Use of MPEG-21 for License Protection and Key Management in DRM Systems

Eva Rodríguez, Isabel Gallego, Jaime Delgado
Universitat Politècnica de Catalunya, Departament d'Arquitectura de Computadors, Campus Nord, Mòdul D6, Jordi Girona 1-3, E-08034 Barcelona, Spain
{evar, isabel, jaime.delgado}@ac.upc.edu

Abstract

This work proposes a solution to the problem of the secure management and distribution of licenses and keys associated to protected resources. We have identified different use cases to illustrate the requirements of a DRM system including download, superdistribution, streaming and groups or domains of users and/or devices of a user. The different mechanisms that we propose are based in MPEG-21 standard. These mechanisms enable the secure distribution of the protected content, licenses and keys, for the different scenarios analysed. Moreover, the solutions provided support joint and separate distribution of content, licenses and keys.

1. Introduction

There are different DRM initiatives that have specified mechanisms to manage licenses and keys. Nevertheless, there is no general solution, since some of them are associated to specific applications like the mobile environment (Open Mobile Alliance [1]) or broadcast applications (Digital Media Project [2] or TV-AnyTime [3]). Furthermore, most of these initiatives do not specify how to manage in a secure way the licenses and keys associated to protected digital content.

In order to propose a general a solution to this problem, first we have identified a set of representative scenarios considered by the most relevant DRM initiatives, including content download, streaming and superdistribution. Second, we have chosen MPEG-21 [4], the most general and standard DRM initiative, as basis for our solution that has the aim to provide general mechanisms for the management of security information (licenses and keys). Third, we have considered two different options for the use cases studied: separate and joint distribution of protected content and licenses. Finally, we have specified the mechanisms that provide a general solution for the secure management of licenses and keys taking into account separate and joint distribution of security information and digital content. The proposed solution is based on the utilisation of different elements specified in the MPEG-21 standard [4].

2. Security in current DRM Systems

This section presents standard initiatives that deal with the protection and governance of multimedia content. Currently, the most representative initiatives are the following:

- MPEG-21
- Open Mobile Alliance DRM
- Digital Media Project

2.1 MPEG-21

MPEG-21 [4] standard is divided into several parts, which deal with different aspects of multimedia information management.

Part 4 of the MPEG-21 standard, Intellectual Property Management and Protection (IPMP) Components [5] provides mechanisms for users to protect a Digital Item (DI), which is the fundamental unit of distribution and transaction in the MPEG-21 framework, and its declaration using a specified schema. Mainly, it defines a language to provide protection and governance (i.e. control of content usage rights and conditions by means of a digital license) to any part of a DI. The IPMP DIDL protects a part of the hierarchy of a DI, and provides mechanisms to associate appropriate identification and protection information to the protected part.

IPMP Components also defines the information regarding the protection of a DI. This information falls into two categories: information about protection and governance related to the whole DI and information about the specific protection applied to a certain part of a protected DI. The general protection information includes the collection of licenses and lists of protection tools used, which can be later referred from specific protected elements. On the other hand, the specific information includes the specific tools and protection keys that have been applied, the licenses which are specific to that content, etc. These two categories of information are expressed with two top-

0-7695-3030-3/07 $25.00 © 2007 IEEE
DOI 10.1109/AXMEDIS.2007.20

level elements: IPMPGeneralInfoDescriptor and IPMPInfoDescriptor respectively. IPMP Components defines the *Tool* element that can be used to specify the IPMP tool information required to protect the Digital Item or its parts. IPMP tools are modules that perform (one or more) IPMP functions such as authentication, encryption, decryption, signatures, watermarking, etc.

Figure 1 shows the structure of the *Tool* element that explicitly describes the IPMP tool used to protect the content and includes the following information: the *IPMPToolID* element that represents the universally unique identifier for an IPMP tool. The *Inline* element is a container to carry the binary of the tool. The *ConfigurationSettings* element is a container to carry detailed configuration settings for a specific IPMP tool. Three other optional elements can be included under the *Tool* element. The *InitializationSettings* that was designed to hold information required to initialise the tool, and the format of this data will depend on the nature of the tool itself. The *RightsDescriptor* element that is used to include governance information for the tool. Finally, the *Signature* element ensures integrity and authenticity for the description information provided for the IPMP tool.

