rights 5
Foreword 5
Modal verbs terminology 5
Introduction 6
1 Scope 7
2 References 7
2.1 Normative references 7
2.2 Informative references 8
3 Definition of terms, symbols and abbreviations 8
3.1 Terms 8
3.2 Symbols 8
3.3 Abbreviations 8
4 Use Cases and Requirements 9
4.1 Introduction 9
4.2 Overview of the End-to-End Architecture 9
4.3 Use Cases for the Preparation of Content 11
4.3.1 Introduction 11
4.3.2 On-Demand Content 11
4.3.3 Live Content 12
4.3.4 Catch-up 12
4.3.5 Electronic Sell Through 12
4.4 Exchange over an Interface 13
4.4.1 Introduction 13
4.4.2 Content Key Delivery to One Entity 13
4.4.3 Secure Content Key Delivery to Several Entities 13
4.4.4 Content Key Delivery with Usage Rules 13
4.4.4.1 Introduction 13
4.4.4.2 Label Filter 14
4.4.4.3 Key Period Filter 14
4.4.4.4 Policy-based Filters 14
4.4.5 Content Key Delivery with DRM Signaling 14
4.4.6 Incremental Update and Extension of the document 15
4.4.7 Content Key Hierarchy Delivery for Content Packaging 15
4.4.8 Root Key Delivery for License Server Operation 16
4.5 Workflow Examples 16
4.5.1 Encryptor Producer and Encryptor Consumer 16
4.5.1.1 Introduction 16
4.5.1.2 Encryptor Producer 17
4.5.1.3 Encryptor Consumer 17
4.5.1.4 Multiple Producers 18
5 XSD Schema Definition 19
5.1 Introduction 19
5.2 Requirements 19
5.3 Structure Overview 20
5.4 Hierarchical Data Model 22
5.4.1 Introduction 22
5.4.2 CPIX Element 22
5.4.3 DeliveryDataList Element 23
5.4.4 DeliveryData Element 24
5.4.5 ContentKeyList Element 26
5.4.6 ContentKey Element 26
5.4.7 DRMSystemList Element 29
5.4.8 DRMSystem Element 29

5.4.9 HLSSignalingData Element 31
5.4.10 ContentKeyPeriodList Element 32
5.4.11 ContentKeyPeriod Element 33
5.4.12 ContentKeyUsageRuleList Element 33
5.4.13 ContentKeyUsageRule Element 34
5.4.14 Usage Rules Filters 35
5.4.14.1 Introduction 35
5.4.14.2 KeyPeriodFilter Element 36
5.4.14.3 LabelFilter Element 36
5.4.14.4 VideoFilter Element 37
5.4.14.5 AudioFilter Element 38
5.4.14.6 BitrateFilter Element 39
5.4.15 UpdateHistoryItemList Element 39
5.4.16 UpdateHistoryItem Element 40

6 Key Management 41
6.1 Key Encryption in the CPIX Document 41
6.1.1 Introduction 41
6.1.2 Keys Used to Secure the CPIX Document 41
6.1.3 Authenticated Encryption 42
6.1.4 Digital Signature 42
6.1.5 Mandatory Algorithms 42
6.2 Key Rotation Support 43
6.3 Hierarchical Keys 43

Annex A (normative): CPIX XSD Schema 44

History 48

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

Foreword

This Technical Specification (TS) has been produced by Joint Technical Committee (JTC) Broadcast of the European Broadcasting Union (EBU), Comité Européen de Normalisation ELECtrotechnique (CENELEC) and the European Telecommunications Standards Institute (ETSI).

NOTE: The EBU/ETSI JTC Broadcast was established in 1990 to co-ordinate the drafting of standards in the specific field of broadcasting and related fields. Since 1995 the JTC Broadcast became a tripartite body by including in the Memorandum of Understanding also CENELEC, which is responsible for the standardization of radio and television receivers. The EBU is a professional association of broadcasting organizations whose work includes the co-ordination of its members' activities in the technical, legal, programme-making and programme-exchange domains. The EBU has active members in about 60 countries in the European broadcasting area; its headquarters is in Geneva.

