Enabling Content and rights transmission in the Educational field with ARMS

ABSTRACT

Authorship and content integrity are the most basic rights that academic authors want to preserve in the educational field. In order to preserve these author rights a special adapted DRM platform, ARMS, was developed. This platform is oriented to the educational domain and we must to highlight the web services interface with a generic educational Academic Management System platform of the educational institution, established in order to verify the user eligibility in this domain before issuance of the license. To guarantee content and rights protection, cryptographic techniques and mechanisms are applied in a fashion where content, rights, protection keys and related metadata are packaged in special containers obeying the MPEG-21 standard. The resulting objects describe here, obeys a special structure where protected objects may only be used by the user of the educational domain to whom the respective license was issued embedded in one of these objects. These neutral resulting objects can then be easily transmissible in open communications channels in a way that enable their management in order to achieve a controlled access and usage. They are the main data transport bodies that enable content protection and rights transmission among participants in content protection lifecycle.

KEYWORDS

DRM, MPEG-21, OpenSDRM, content sharing, rights transmission.

1. INTRODUCTION

Many authors of scholarly content have a fear that their original published digital material is used by others as their own or use it without author consent for many other purposes. Those materials can be easily copied and/or plagiarized and redistributed without any control and with no means to prove authorship. In the educational sector right owners wants essentially to preserve authorship and content integrity (Bates, 2007). The increasing demand of learning resources and the need to protect them, originates different strategies of integrating Digital Rights Management (DRM) and flexible commercial model into applications, management, exchange and trade of web-based learning content by describing rights in license services. Content format compatibility, license compatibility, and other such system properties (Heileman, 2005; Schmidt, 2004) are main issues in current DRM systems. (DRM) is a system, which tries to restrict the illegal content consumption and facilitates the scalable content distribution (Mishra, 2012) applying different techniques to protect digital content. However, the different technologies used by DRM needs to be under the umbrella of a standard (or standards) in order to provide the correct rights interpretation and enforcement when content is shared.

The need to secure the content value chain is emphasized by the Iannela (2006) as also the need to protect the rights of all the entities in new-generation DRM systems evolving for new applications. Despite many existing industrial DRM systems and projects/initiatives such as Marlin DRM, OMA DRM , DMP, …etc, they are oriented to the content industry. The educational sector is left behind. In (Torres, 2010) is proposed an online framework for the registration, search and trade of scholarly objects. Based on MIPAMS the proposed framework (IPOS_DS) is a service oriented architecture that consists in a main web application accessible through a web browser which interacts with different web services enabling features like content registration and certification, content licensing, content accessing and monitoring and search interfaces (Torres, 2009a; 2009b). The license control is very wide in the sense the license can be granted to anyone and it is not specific to the educational domain of an institution. Despite the valuable features it provides it is oriented essentially to the educational commercial sector, like private companies or collecting societies (Torres, 2010). The emphasis of this paper is on the issues related to an object structure based on

MPEG-21 standard that enables the transmission of resources (content and keys) and related data across main players in DRM systems specifically in the educational context. In this paper we propose a standard based object structure for content and license management implementation in order to control the content sharing and associated rights inside the educational domain through the MPEG-21 standard. For the sake of space our focus will be on object structures that enables the transport of the main resources and related data in the information DRM flow. Next section describes DRM and the related information data flow. Section 3 describes ARMS architecture and related DRM operations. Section 4 presents the proposed MPEG-21 objects structure and finally in section 5 is described how a license object is retrieved.

2. DRM AND DATA FLOW

Current DRM systems provides protected content to consumers adopting a license-based schema which separates the protection keys from encrypted content (Hwang, 2009). The encrypted content is delivered to a DRM client from a Content Server (CS) that distributes it while the license including the key (C_{EK}) used to protect content is transported to the DRM client from a license server (LS). After the content is downloaded, users can use it if they have a license (Hanaoka G., 2004). When content flows from content owner to consumer it passes through the distributor that delivers it to the final user. The content flow from the author to the final user in a DRM system drag with it specific data types. Associated with content flow usually there are four kinds of DRM data: the resource, the resource protection key C_{EK}, content metadata and rights expression data. These are packaged into a specific DRM content format by the content owner. DRM content packaging means that a specific DRM content and associated information is embedded into neutral XML file (content object). Also content protection key(s) and usage conditions are packaged in another XML file (rights object). The correct combination of these four kinds of data originates two different objects with different structures: the rights object and the content object (Figure 1). Normally these data types are adapted to be inserted in these structures: content and C_{EK} are adapted to a neutral format like the Base64 encode before being protected through encryption. Metadata are essentially expressed in the Dublin Core format and MPEG-21 REL is used as the neutral language for rights expression.