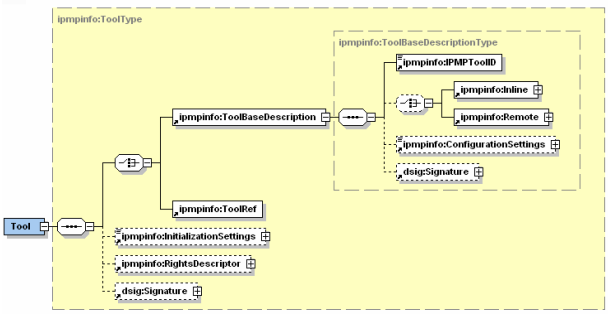

Figure 1. Structure of the Tool Element

Part 5 of the MPEG-21 standard [6] defines a Rights Expression Language (REL) for issuing rights for users to act on digital resources. MPEG-21 REL standard specification [6] provides mechanisms to encrypt the contents of a license. These mechanisms make use of the XML Encryption Syntax and Processing (XML Encryption) [7]. The MPEG 21 REL defines the *encryptedLicense*, *encryptedGrant* and *encryptedGrantGroup* elements that contain the encrypted content of a license, grant or grant Group respectively. Nevertheless, this standard does not specify how sensible information within a license can be encrypted, for example the content encryption keys that can be delivered to users within licenses. For this purpose, in [8] we proposed the definition of the *protectedResource* element. This element can be used for resources that have been protected with some form of encryption (symmetric key and/or public key). The *protectedResource* element forms part of the multimedia extension one of the MPEG-21 REL standard. This extension has been defined in the Mobile and Optical Media (MAM) Profile [9] that has been defined to facilitate the interoperability with OMA DRM REL [10].

MPEG-21 REL can be extended to support new business models defining extensions. On the other hand, the entire REL may need to be restricted to some profiles for interoperability or optimisation purposes. Three profiles have been specified and included in this part of the standard as amendments. The first one, so-called Mobile And optical Media (MAM) profile [9] addresses the needs of the mobile and optical media domains. The second one, the Dissemination and Capture (DAC) profile [11], was designed to be able to represent the concept of the OMA DRM v2.0 Extensions for Broadcast Support [12]. Finally, the Open Release Content (ORC) profile [13] has been specified to support the different types of Creative Commons [14] licenses.

In the REL MAM profile the security data to protect the content was included, as explained above, defining the *ProtectedResource* element (Figure 2). This element represents a piece of content that is protected with some form of (symmetric key and/or public key) encryption. It is made up of the following elements: the *r:digitalResource* that specifies the resource under consideration. The *xenc:EncryptedData* a placeholder to carry the information about encryption of the resource. And the *xenc:EncryptedKey* contains information about encryption of the key used to encrypt the resource.

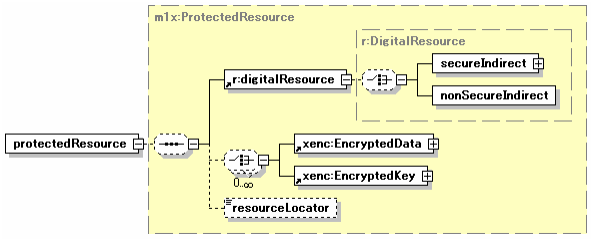

Figure 2. Structure of the *ProtectedResource* element

2.2 Open Mobile Alliance

The Trust and Security Model of Open Mobile Alliance [12] is based on the DRM Agent that embodies a trusted environment within which DRM Content can be securely consumed. Its role is to enforce permissions and constraints and to control access to DRM Content.

The basic aspects for distributing DRM Content in OMA can be summarised as follows:

- Content Protection: Content is packaged in a secure content container (DCF). DRM Content is encrypted with a symmetric content encryption key (CEK). The CEK needed to unlock DRM Content inside a DCF is contained within a Rights Object (RO). Thus it is not possible to access DRM Content without a RO. DRM Content can only be used as specified in a RO. OMA DRM includes a mechanism allowing a DRM Agent to verify the integrity of a DCF, protecting against modification of the content by some unauthorised entity.
- Rights Object Protection: ROs are used to specify consumption rules for DRM Content. The Rights Expression Language defined by OMA DRM specifies the syntax and semantics of permissions and constraints governing the usage of DRM Content. A RO is protected using a rights encryption key (REK). The REK is used to encrypt sensitive parts of the RO, such as the CEK. In addition, the RO is digitally signed by the Rights Issuer. During delivery, the REK is cryptographically bound to the target DRM Agent. In this way only the target DRM Agent can access the RO, and thus the CEK.