European Broadcasting Union
CH-1218 GRAND SACONNEX (Geneva)
Switzerland
Tel: +41 22 717 21 11
Fax: +41 22 717 24 81

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 ETSI deliverables except when used in direct citation.

Introduction

The present document defines a container allowing the exchange between entities of content protection information typically made of keys used for encrypting content and any associated DRM specific information. There may be one or several keys and these keys may be protected by one or several DRMs, hence there may be one or several DRM specific information. There is no assumption on the entities exchanging this information, but it is not expected that a client device will use this exchange format. The goal is to allow entities involved in the content preparation workflow to get the content protection information so that, for example a DASH MPD can be generated with all content protection information.

Because the defined container is not made for a specifically defined content preparation workflow but is generic, conformance is not considered to be a critical part of CPIX. As a consequence, no conformance is defined for the present document.

1 Scope

The scope of the present document is to define a Content Protection Information Exchange (CPIX) Format. A 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 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.

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.

Referenced documents which are not found to be publicly available in the expected location might be found at https://docbox.etsi.org/Reference.

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 necessary for the application of the present document.

[1] Guidelines for Implementation: "DASH-IF Interoperability Points", version 4.3, November 2018.

NOTE: Available at https://dashif.org/guidelines/.

[2] DASH-IF registry of DRM System IDs.

NOTE: Available at https://dashif.org/identifiers/content_protection/.

[3] IETF RFC 6030: "Portable Symmetric Key Container (PSKC)", October 2010.

[4] W3C® Recommendation 5 April 2012: "W3C XML Schema Definition Language (XSD) 1.1 Part 2: Datatypes", David Peterson et al.

NOTE: Available at https://www.w3.org/TR/xmlschema11-2/.

[5] W3C® Recommendation 11 April 2013: "XML Encryption Syntax and Processing Version 1.1", Donald Eastlake, Joseph Reagle, 10 December 2002.

NOTE: Available at https://www.w3.org/TR/xmlenc-core/.

[6] W3C® Recommendation 11 April 2013: " XML Signature Syntax and Processing Version 1.1", Donald Eastlake, Joseph Reagle, David Solo, et al. (Second Edition). 10 June 2008.

NOTE: Available at https://www.w3.org/TR/xmldsig-core/.

[7] ISO/IEC 23001-7:2016: "Information technology -- MPEG systems technologies -- Part 7: Common encryption in ISO base media file format files", February 2016.

NOTE: Available at https://www.iso.org/standard/68042.html.

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.

Not applicable.

3 Definition of terms, symbols and abbreviations

3.1 Terms

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

content: one or more audio-visual elementary streams and the associated MPD if in DASH format

content key: cryptographic key used for encrypting part of the content

content key context: portion of a media stream which is encrypted with a specific content key

content protection: mechanism ensuring that only authorized devices get access to content

document key: cryptographic key used for encrypting the content key(s) in the CPIX document

DRM signaling: DRM specific information to be added in content for proper operation of the DRM system when authorizing a device for this content

NOTE: It is made of proprietary information for licensing and key retrieval.

Protection System Specific Header (PSSH): part of an ISO BMFF file

NOTE: This box contains DRM Signaling.

3.2 Symbols

Void.

3.3 Abbreviations

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

AES	Advanced Encryption Standard
BMFF	Base Media File Format
CBC	Cypher Block Chaining
CDN	Content Delivery Network
CMS	Content Management System
CPIX	Content Protection Information eXchange
DASH	Dynamic Adaptive Streaming over HTTP
DRM	Digital Right Management
EPG	Electronic Program Guide
FPS	Frames Per Second
HD	High Definition
HDR	High Dynamic Range

HDS	HTTP Dynamic Streaming
HLS	HTTP Live Streaming
ISO	International Organization for Standardization
IV	Initialization Vector
KID	Key IDentifier
MAC	Message Authentication Code
MPD	Media Presentation Description
OD	Optional with Default value
PKCS	Public Key Cryptography Standards
PSSH	Protection System Specific Header
RSA	Rivest, Shamir, & Adleman
SD	Standard Definition
SHA	Secure Hash Algorithm
UHD	Ultra High Definition
URI	Uniform Ressource Identifier
UUID	Universally Unique IDentifier
VOD	Video On Demand
WCG	Wide Color Gamut
XML	eXtensible Markup Language
XSD	XML Schema Definition

4 Use Cases and Requirements

4.1 Introduction

Content Keys and DRM Signaling, a.k.a. content protection information, 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.

