ARMS – A NEW APPROACH TO CONTROL CONTENT SHARING AND RIGHTS DISTRIBUTION

J. Marques[1], C. Serrão[2]

[1] *IPCB/EST (PORTUGAL)*
[2] *ISCTE/IUL (PORTUGAL)*

Abstract

As in other areas, one of the main issues in the educational sector is related with content distribution and sharing. Ensuring that the terms and conditions stated by content owners on the license are respected by the other participants of the value chain, such as distributors (eg. teachers) or consumers (eg. students) is a concern. The assignment of licenses is a need in order to the distributor in the DRM system unambiguously communicate the licensing of the content giving an enhanced user experience. Not only is important to validate the issued license verifying if the terms and the conditions stated in the parental license are respected in the child license but also is important to verify if this license is generated to users that are in a controlled domain.

In this paper we will describe our rights-sharing control mechanism based in MPEG-21 standard that augments the control over a domain (the institution educational domain) through the validation of the license to be generated. Through a specific DRM system oriented to the educational context (ARMS - Academic Rights Management System) content owners are allowed to control which users can obtain a license within the constraints imposed by him, giving them the power to control the content usage in the educational domain. To enable this feature some special control mechanism, MPEG-21 based, were implemented in order to control the license issuance. With these verification mechanisms is possible to make the license distributor act like a domain controller regulating the issuance of licenses in the educational context. Our proposal, when applied in the educational domain, greatly increases the expressive power of digital rights management framework without requiring an upgrade to end-user devices.

Keywords: DRM, intellectual property, Mpeg-21, content and rights protection, content sharing.

1 INTRODUCTION

Sharing of content is a common practice that, combined with appropriate business models, need not be detrimental to the interests of content providers. Like other businesses areas the educational sector faces this challenge. Learning and education place some very specific demands on the rights management such as attribution/authorship and content integrity. Many of the main content owners and creators (teachers, researchers,…) in the educational field intents to preserve mainly two IP basic rights: the authorship and content integrity [1]. A content owner can grant permission to use it as long as he is properly acknowledged and with the assurances that the content is properly expressed and interpreted. Digital Rights Management (DRM) provides techniques and mechanisms, which congregates hardware and software to ensure the rights preservation of content providers against illegal usage [2]. Modern DRM provides protected content to consumers adopting a license-based schema which separates the protection keys from encrypted content [3]. From a content protection point of view integrity of the license and the content are necessary to resist any modification [4]. Also, content confidentiality must be assured in order to guarantee that only the legitimate user have access to the content. To provide the integrity functionality, the digital signature is in widespread use and is normally based in public key infrastructure where Certification Authorities (CA) are used to validate these signatures. Cryptography is a general measure to reach basic content protection providing content confidentiality. The encrypted content is delivered to a DRM client from a Content Distributor that distributes it while the key used to protect content is transported to the DRM client from a Content Rights distributor (the License Server). This key is normally inserted in a pre-prepared digital object that embeds also the usage terms and conditions in a license. After the content is downloaded, users can freely use the contents if they have this object. When a user wishes to perform some particular operation on the content, the DRM Client checks that the user possesses a license granting that permission, and that any constraints associated with the permission are satisfied. If the permission

does not exist, or the constraints are not satisfied, the DRM client will refuse to carry out the operation. Not only is necessary to ensure that rights are correctly assigned but also ensure that content usage is exercised by users in a specific domain respecting the conditions initially defined by the rights holder. Controlling the licensing and to whom is granted is a way to ensure that the license terms and conditions are respected in a specific domain.

In this paper we will describe a rights-sharing control mechanism based in MPEG-21 standard that permits to augment the content control distribution on a domain (the institution educational domain) through the validation of the license to be delivered in the ARMS system. This allows content owners to control which users enter their domains within the constraints imposed by the content provider. For example, if a teacher wants a content be distributed to students in a specific course the mechanism will verify if the students satisfies that condition before generate a usage license. We will describe how our mechanisms maps to a variety of sharing scenarios and derive the context information required to implement these scenarios. Also we demonstrate the practicality of our model by outlining how it could be implemented using ARMS. ARMS enabled with MPEG-21 mechanisms could apply cryptographic tools to preserve content integrity and also digital signatures to preserve rights authorship. Also with the verification mechanisms mentioned is possible to make the license distributor acts like a domain controller regulating the issuance of licenses in the educational context meanwhile ensuring the respect for the line of succession rights. Our proposal, when applied in the educational domain, greatly increases the expressive power of digital rights management framework without requiring an upgrade to end-user devices.