2.3 Digital Media Project Forum

Digital Media Project Forum is developing a series of specifications for Interoperable DRM called Interoperable DRM Platform (IDP) [15] to satisfy the needs of a broad range of value-chain users. The DMP approach is based on identify prominent use cases used to focus the development of specifications. Chillout [16] is the Open Source DRM Software implementing the open Digital Media Project's (DMP) Interoperable DRM Platform (IDP) specification.

All the information to control the content usage is defined in the DMP Content Information (DCI) based on a DMP defined subset of MPEG-21 Digital Item Declaration Language (DIDL) [17] and extended by many DMP namespaces. The DMP DCI structure allows the ordered aggregation of Content Identifiers, DMP-specific information, DRM information and Licenses with Content and Content Elements.

3. Open Issues in DRM security aspects

Most of the current initiatives that specify DRM systems or the elements that form these systems does not specify how to securely manage licenses and keys. Then, we have checked minimum security requirements in DRM, for these initiatives, to determine where can be needed keys and licenses to encrypt, sign or deal with certificates.

Table 1. Protection aspects in DRM OMA and DMP initiatives

	OMA	DMP	MPEG-21
Content	Content is stored on Content Issuer	Content is stored on Content Provider Storage	Out of scope
License	Licenses are stored in Rights Issuer or also in Content Issuer and can be signed or encrypted.	Licenses are stored on License Provider Device and can be signed using License Provider certificate (but not encrypted).	Out of scope
Key	Keys are stored in Key Management Centre and can be encrypted.	Keys are Encrypted with the PAV Device Public or the Domain Key in case of Domain License	Out of scope
Trust	Device is trusted	Device is trusted	Device can be trusted or non-trusted

Table 1 summarises the study performed. Based on this study we decided to base our solution in the MPEG-21 standard, as it is one of most general initiatives that defines a multimedia framework for the delivery and consumption of multimedia content in a controlled way. Moreover, we have chosen MPEG-21 to avoid the restrictions regarding the management and protection of content, licenses and keys that the other standard initiatives state (see Table 1).

In order to specify a general solution for the secure management of licenses and keys in DRM systems, we have selected representative use cases that different DRM initiatives, as OMA [1] or DMP [2], consider to illustrate specific requirements for our system. These use cases and combinations thereof cover the current most common ways of distribution and superdistribution of multimedia content to end-users taking into account groups of users and/or groups of devices. For each use case, we have defined how content is protected, governed and packaged taking into account the different modules of a DRM architecture (MIPAMS [18]). Moreover, we also have specified for each use case how the rights are enforced, and how the content is unprotected and rendered.

4. Use Cases: DRM Scenarios focusing in security

This section presents different use cases to illustrate on one hand protection and governance of multimedia content, and on the other hand the consumption of the protected content that includes the enforcement of rights, unprotection and processing of the multimedia content.

We have considered most common scenarios that different DRM initiatives have taken into account [1] [2] [3]. The uses cases that we analysed to illustrate specific requirements of our system include download of multimedia content, streaming, domains of users and/or devices of a user and superdistribution of multimedia content.

The use cases presented in this section are based in DMAG-MIPAMS [18] that is an architecture to manage multimedia information taking into account digital rights management (DRM) and protection. The modules of the DRM architecture involved in the selected use cases are the following:

- Intermediary: Usually is an integral part of the trusted client with which the client application must interact to enforce DRM. Main functionalities include: require certification to Supervision Server, require verification to Supervision Server, require online authorization to Governance Server, license download from Governance Server, send offline operations to Supervision Server, download unprotection tools from Protection Server, etc.
- Content Server: Offers the following functionalities, enable users to browse/select content, provide the content that final users may request to user applications, encode and add metadata to received raw contents from providers, register the digital items/objects describing resources (metadata), etc.
- Protection Server: Offers a service for protecting the content or digital objects, which become protected objects, mainly using encryption techniques and scrambling.
- Governance Server: Performs the following functionalities, generate licenses (end-user, distribution, etc.), store licenses, perform online license-based authorization, translate licenses, etc.
- Supervision Server: It authenticates and supervises actors and system components (users, tools, device components, etc.) and receives and store action reports.

The purpose of this analysis is to determine how licenses and keys can be managed and delivered securely to users within DRM architectures.