This clause presents different use cases where such exchanges are required. Clause 4.2 is an overview of the general context in which exchange of content protection information is happening, clause 4.3 describes some workflows for content creation and clause 4.4 goes in the details of how content protection information can be exchanged over an interface between two entities.

4.2 Overview of the End-to-End Architecture

This clause gives a general overview of the context in which content protection information needs to be exchanged between entities in the backend. It completes clause 7.5 of [1] by putting more emphasis on the backend aspects.

This clause takes DASH content as an example for providing more specific and clear understanding, but this can be generalized to other streaming formats, such as HLS.

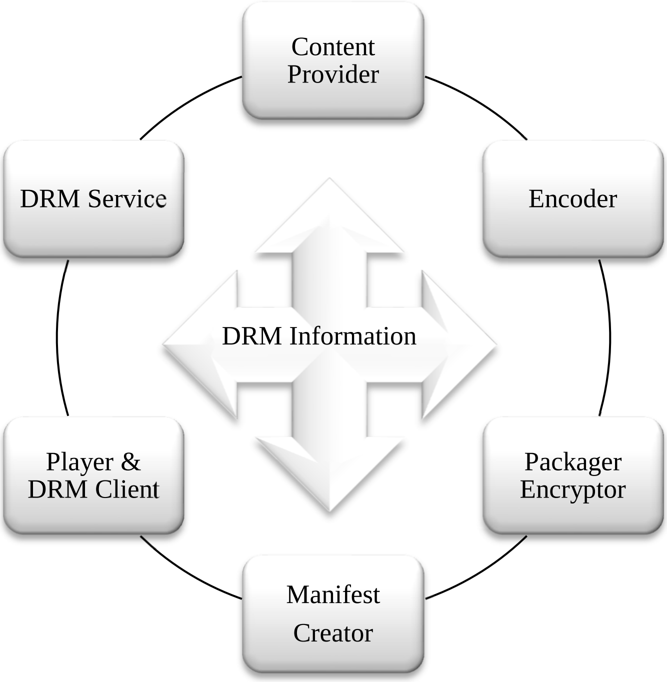

Figure 1: Logical roles that exchange DRM information and media

Figure 1 shows logical entities that may send or receive DRM information such as media 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 media keys and asset identifiers, can differ; so various information flows are possible. This is an 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 media in a specified set of formats with different bitrates, resolutions, etc., possibly determined by the publisher.

- **Packager/Encryptor:** A service provider who encrypts and packages media, inserting DRM Signaling and metadata into the media files. In the case of DASH packaging, this consists of adding the `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 one or more `PSSH` boxes containing license acquisition information (from the DRM Service). 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., then send that information to other entities that need it, including the DRM Service and Streamer, and probably the Content Provider. However, the Packager could receive that information from a different point of origin, such as the Content Provider or DRM Service.

- **Manifest Creator:** A service provider which generates the media manifests which group the various media files into a coherent presentation. These manifest files may contain DRM Signaling information. For DASH, the MPD Creator is assumed to create one or more types of DASH MPD files and provide indexing of Segments and/or `sidx` indexes for download so that players can byte range index Subsegments. The MPD shall 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`** 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 Service.

- **DRM Client:** It gets information from different sources: media manifest files, media files, and DRM licenses.

- **DRM Service:** The DRM Service creates licenses containing a protected Content Key that can only be decrypted by a trusted DRM 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 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. For DASH, the DRM Service typically shall supply the Streamer and the Packager license acquisition information for each UUID **`ContentProtection`** 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.

4.3 Use Cases for the Preparation of Content

4.3.1 Introduction

This clause describes some workflows for content preparation where content protection information is exchanged between or carried through some entities.