MPEG-21 is a set of specification standard (ISO/IEC:2100) that defines a neutral format based in digital items (Dis) that enables data transmission by a standard channel of communication like Internet. Of particular importance towards the fulfillment of universal media access is the availability of an open object data model. MPEG-21 has delivered some specifications addressing precisely this aspect: the Digital Item Declaration (MPEG-21:DID, 2005) and the Intellectual Property Management Protection (MPEG-21:IPMP, 2006).With a standard structure widely accepted is possible to the final user acting on the client DRM side gets the content object and get a clear resource, content metadata and associated rights. This way is possible to establish a common structure of these objects that foster content sharing in the educational field.

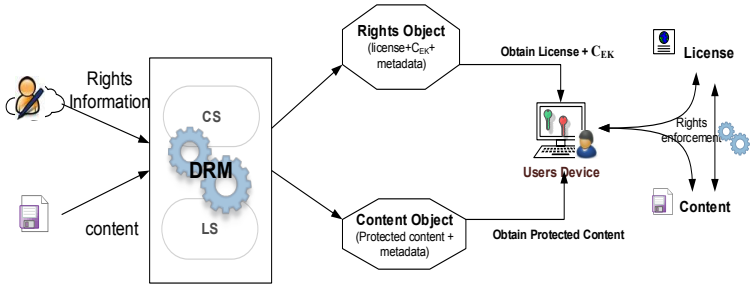

Figure 1: DRM information flow.

Despite some initiatives like SCORM or IMS that defines a structure for learning objects they don´t explain how they do the rights enforcement. Other initiatives like Creative Commons also permits to attach copyright information but don't permit the enforcement of rights through technological means. Our proposed system is based on standards and is oriented to content and rights protection in the educational field .The content is protected using two methods involving the DI concept from MPEG-21 specification (MPEG21:DID). One is related with the content in the raw form using symmetric cryptography and the other

is related with the encryption of the key used to protect the content. In each method the result is embedded in a special package obeying MPEG21 Digital Item specification. These special packages (content and rights objects) can them be downloaded by the user through a DRM enabled device.

Our proposal is oriented to define content and rights objects structures based on MPEG21 targeted to control the license issuance in the educational domain. To control if users are eligible inside a specific domain the license distributor (LS) checks its profile before issuing the usage license. To do so, the LS on the DRM system validates the requesting user getting data from the institutions Academic Management System (AMS), where all scholar activities are registered (Figure 2) and then delivers the rights object.

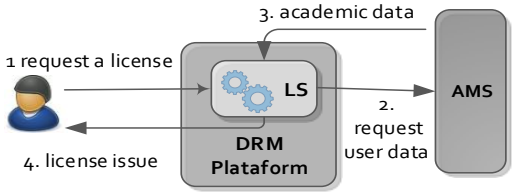

Figure 2: DRM interactions with AMS.

3. ARMS ARCHITECTURE

ARMS is based on OpenSDRM platform (OpenSDoRM, 2005) that is has been developed in the MOSES (MPEG Open Security for Embedded Systems) project. It is web services oriented and consists of actors and components that interact with each other (Serrão, 2005). ARMS is based on the flexible web services approach consisting of several components and services, which provide the functionality needed for governing and protecting content.The main evolution of ARMS architecture is related with the insertion of a new web service interface with the Academic Rights Management (AMS) system of the educational institution through the License Server. One of the advantages of having service-oriented content management functionality relies on the possibility of decoupling it into different subsystems depending on the needs of the application area intended to be used, while being able to share the same common services between different applications with different requirements. Content management service functionality (register and search content), security (licensing, protection, tracking,…) and distribution (content transfer) related services are some of service functionalities provided by web services in DRM systems. ARMS,