4.1 Content Download

In this scenario, depicted in Figure 3, a user wants to download a music album. First, the user connects to a distributor Web Site, and selects the album that she wants to purchase. Then, the Intermediary connects to a Content Server to request the content that is protected by the Protection Server and sent to the user. After downloading the protected content, the user purchases a license that grants her the right to play the content during a certain interval of time. The intermediary initialises a connection with the Governance Server to acquire the associated rights to the content (License with the content encryption key that is requested to the Protection Server) and a protected version of the license is sent to the user. Finally, the user can perform an action, i.e. a play, and if the Governance Server authorises this action the content is unprotected and displayed.

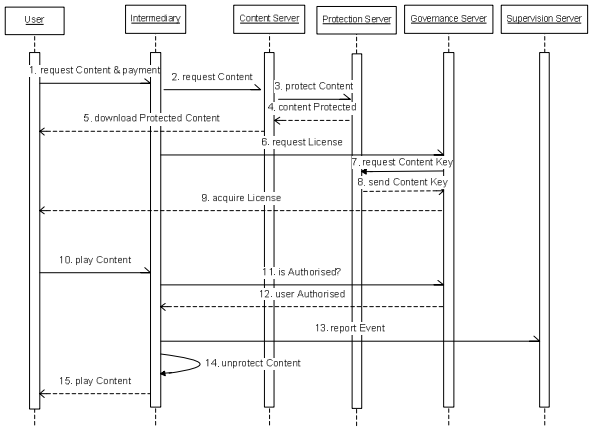

Figure 3. Content Download Use Case

4.2 Streaming

In this scenario (see Figure 4) a user that wants to download a multimedia stream must previously acquire from the Content Server information related with the streaming session (Token Streaming Session). Afterwards the user can purchase a license to obtain the associated rights to the stream (License and stream master key). Finally, if the user is authorized by the Governance Server, he can access to the different streams.

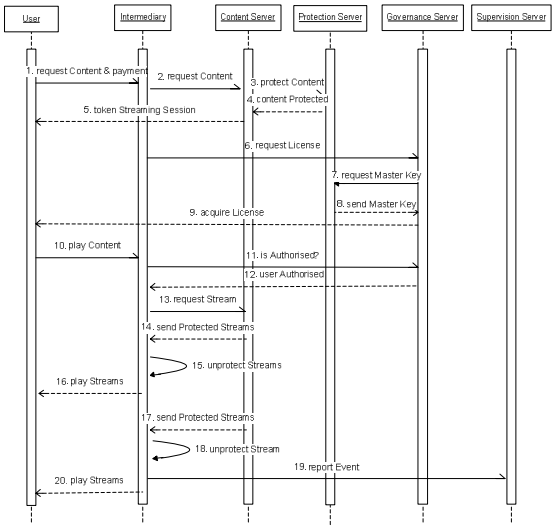

Figure 4. Streaming Use Case

4.3 Superdistribution

In this scenario a user that has downloaded content from a Content Server can distribute this protected content to others users and/or devices. The user can transfer the protected content, but the receiving user or device must previously acquire the associated rights to access to the unprotected content. This is shown in Figure 5.

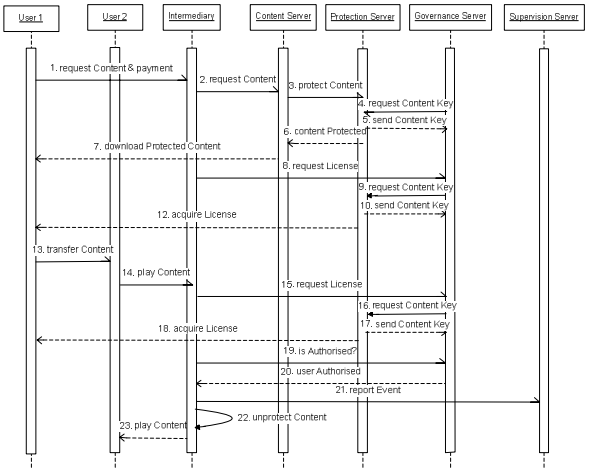

Figure 5. Superdistribution Use Case

4.4 Domains

In this scenario (see Figure 6) a set of users and/or devices can share content if they are previously joined to a domain (Domain-License). The users and/or devices must acquire the rights associated to a content and to a specific domain (Content-Domain-License). A user and/or device can download the protect content and acquire the rights associated to this content as usual before performing an authorised action. At the same time this user and/or device can transfer this protected content with the associated rights to another user and/or device of the same domain.