As for the previous clause, this clause takes DASH content as an example for providing more specific and clear understanding, but this can be generalized to other streaming formats, such as HLS.

4.3.2 On-Demand Content

The flow for preparing On-Demand Content requires that a media asset is available non-encrypted, ideally in the maximum resolution so that an adaptive streaming presentation can be prepared.

One possible flow is that a Content Management System (CMS) creates a workflow ensuring that DASH Content is prepared. 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 Keys or requests them from a DRM system. The DRM system also provides `PSSH` boxes to be added to the media files, as well as **`ContentProtection`** elements to be added to the MPD file. When the encrypted DASH Content is ready, the MPD is generated by an MPD Generator. It asks the DRM system the required DRM Signaling 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 Figure 2 where arrows show the flow of information.

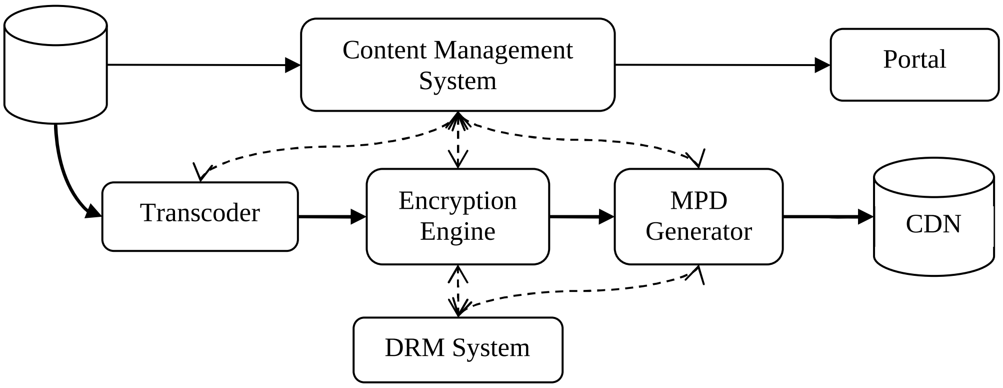

Figure 2: Example of workflow for On-Demand Content preparation

4.3.3 Live Content

Metadata is regularly imported with new or updated information. Metadata can include different type of information on the EPG events such as the duration of the event, the list of actors, the output controls usage rules, a purchase window, etc.

Content is continuously received, transcoded in the desired format and encrypted if any type of entitlement is required.

One or many Content Keys can be used if key rotation is used or not. Such setting is static, and configuration is hard coded in the relevant equipment, hence a CMS is not required for this workflow to operate. As for Content on-Demand, keys are generated by the encryption engine or the DRM system and are available to all DRM systems and the encryption engine at the right moment depending on how these keys are used. The encoder requests to the DRM systems their specific signaling, if any, to be added in the MPD.

Encrypted segments and the media manifest are uploaded on a CDN making it available to users.

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).

This flow is summarized in Figure 3 where arrows show the flow of information.

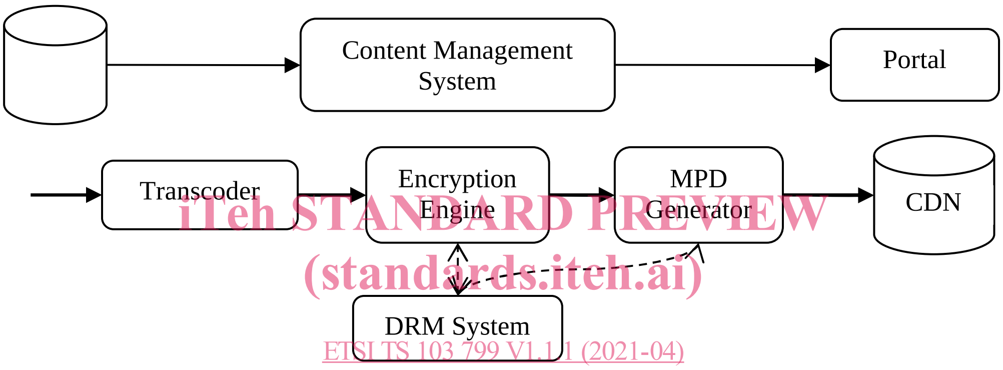

Figure 3: Example of workflow for Live Content preparation

4.3.4 Catch-up

Live Content has already been encoded and encrypted (if required) for Live unicast. All DRM systems have access to the keys.