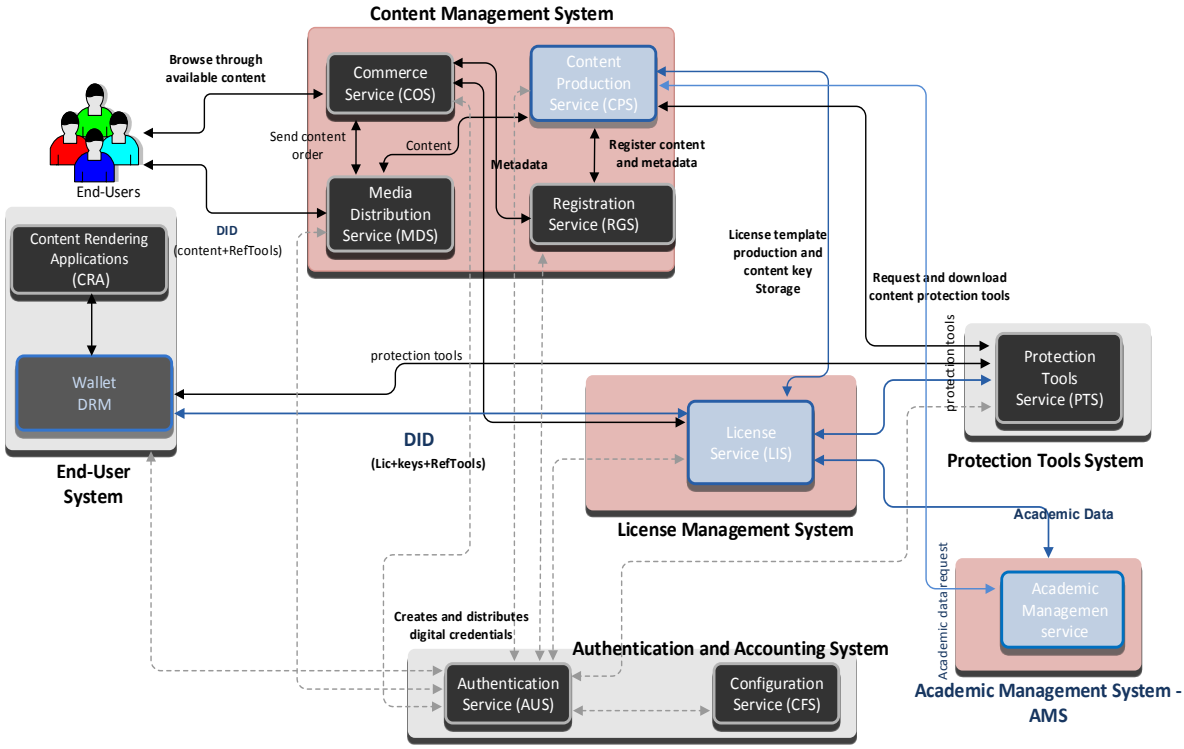

Figure 3 : ARMS main components interactions

allows access to content to be shared amongst a pool of users belonging to academia, within limits defined by the content provider.

The data flow is described next. First, the user downloads protected content, for example a protected PDF lesson, with some content related metadata embedded in a content object obeying a specific MPEG21 DID structure (MPEG-21: DID). Then, the LS generates a license granting to that user the right to view the lesson according to the conditions selected. Finally, when the user wants to view the PDF lesson, a connection between the player and the License Server (LS) is established, and the license is embedded in a rights object containing the encrypted content protection key that can be downloaded by the user that request it. Then, the protected PDF is decrypted using the key extracted from the license and can be finally used. However, to verify if the license requester belongs to the Institution educational domain the LS contacts the AMS (Figure 3). Using web services the LS get data from AMS and then verify if the requester belongs to educational institution, and then proceed to license generation to be embedded in the rights object.