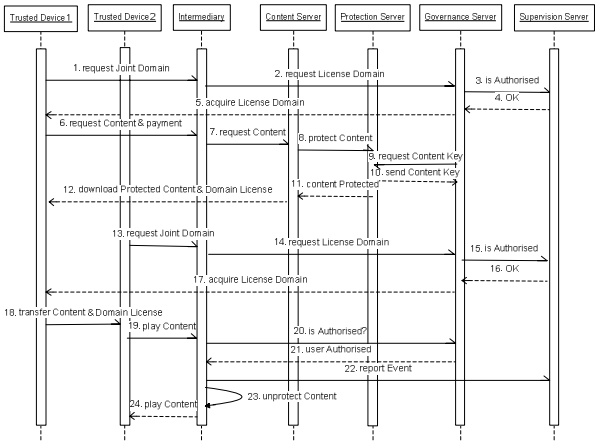

Figure 6. Domains Use Case

5. Securing Standard DRM initiatives

This section presents the solution that we propose for managing licenses and content encryption keys in a secure way for the different scenarios analysed. For this purpose three mechanisms have been defined taking into account not only the MPEG-21 IPMP Components standard specification [5], that specifies how digital content and Digital Items [16] can be protected and how the protection and governance information can be associated to the protected content, but also the MPEG-21 Rights Expression Language (REL) [6] and OMA DRM specification [19].

In the first solution that we propose, the protected content and licenses are delivered separately to the user. In this case, the licenses contain the key used to encrypt the content in a protected form. In the second solution, the protected content and the licenses are delivered together to the user within a digital object, but in this case the key that will be used to unencrypt the content is within the license in a protected form. Finally, the third solution proposed considers that the protected content and the licenses governing this content are delivered together to the user within a digital object. In this case, the content encryption key is within the protection information in protected form or the protection information has a reference to a service where the content encryption key can be retrieved.

Table 2 summarises the different ways of secure delivering of licenses and keys to users for the four different use cases presented in Section 4.

Table 2. Licenses and key management for the use cases

	Download	Streaming	Superdist ribution	Domains
Separate distribution of protected content and licenses	X	X	X	
Join distribution of protected content and licenses (contain the content key)		X		
Join distribution of protected content, licenses and content keys	X	X		X

For two of the solutions presented, content keys will be delivered to users within licenses. Then, it is important to define mechanisms to enable the protection of sensible parts of licenses.

5.1 MPEG-21 security elements

This section presents the elements of different parts of MPEG-21 standard that we have chosen for our solution. Most of these elements have been included in the standard from our proposals [8][20][21].

For the secure management of keys we will consider the *protectedResource* element that we proposed in [11] and that currently form part of the MPEG-21 REL MAM profile [9]. This element can be used for resources that have been protected with some form of encryption (symmetric key and/or public key). The *protectedResource* element contains: the name of the resource that has been protected, information about the encryption of the resource, information about encryption of the key or keys used to encrypt the resource and the location of the associated resource. The other element that our solution will consider is the *IPMPInfoDesciptor* element that we proposed in [20] [20] and that currently forms part of the MPEG-21 IPMP Components standard specification [5]. The *IPMPInfoDesciptor* element under the *RightsDescriptor* element was defined to associate protection information with protected licenses governing multimedia content. Nevertheless, this solution only can be used for joint distribution of content and licenses, because although licenses could be protected in any way and at any level of granularity, they always will be within or associated through a reference or through a service reference to an MPEG-21 IPMP DIDL document.

For the secure management of licenses our solution makes use of the *RightsDescriptor* element of the IPMP Info schema that we proposed in [5]. This element can be used as placeholder for the protected license.

5.2 Separate distribution of protected content and licenses

This approach considers that the resource and the license are delivered separately. Then, the digital object contains the resource protected, and the license contains the governance rules and the key that will be used to unprotect the content. This solution makes use of the IPMP Components standard specification to protect digital assets and of the MPEG-21 REL to define the rights and conditions of use of digital assets. Finally, it makes use of the protected resource element that we proposed and that currently forms part of the Multimedia Extension One of the MPEG-21 REL [6].