Additional metadata may be required for ensuring that events are effectively available in catch-up. These are made available to the Portal and some Live events are identified as being able to be replayed as On-demand. Optionally, the operator may choose to replace the advertising content with targeted ads.

4.3.5 Electronic Sell Through

In order to make available its Content in a defined and controlled quality, a content owner 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, Content is ready and stored along with the Content Key(s).

Later the content owner distributes the prepared Content to retail platforms along with metadata so that it becomes marketable on multiples Portals. In parallel, the content owner 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.

4.4 Exchange over an Interface

4.4.1 Introduction

This clause gives details on how content protection information is exchanged or transferred over an interface between two or more entities.

4.4.2 Content Key Delivery to One Entity

In the simplest use case shown in Figure 4, content protection information is made of a Content Key. One entity sends a Content Key to the other entity.

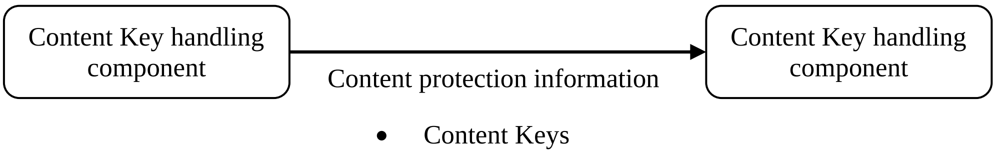
Content Key handling component
Content protection information
Content Key handling component
• Content Keys

Figure 4: Content Key delivery to one entity

The primary data model carried by content protection information document is made of one to many Content Keys with their associated KIDs. Any context or meaning is attributed externally. The document simply serves as a standard way to serialize Content Keys for delivery.

4.4.3 Secure Content Key Delivery to Several Entities

This use case shown in Figure 5 is an extension of the use case of clause 4.4.2 and is compatible with the use cases presented in the following clauses.

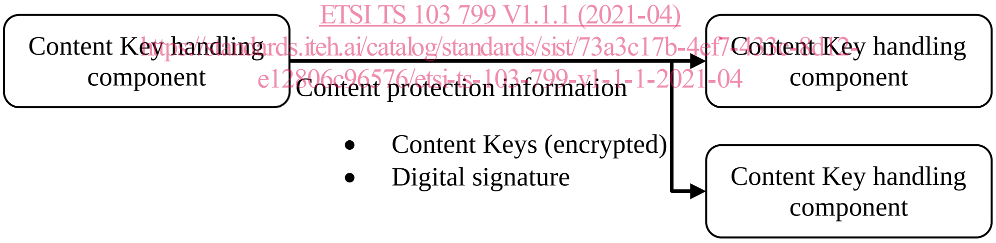
Content Key handling component
Content protection information
Content Key handling component
Content Key handling component
• Content Keys (encrypted)
• Digital signature

Figure 5: Secure Content Key Delivery to Several Entities

The entities exchanging Content Keys may want to rely upon a trust relationship that ensures authentication and privacy of communications. Such a mechanism can be provided by the communication protocol used to deliver the document, but the document can also be self-protected. CPIX documents can deliver Content Keys in encrypted and digitally signed form, enabling confidentiality, authentication and nonrepudiation.

In situations with more than one recipient, the document allows each one to decrypt the Content Keys using its own private key.

4.4.4 Content Key Delivery with Usage Rules

4.4.4.1 Introduction

These use cases are extension of the use case of clause 4.4.2 and present different rules that can be applied on a Content Key when delivered to an entity as shown in Figure 6. Each usage rule defines a set of filters that are used to define a Content Key Context. If a rule match is found, the Content Key referenced by the usage rule is to be used to encrypt the Content Key Context defined by the rule.