DRM operations can be systematized in several phases:

- Certificate Requesting and Registration: this phase is the initial and mandatory; all participants having main roles on content preparation and distribution must register to AUS and request certificates. After registration and a successful login on the DRM system the content owner can upload content.
- Content preparation, content rights and metadata: content owners after successful authentication are considered trusted users entities in DRM system, and can prepare content to be protected. To do this, they use authoring applications and tools that incorporates DRM protection technology. Content protection is achieved using some specific tools like the ones that enable watermarking and symmetric cryptography. At this phase content provider usually generates content identifier (ID_C), content metadata (C_M) and content encryption secret key (C_{EK}) needed to protect content.
- Content packaging and containers: the CPS generates a specific C_{EK} for a specific content IDc and with that key encrypts the content. The obtained encrypted content is packaged with some content related metadata and I_{DC} in a XML MPEG-21 specific format. To provide integrity and non-repudiation the content package will be digitally signed by the content provider.
- Keys, metadata and licensing rights: keys used for content encryption and other content related metadata (specific delivery information, content description, etc) are made available to the content preparation service (CPS). Also, after finish content preparation and packaging, some necessary information will be sent to LS (C_M, licensing details, etc). Rights definition is done by the content owner through specific content provider tools that assigns the basic grants for distribution and assigns metadata in a specific format. This data is transmitted to the rights distributor (LS) that will issue it to the final user.
- License storage: the rights definition and some other related metadata applied over content with a specific IDc are stored at the LS. The content distribution process can be split into two parts: first a provider distributes the content and the associated license to a consumer C_1 and the second where a consumer C_1 redistributes the content to another consumer C_N. The customer C_N using a client device could also receive a protected content shared by original customer using client device through email, instant message, or P2P. C_N can use the content with basic grants. If C_N have interests in it, he could acquire the corresponding license from the DRM provider using the client device. After selecting the desired content, client C sends a request for issuing a usage license referring to this content IDc to the License issuer service (LS). LS checks the client request obtaining user academic data from the AMS. If the user request is valid LS issues a specific license for that content and that user.
- Licensing distribution and acquisition: at this phase, LS verifies the identity of client C and request license for the content identified with IDc. Then LS contacts the AMS inquiring it if the user license issuing request is eligible. If the user request is eligible, then a license is generated for that content with IDc. Using the MPEG-21 rights expression language and the necessary cryptographic information for content protection and consumption and sent it to the client DRM agent. To do this, LS contact CPS to get specific C_{EK} to this specific content with IDc. Than C_{EK} is encrypted with the client C public key $K_{pub}C$. This license is embedded in a compliant MPEG-21 rights object containing the encrypted C_{EK}, content related rights and metadata. To provide integrity and non-repudiation, the rights object is digitally signed by the issuer.
- License interpretation and license utilization: content consumption is possible only after the DRM client authenticate the license and decrypt content encryption key and usage policies from the license object.

- Content consumption: to content be usable the user needs to obtain the rights object. After getting this object are obtained important security measures are implemented inside client subsystem while content is being decrypted and rendered. To an attacker these security measures circumvention must turn infeasible:
  1 - The extraction of unprotected content. This allows an unlimited distribution of content and unrestricted rendering of content without the associated license.
  2 – The extraction of cryptographic keys. This allows the unauthorized access to digital content and the distribution services.

In the next section the implementation of the designed MPEG-21 IPMP and REL objects structures are described in order to enable content protection and governance through the MPEG-21 Digital Item (DI) concept. An effective way to protect content is to encrypt it, so we will focus on cryptographic tools for providing the MPEG-21 protection functionality. IPMP expressions containing protection information, such as the IPMP tools enabling content protection, initialization settings, keys and governance information (such as licenses that govern the content or references to these licenses or license services) are used herein.