In order to illustrate how content, licenses and keys are delivered to users, we present a content consumption scenario in which a user receives a digital object with a protected music track and a license with the usage rules and the content key in a protected way. Figure 7 shows the Digital Item with the protected asset.

```
<DIDL>
  <Container>
    <Item>
      <Descriptor id="Track1">
        <Statement mimeType="text/plain">Blue suede
shoes</Statement>
      </Descriptor>
      <Component>
        <Resource mimeType="application/ipmp">
          <ipmpdidl:ProtectedAsset mimeType="audio/mp3">
            <ipmpdidl:Info>
              <ipmpinfo:IPMPInfoDescriptor>
                <ipmpinfo:Tool>
                  <ipmpinfo:ToolBaseDescription>
                   <ipmpinfo:IPMPToolID>
                     urn:mpegRA:mpeg21:IPMP:GFTR977
                     </ipmpinfo:IPMPToolID>
                   <ipmpinfo:Remote
ref="urn:IPMPToolsServer:DRMS06565_FGR"/>
                  </ipmpinfo:ToolBaseDescription>
                </ipmpinfo:Tool>
              </ipmpinfo:IPMPInfoDescriptor>
            </ipmpdidl:Info>
            <ipmpdidl:Contents
              ref="http://www.mmw.com/ShookUp/03_
Blue__shoes.mp3"/>
          </ipmpdidl:ProtectedAsset>
        </Resource>
      </Component>
    </Item>
  </Container>
</DIDL>
```

Figure 7. Digital Item example

The Digital Item also contains information about the tools used to protect the digital asset. Figure 8 presents

the license with the governance rules and the content key in a protected form.

```
<r:license>
  <r:grant>
    <r:keyHolder> ... </r:keyHolder>
    <mx:play/>
    <mlx:protectedResource>
      <r:digitalResource>
        <r:nonSecureIndirect URI="
http://www.mmw.com/ShookUp/03_ Blue_suede_shoes.mp3"/>
      </r:digitalResource>
      <xenc:EncryptedData>
        <xenc:EncryptionMethod
Algorithm="http://www.w3.org/2001/04/xmlenc#kw-aes128"/>
        <dsig:KeyInfo>
          <dsig:RetrievalMethod URI="#EK"
Type="http://www.w3.org/2001/04/xmlenc#EncryptedKey"/>
          <dsig:KeyName>Name for Key - Content
Encryption</dsig:KeyName>
        </dsig:KeyInfo>
      </xenc:EncryptedData>
      <xenc:EncryptedKey Id="EK">
        <xenc:EncryptionMethod
Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1_5"/>
          <dsig:KeyInfo>
            <dsig:KeyName>Name - User Key</dsig:KeyName>
          </dsig:KeyInfo>
          <xenc:CipherData>
            <xenc:CipherValue>AQABAA==</xenc:CipherValue>
          </xenc:CipherData>
          <xenc:ReferenceList>
            <xenc:DataReference URI="#ED"/>
          </xenc:ReferenceList>
          <xenc:CarriedKeyName>Content Encryption Key
Name</xenc:CarriedKeyName>
        </xenc:EncryptedKey>
      </mlx:protectedResource>
  </r:grant>
  <r:issuer> ... <r:issuer>
<r:license>
```

Figure 8. License example

5.3 Joint distribution of content and licenses

In this section we propose two different ways of managing licenses and keys, when content and licenses are jointly distributed to users.