2 CONTENT FLOW AND PROTECTION IN DRM

A DRM system plays important roles in several processes that are involved in the flow of content, as shown in Figure 2. It enable the creator to protect and specify the desired ownership rights over content. It enables the provider to derive appropriate metadata from the content and specify the provider rights. It allows the consumer to specify the desired content and the various options in the use of content. It also enables the provider to monitor the content usage and track payment information. So we must consider three roles in this flow: content Creator, content Distributor and the Final user In content lifecycle we must consider these main high level functions related with content protection: the creation the distribution and the usage. Content creator creates content and uploads it to the Provider. This content is then encrypted, encoded, packaged and bounded to a license created by the License Creator. Finally, the user obtains the protected content from the provider and also obtain the encrypted content protection key C_{EK} and the respective license from the License creator/issuer. Then the content processor on the user device uses them to access the content, which is further rendered by the content renderer (Figure 2).

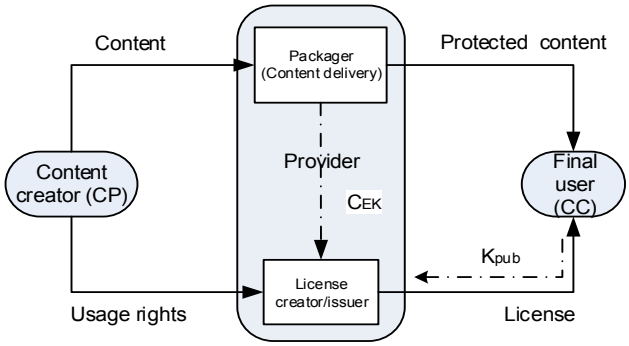

Figure 2: content flow in DRM

In a traditional DRM architecture, creation, distribution and consumption of digital content are carried out by Content Provider (CP), Content Distributor (CD) or Provider, and Content Consumer (CC), or Final User respectively. A DRM system manages the appropriate access and use of content. The major functionalities of this system are numerous. They include facilitating the packaging of raw content into an appropriate form for easy distribution and tracking, protecting the content for tamper-proof transmission, protecting content from unauthorized use, and enabling specifications of suitable rights, which define the modes of content consumption. One of major functions in any DRM solution is related with the management of interactions between users and content. For DRM systems to work effectively, it is necessary for content creators and distributors to be able to expresses the intended rights associated with digital content in a machine-readable form. Also, digital content rendering

environments must be able to interpret and enforce these rights. Enforcement of rights are one of the common functionalities to prevent unauthorized usage in DRM [12]. Rights are expressed in a special purpose language, XML based, designed Rights Expression Language (REL) that syntactically bound a digital object identifier, an actor identifier, a content encryption key and set of conditions. The license is the most important concept in REL and is considered a container of grants, each one of which conveys to a principal the privilege to exercise a right against a resource. Many rights expression languages license definitions [6][10][11] make use of eXtensible Markup Language (XML) due to its extensibility and flexibility. The online DRM system is basically a set of content and rights management related services offered by the CP to CC and CD. The DRM client is the entity at consumer side responsible for performing the DRM specific operations in a secure way over content while enforcing the right specifications expressed in the license.

To protect content the provider encrypt it with a secret key, C_{EK}, encode it in a universal format (e.g.: base encode 64) and then package it with related metadata. To access the protected content the user needs the secret key, C_{EK}. That key is delivered by the License Issuer to an authorized and authenticated DRM user that request a content specific related license. This key, to be only accessible to the specific user that requested it, is encrypted with his own public key (K_{pub}) and delivered to him packaged with metadata and related rights expressed in the license. The user can then access content decrypting it with his own private key (K_{priv}) stored in a device enabled with special DRM features (figure 3).