4. CONTENT AND RIGHTS OBJECTS

To be easily transmissible both generated objects (content and rights) are designed in a flexible structure using MPEG-21 standard specifications (MPEG-21:REL, 2004; MPEG-21:IPMP, 2006; MPEG-21:RDD, 2003; MPEG-21: DID, 2005) in order to guarantee resource protection while enabling its transmission through open communication channels like he Internet. The concept of DIs is widely applied and MPEG-21 REL will be provided for the creation of rights expressions enabling usage actions over content. Content and protection keys are delivered to the end user in an encrypted form embedded in a DID content object.
For the sake of simplicity we must distinguish two types of MPEG-21 DID documents representing digital objects related with DIs: the DID document representing the Content object (DID_C) and the DID document representing the Rights Object (DID_L). To generate the DID_C a special module or *script* is implemented in the CPS. This module works as a bridge between the source and the final DID object. The symmetric key algorithms such as, AES or 3DES used to encrypt the content may be same or different in the source. The PTS connection gives the content provider the tool that he needs to select and encrypt the content. With the protection key(s) and related metadata the module creates the DI_C object. When the DI_C arrives to the final user the user device obtain the information related with which tool was used and where is located the corresponding license. Than the device can make a connection to PTS ARMS component to get the rights protection tool and to LS to obtain the corresponding license.

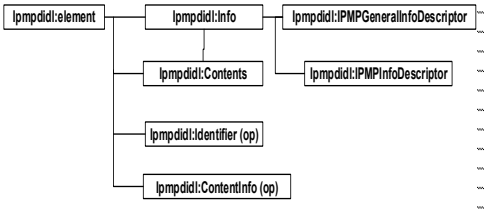

Figure 4: IPMP basic elements

```
...
<Declarations>
  <Descriptor>
    <Statement mimeType="text/xml; charset=UTF-8">
      <ipmpinfo:IPMPGeneralInfoDescriptor>
        <ipmpinfo:ToolList>
          <ipmpinfo:ToolDescription localID="AESEncrypt">
<ipmpinfo:IPMPToolID>urn:mpegRA:mpeg21:IPMP:tool:id:0001</ipmpinfo:IPMPToolID>
            <ipmpinfo:Remote ref="urn:IPMPToolsServer:ToolEnc005-3485"/>
          </ipmpinfo:ToolDescription>
        </ipmpinfo:ToolList>
        <ipmpinfo:LicenseCollection>
          <ipmpinfo:RightsDescriptor>
            <ipmpinfo:LicenseService>
                <r:serviceReference>
                  <sx:uddi>
                    <sx:serviceKey>
                      <sx:uuid>aa1198c0-8abe-11d7-a7b8a03c50a334</sx:uuid>
                    </sx:serviceKey>
                  </sx:uddi>
                  <r:serviceParameters>
                    <r:datum> ... </r:datum>
                  </r:serviceParameters>
                </r:serviceReference>
            </ipmpinfo:LicenseService>
          </ipmpinfo:RightsDescriptor>
        </ipmpinfo:LicenseCollection>
      </ipmpinfo:IPMPGeneralInfoDescriptor>
    </Statement>
  </Descriptor>
</Declarations>
...
```

Figure 5 –part of DID_C content object

In order to enable content protection implementation MPEG-21 IPMP provides tools. Using the top elements from IPMP *schema* relatively to the sub-elements "*info*:" "*IPMPGeneralInfoDescriptor"* and "*IPMPInfoDescriptor"* (figure 4), is possible to assign the protection and governance of a DI (overall or in some parts). These sub-elements allows the creation of a DID content object where is defined the localization to obtain the content related licenses and also the tools needed to encrypt/decrypt content (Figure 5). An example of a content digital item structure (DID_C) with these elements can be show bellow (Figure 6). Some Content metadata (Dublin Core – DC and Digital Item identification - DII) are there introduced.