The first mechanism proposed is based on the solution proposed in Section 5.2, for separate distribution of content and licenses. Nevertheless, in the case of joint distribution, the license will be associated to a Digital Item by means of the *RightsDescriptor* element of the IPMP Info schema [5]. In this way, licenses and keys are securely delivered to the user within a Digital Item. Figure 9 illustrates an example of a Digital Item with a protected license, that contains the usage rules and the content encryption key encrypted.

```
<DIDL>
 <Container>
  <Item>
   <Descriptor id="Track1">
    <Statement mimeType="text/plain">Blue suede shoes
    </Statement>
   </Descriptor>
   <Component>
    <Resource mimeType="application/ipmp">
     <ipmpdidl:ProtectedAsset mimeType="audio/mp3">
      <ipmpdidl:Info>
       <ipmpinfo:IPMPInfoDescriptor>
        <ipmpinfo:Tool>
         <ipmpinfo:ToolBaseDescription>
          <ipmpinfo:IPMPToolID>
            urn:mpegRA:mpeg21:IPMP:GFTR977
          </ipmpinfo:IPMPToolID>
          <ipmpinfo:Remote
ref="urn:IPMPToolsServer:DRMS06565_FGR"/>
          </ipmpinfo:ToolBaseDescription>
         </ipmpinfo:Tool>
        </ipmpinfo:IPMPInfoDescriptor>
       </ipmpdidl:Info>
       <ipmpinfo:RightsDescriptor>
        <ipmpinfo:License>
         <r:license>
          <r:encryptedLicense
Type="http://www.w3.org/2001/04/xmlenc#Content">
          <enc:EncryptionMethod
Algorithm="http://www.w3.org/2001/04/xmlenc#3des-cbc"/>
          <dsig:KeyInfo>
           <dsig:KeyName>SymmetricKey</dsig:KeyName>
          </dsig:KeyInfo>
          <enc:CipherData>
           <enc:CipherValue>
             Ktd63SDfkDWEjeSdkj39872A5ToQ...
           </enc:CipherValue>
          </enc:CipherData>
         </r:encryptedLicense>
        </r:license>
       </ipmpinfo:License>
      </ipmpinfo:RightsDescriptor>
     </ipmpinfo:IPMPInfoDescriptor>
    </ipmpdidl:Info>
    <ipmpdidl:Contents
                ref="http://www.mmw.com/ShookUp/03_
Blue_suede_shoes.mp3"/>
   </ipmpdidl:ProtectedAsset>
  </Resource>
</Component>
</Item>
  </Container>
</DIDL>
```

Figure 9. Digital Item example – Protected License

The second solution that we propose for joint distribution of content, licenses and keys, make use of the *RightsDescriptor* element for managing protected licenses and of the *InitializationSettings* for handling keys. Figure 10 shows an example of a Digital Item that carries a protected digital asset, the associated license with the usage rules and the content encryption key both in a protected form.

```
<DIDL>
 <Container>
  <Item>
   <Descriptor id="Track1">
    <Statement mimeType="text/plain">Blue suede shoes
    </Statement>
   </Descriptor>
   <Component>
    <Resource mimeType="application/ipmp">
     <ipmpdidl:ProtectedAsset mimeType="audio/mp3">
      <ipmpdidl:Info>
       <ipmpinfo:IPMPInfoDescriptor>
        <ipmpinfo:Tool>
         <ipmpinfo:ToolBaseDescription>
          <ipmpinfo:IPMPToolID>
            urn:mpegRA:mpeg21:IPMP:GFTR977
          </ipmpinfo:IPMPToolID>
          <ipmpinfo:Remote
ref="urn:IPMPToolsServer:DRMS06565_FGR"/>
          </ipmpinfo:ToolBaseDescription>
          <ipmpinfo:InizializationSettings>
           <xenc:EncryptedKey Id="EK">
            <xenc:EncryptionMethod
Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1_5"/>
             <dsig:KeyInfo>
              <dsig:KeyName>Name - User Key</dsig:KeyName>
             </dsig:KeyInfo>
             <xenc:CipherData>
              <xenc:CipherValue>AQABAA==</xenc:CipherValue>
             </xenc:CipherData>
             <xenc:ReferenceList>
              <xenc:DataReference URI="#ED"/>
             </xenc:ReferenceList>
             <xenc:CarriedKeyName>Content Encryption Key
Name</xenc:CarriedKeyName>
           </xenc:EncryptedKey>
```

```
          </ipmpinfo:InizializationSettings>
         </ipmpinfo:Tool>
        </ipmpinfo:IPMPInfoDescriptor>
       </ipmpdidl:Info>
       <ipmpinfo:RightsDescriptor>
        <ipmpinfo:License>
         <r:license>
          <r:encryptedLicense
Type="http://www.w3.org/2001/04/xmlenc#Content">
           <enc:EncryptionMethod
Algorithm="http://www.w3.org/2001/04/xmlenc#3des-cbc"/>
          <dsig:KeyInfo>
           <dsig:KeyName>SymmetricKey</dsig:KeyName>
          </dsig:KeyInfo>
          <enc:CipherData>
           <enc:CipherValue>
             Ktd63SDfkDWEjeSdkj39872A5ToQ...
           </enc:CipherValue>
          </enc:CipherData>
         </r:encryptedLicense>
        </r:license>
       </ipmpinfo:License>
      </ipmpinfo:RightsDescriptor>
     </ipmpinfo:IPMPInfoDescriptor>
    </ipmpdidl:Info>
    <ipmpdidl:Contents
                ref="http://www.mmw.com/ShookUp/03_
Blue_suede_shoes.mp3"/>
   </ipmpdidl:ProtectedAsset>
  </Resource>
</Component>
</Item>
```

Figure 10. Digital Item example – Protected Licenses and Keys

6. Conclusions

In this paper we have proposed different alternatives for the secure management of licenses and keys associated to protected multimedia content in DRM systems. The solution is based on the MPEG-21 standard, since it is the most general initiative that defines the components for a complete DRM system.