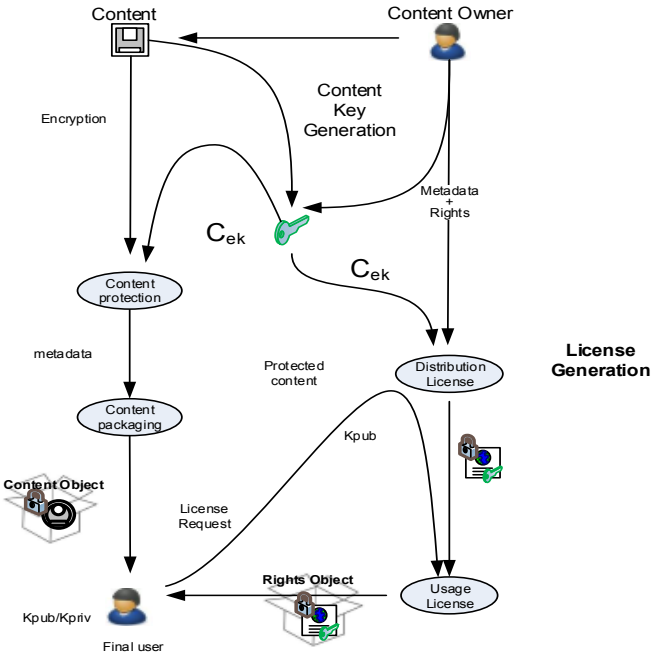

Figure 3 – content and keys flow in DRM System

Protecting content by modern cryptographic techniques is a current feature that most DRM systems does very well. The challenge is ensuring that the terms and conditions stated by content owners on the license are respected by the other participants of the value chain, such as distributors or consumers. Licensing is a key aspect in order to control content usage in a specific domain.

2.1 Licensing

A license is an aggregation of permissions awarded by some rights-holder to some beneficiary that can only be issued on the authority of the rights-holder [5]. Rights issuers only generate licenses according to some policy set by the relevant content holder that provides content. The assignment of licenses is a need in order to the distributor in the DRM system unambiguously communicate the licensing of the content giving an enhanced user experience. Not only is important to validate the issued license verifying if the terms and the conditions stated in the parental license are respected in the child license but also is important to verify if this license is generated to users that are in a controlled domain. This way is possible to establish a clean and valid line of succession rights that can contribute to a more effective trust among participants in the value chain. In the educational area this is a concern because many times the content owner not only wants to preserve their basic rights

(authorship, content integrity) but many times also maintain the content usage controlled in this domain.

The MPEG-21 standard specifies mechanisms to enable controlled distribution of multimedia content through the complete digital value chain MPEG-21 REL [6] and RDD [7], specify mechanisms to create rights expressions that govern the distribution and consumption of multimedia content. The "issue" and "delegation" control mechanism defined in MPEG-21 could be used to control the distribution. These mechanisms, when applied in a DRM system, can be used to determinate whether licenses that govern digital objects have been generated obeying the terms and conditions stated by content holders through a rights expression language (REL) when they are distributed. In [8] some verification algorithms are presented that can be used by DRM systems to enable the governed distribution of content and some different scenarios in which a DRM system can make use of the appropriate verification algorithms. However we go one step further applying some controls that verify it the requesting license user is eligible and if the generated license to be distributed obeys initial terms and conditions defined by the content owner.

This paper, presents a DRM system, intended for sharing access to content based on controlled domain concept. ARMS Academic Rights Management System) is a service-oriented content management system, based on OpenSDRM [9] platform, mainly intended to the management of rights on the educational field. OpenSDRM architecture was completely described almost in its current shape and has proved to be useful in various application scenarios. The main evolution of OpenSDRM targeting ARMS architecture is oriented with the insertion of a new web service interface with the Academic Rights Management (AMS) system of the Educational institution through the License Server. 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 operations provided by each service are based on SOAP web services Simple Object Access Protocol. 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, allows access to content to be shared amongst a pool of users belonging to academia, within limits defined by the content provider. Through the insertion of control modules in the License Server is possible to verify if the user is eligible when request a specific usage license. To do this a special interface is introduced in ARMS architecture enabling the exchanging of information with the License Server and the AMS that controls and regulates all academic activities in the educational institution (figure 1). ARMS followed an approach based on web services that turns possible the integration of this external component depending the integration level on the implemented interfaces. Using web services this component can deliver the information needed to verify the eligibility of the user and validate terms and conditions to generate licenses applying specific mechanisms based on MPEG-21. The central component of the License Server offers several services to the application layer regarding interpretation of licenses, as well as to provide the central key store for protected content. In order to enable the interpretation of the licenses some specific tools are enabled through the implementation of several modules: the transport tools, the protection tools and the governance tools. Inside the governance tools, the license validator is one of the most important modules because apply the mechanisms that verifies the legitimacy of the license requester inside the institution educational domain and verify if the original terms and conditions are in accordance with the line of succession rights expressed in progenitor license.