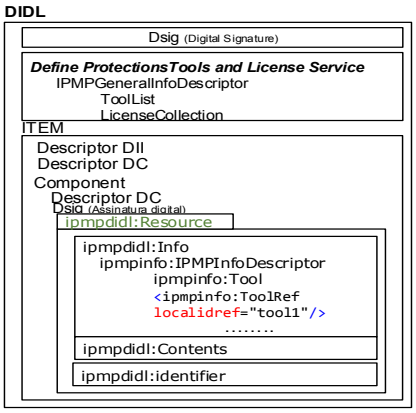

Figure 6 : DIDc object structure

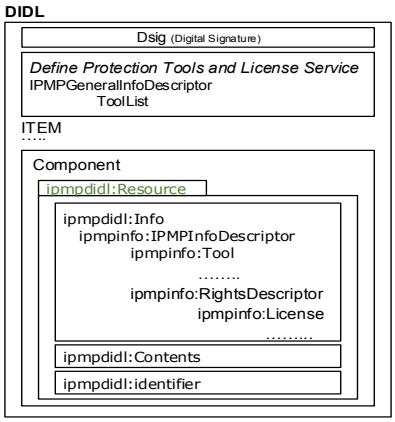

Figure 7: DID_L object structure

The original resource is base64 encoded and embedded in "<ipmpdidl:Contents>". The reference to resource protection method is provided by the element "ipmpdidl: resource" that incorporates the three basic elements "IPMP: Info", "IPMP: Identifier" and "IPMP: Contents" and respective sub-elements. The protection tool used and how to obtain the license are indicated as sub-elements of the DIDL element, at the top of the DID document. The element "<ipmpinfo: ToolRef>" contains the identifier of the corresponding protection tool related with the encryption algorithm used. This way the user can be informed about the encryption method used to protect content. Through the inclusion of the top elements "<IPMPGeneralInfoDescriptor>" and "<IPMPInfo Descriptor>", representing the governance and MPEG-21 IPMP protection, we are able to not only protect the content, but also indicate how governance can be done and indicate(s) the necessary protection (s) tool(s). To express content associated rights can be through element "IPMPGeneralInfoDescriptor". The sub-element "LicenseCollection" lets you specify, through the element "RightsDescriptor", how we can obtain rights associated with the resource by reference to a license server. The digital signature allows to check the integrity of the object. To identify unambiguously the resource is possible to insert attributes in the element "item" from other XML namespaces (e.g., Dublin Core) capable of providing descriptive information about that DI, as registration information (such as DOI).

The symmetric content encryption key (C_{EK}) can be automatically generated from a specific key generation module installed on the CPS. The management of these keys can be done dynamically through a cryptographic hash calculation algorithm $Hash_{SHA1}$ based on content and user identification, in order to generate a strong key (for example, $C_{EK} = Hash_{SHA1}$ ($Hash_{SHA1}$ (Content) + $Hash_{SHA1}$ (AuthorID)). When the user makes a request for a license for a particular content this key is encrypted with the user public key $K_{pub}U$ and then incorporated in the license. This license is them embedded in a DID object. In the same way as when the content protection was done this key in protected using the same technique using the IPMP element to protect it with RSA asymmetric algorithm and inserting it into the element "resource" of DIDL object, together with the respective usage license (Figure 7). The outcome results is a rights object with an identical structure to the content object.

5. OBJECTS USAGE

The structure of digital objects defined herein involve the encryption of content and embedding it in DID_C document. The key that protects content (C_{EK}) is encrypted and embedded it in the DID_L document. The metadata inserted in these objects remains inside them without any protection. This allows third parties

to access and identify the metadata and get content related information. The protection given by the IPMP tool refers only to the resource (content or protection key) in the DID document. Therefore is appropriate to insert your statement on the element "resource". This way the user can be presented with content rights information at the beginning content usage. When the user gets the content object the player on his device reads this information and is informed about content rights and where he can obtain the related license. The user is then redirected to the respective license server and then obtain (if is eligible) the usage license (Figure 8). The user can then unprotect the C_{EK} (defined in "ipmpdidl:Contents" DID_L object element) with his own private key $K_{priv}U$ stored on this device obtained during the registration procedure in the ARMS platform.