First, we have selected a set of representative use cases that cover the most common ways of distribution and consumption of multimedia content including groups of the users and/or devices (Superdistribution or Domains) and multimedia streaming.

Finally, we proposed the solution for managing licenses and keys in a secure way taking into account separate and joint distribution of the protected content, licenses and keys. All the mechanisms proposed make are based on the MPEG-21 standard specifications.

Future work should focus in the development of tools that can be used in DRM applications according the different use cases identified.

Acknowledgements

This work has been partly supported by the Spanish Administration (DRM-MM project, TSI2005-05277) and VISNET-II, a European Network of Excellence, co-funded under the European Commission IST FP6 program (IST-1-038398).

References

[1] OMA, http://www.openmobilealliance.org/

[2] DMP, http://www.dmpf.org/

[3] TV-Anytime, http://www.tv-anytime.org/

[4] MPEG-21 standard, http://www.chiariglione.org/mpeg/standards/mpeg-21/mpeg-21.htm

[5] ISO/IEC, ISO/IEC IS 21000-4 Intellectual Property Management and Protection Components

[6] ISO/IEC, ISO/IEC IS 21000-5 – Rights Expression Language

[7] XML Encryption, http://www.w3.org/TR/2002/REC-xmlenc-core-20021210/

[8] Delgado. J., Prados, J, Rodríguez, E. "An MPEG-21 REL mobile profile". ISO/IEC JTC 1/SC 29/WG 11/M12229. July 2005, Poznan (Poland).

[9] Wang, X., Delgado, J., Barlas C. "ISO/IEC 21000-5/FDAM 1 Rights Expression Language: the MAM profile". ISO/IEC JTC 1/SC 29/WG 11/N8342 Klagenfurt, Austria, July 2006

[10] OMA DRM Rights Expression Language, OMA-Download-DRMREL-V2_0-20050825-C. August 2005

[11] Kim, T., Chiariglione, F., Wang, X. "ISO/IEC 21000-5/FPDAM 2 Rights Expression Language: the DAC profile". ISO/IEC JTC 1/SC 29/WG 11/N8812 Marrakech, January 2007

[12] OMA DRM Architecture, http://www.openmobilealliance.org

[13] Kim, T., Delgado, J., Schreiner, F., Barlas, C., Wang, X. "ISO/IEC 21000-5 FPDAM/3 ORC (Open Release Content). ISO/IEC JTC 1/SC 29/WG 11/N9108. San Jose, USA, April 2007

[14] Creative Commons, http://www.creativecommons.org/

[15] Interoperable DRM Platform specification (IDP), phase II, http://www.dmpf.org/open/dmp0765.zip

[16] Chillout, the Interoperable DRM Platform Reference Software, http://chillout.dmpf.org/

[17] ISO/IEC, ISO/IEC 2nd Edition IS 21000-2 – Digital Item Declaration

[18] Torres, V., Delgado, J., et al. An implementation of a trusted and secure DRM architecture. *In On the Move to Meaningful Internet Systems 2006: OTM 2006 Workshops (IS'06)*. Lecture Notes in Computer Science, vol. 4277. Springer-Verlag, 2006, 312-321.

[19] OMA DRM Specification, OMA-TS-DRM-DRM-V2_0-20050901-C. September 2005.

[20] Rodríguez, E.; Llorente, S.; Delgado,J. "DMAG answer to MPEG-21 Intellectual Property Management and Protection Call for Proposals". ISO/IEC JTC 1/SC 29/WG 11 MPEG2003/M10832. July 2004.

[21]Lauf, S., Rodriguez, E . "The MPEG-21 Book. Chapter 4 – IPMP Components". John Wiley & Sons, Ltd, pp. 117-138. ISBN: 0-470-01011-8.