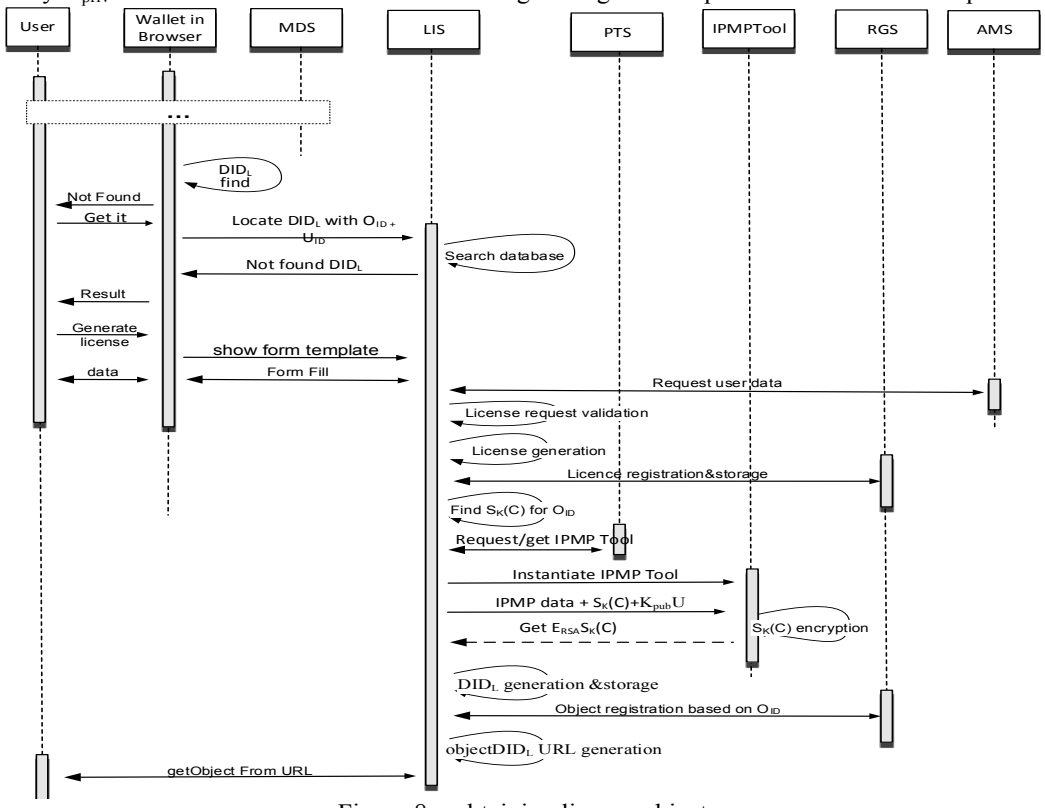

Figure 8 – obtaining license object

When a user gets both objects them he can use content in the conditions specified in the license. One of the main features not discussed in this paper is the role of the AMS. With the data it provides, the license server (LIS) on ARMS can verify not only if the license requester belongs to the educational domain but also, applying the correct validation mechanisms, verify if the requester obeys the conditions stated by the content owner in the distribution license. However for the sake of space is impossible to present these mechanisms here.

6. CONCLUSIONS

Resources and metadata can be embedded in a highly flexible structure supported by MPEG-21 standard. Providing an open multimedia framework MPEG-21 can contribute to a standard way of data transport and a high level of content rights protection. Using MPEG-21 is possible to establish a common base structure that enables not only content protection and the governance of rights but also a flexible format for content and rights transmission in an open environment like the Internet. ARMS provides the adequate infrastructure services enabling the integration and interaction of actors and components. The ARMS platform encompassing a set of web services and back office modules can ensure a high level of control over content protection. Being oriented to meet user needs in the educational context through the interaction with the academic management system verifying user's eligibility it can control the license issuance in the

educational domain. With these structures is possible to transport content and associated rights in a fashion where they can be very easy associated by the final user. Using these proposed content and rights objects structurally based on MPEG-21 standard with the correct protection tools is possible establishing a neutral transport format that enables the content governance when it is shared in the educational field. The MPEG-21 enabled object structure is very flexible and provides the vehicle where content, metadada, keys and related rights can be transported in open communication networks. This way is possible to enable a content rights control in the educational domain using open standards like MPEG-21 contributing to the establishment of a universal resource transport standard where rights can be governed.

7. REFERENCES

Bates, M., Loddington, S., Manuel, S., & Oppenheim, C. (2007). Attitudes to the rights and rewards for author contributions to repositories for teaching and learning. *Association for Learning Technology Journal*, *15*(1), 67-82.

DMP, Digital Media project, available at: http://www.dmpf.org/.

Erickson J. S., 2003. *Fair use, DRM, and trusted computing*. Communic of the ACM, Vol.46, Issue 4, p. 34-39, April 2003.

Hanaoka, et. al., 2004. *Managing Encryption and Key Publication Independently in Digital Rights Management Systems*. IEICE Transaction Fundamentals Electronics, Communications and Computer Sciences, Vol.E87-A, No.1,Jan. 2004.

Heileman, G., and Jamkhedkar P., 2005. *DRM interoperability analysis from the perspective of a layered framework.* In Proceedings of the Fifth ACM Workshop on Digital Rights Management, pages 17–26, Alexandria, VA, Nov. 2005.

Hwang, S. O. (2009). How Viable Is Digital Rights Management?.*Computer*,*42*(4), 28-34.

IANNELLA, R. 2006. Digital rights management. In *Handbook of Information Security*, H. Bidgoli, Ed, Vol. 3, Wiley.

IPOS-DS (Intellectual Property Operations System– Digital Shadow), www.digitalmediavalues.com

Jamkhedkar, P., and Heileman G., 2008. *A formal conceptual model for rights*". Proceedings of the 8th ACM workshop on Digital rights management. ACM, 2008.

Marlin, Marlin project, available at: http://www.marlin-community.com/.

Mishra, D., & Mukhopadhyay, S. (2012, October). Privacy preserving hierarchical content distribution in multiparty multilevel DRM. World Congress on *Information and Communication Technologies (WICT-2012*) (pp. 525-530).

MOSES - *MPEG Open Security for Embedded Systems project.* http://www.crl.co.uk/projects/moses/

MPEG-21: IPMP, 2006-ISO/IEC (2006). ISO/IEC IS 21000:4–Part 4: *Intellectual Property Management and Protection Components.*

MPEG-21: REL, 2004-ISO/IEC (2004). ISO/IEC IS 21000:5 – Part 5*: Rights Expression Language*

MPEG-21:DID, 2005- ISO/IEC (2005) Information Technology – Multimedia framework (MPEG-21) – part 2: *Digital Item Declaration*, ISO/IEC 21000-2:2005, July. 2005.

MPEG-21:RDD, 2003, ISO/IEC (2003). ISO/IEC IS 21000-6 – part 6: *Rights Data Dictionary*

MPEG-21:VTS, 2004, ISO/IEC, Information Technology – Multimedia framework (MPEG-21) – part 1: *Vision, Technologies and Strategy*, ISO/IEC TR 21000-1:2004, November 2004.

OMA, Open Mobile Alliance, available at: http://www.openmobilealliance.org/.

OpenSDRM – OpenSDRMSpecification, 2005, ADETTI, available at: http://www.opensdrm.org/files/ OpenSDoRM_ API_Specification.pdf

Schmidt A., Tafreschi O., and R., Wolf., 2004. *Interoperability challenges for DRM systems*. In IFIP/GI Workshop on Virtual Goods, Ilmenau, Germany.

Serrao, C. et al., 2003. *OpenSDRM – An open and secure digital rights management solution*. November 2003. http://www.crl.co.uk/projects/moses/Public/docs/IADIS03No74.pdf

Serrão, C., Dias, M., & Delgado, J., 2005. *Using Web-Services to Manage and Control Access to Multimedia Content*. In ISWS05-The 2005 International Symposium on Web Services and Applications, Las Vegas, USA.

Torres, V., Delgado, J., Maroñas, X., Llorente, S., & Gauvin, M. (2009a). A web-based rights management system for developing trusted value networks. In*Proc. of the 18th International WWW Conference Developer's Track* (pp. 57-59)

Torres, V., Delgado, J., Maroñas, X., Llorente, S., & Gauvin, M. (2009b). Enhancing Rights Management Systems through the Development of Trusted Value Networks. In *WOSIS* (pp. 26-35)

Torres, V., Tous, R.,Delgado, J. (2010). Reliable scholarly objects search and interchange framework. A: International Conference on Electronic Publishing. "14th International Conf. on Electronic Publishing". Helsinki: 2010, p.57-68.