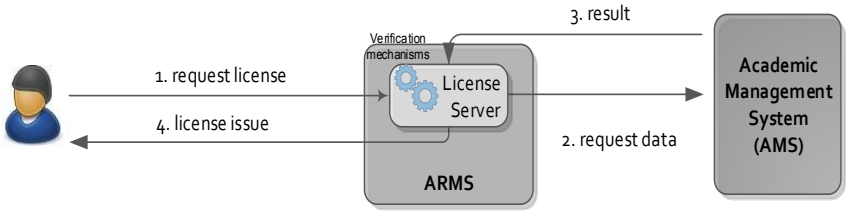

Figure 1 – License issue validation

MPEG-21 REL is used in the rights managing model of the ARMS system to establish the progenitor requirements through control set and verify users' qualification when they request a license. The License Server holds a database of registered users and verifies them on behalf of progenitors and

qualifies them (obtaining related information from the AMS) before license issuing. Distribution and usage licenses are key elements. The distribution license is used to express transmitted rights to next role on the value chain. The usage license focus on rights requested to the distributor generate and deliver a license to the final user. A parallel stream of rights produced between users could exists when rights are shared and transferred from one to another if the transmitted rights are enabled to do this.

The License Service (LS) deals with the rights definition and issuance of licenses. Rights definition are setup by content owners or rights holders after registering content. They include the rights being offered for acquisition by other users and the conditions being applicable to those rights. As a result of a rights purchase a license is generated and could be issued. Licenses are expressed using MPEG-21 REL. Through the interaction among LS and AMS the ARMS system can obtain remarkable user data (figure 5) in order to verify if a license requesting user belongs to a specific domain (in this case the institution educational domain.

Figure 5 - Data obtained from the web service interactions between LS and AMS

If this verification is valid then the user is considered legitimate in the educational institution domain and the LS can proceed to verify the user eligibility relatively to conditions stated by rights distributor and transmit these rights according the inheritance line.

2.2 Rights transmission

Digital content is highly vulnerable to unauthorized use and illegal redistribution. License is a key concept needed to implement rights managing policies useful for knowledge content based distribution. Our emphasis is the license structure itself in order to enable rights transmission. For the sake of convenience the encryption process of the license content is omitted. Our license management scheme considers integrating a rights management into the License Server of an existing DRM system adapted to support AMS interactions. Our approach consists in separating content from the rights and embed them in a digital object obeying MPEG-21 DID [13]. The result consists in two objects: the content object (containing metadata and protected content) and the rights object (containing metadata, license and content protection key). The generated digital objects have similar structures however we propose the rights object having the protection content key within the digital item but outside the license. Protected content and related protection key are embedded in different objects but to MPEG-21 IPMP) [14] they are considered in the same way: as resources. These resources are also encoded in base-64 format. All items are digitally signed as also the whole digital object that is signed by the issuer.

To protect the resource and preserve his confidentiality, the MPEG-21 IPMP standard defines the notion of tool, which represents an encryption algorithm providing security services. This IPMP tool contains all required information about the type of algorithm and its parameters. The tool can be integrated on the level in the DID hierarchy, which is required to ensure the security of the content.

The metadata can remain unencrypted and them any recipient can read this before take any action on content usage. In this case, the IPMP tool refers only to the resource in the DID.

In the educational field, a knowledge based content can be shared among teachers and students and reused. Sometimes, the rough material is used and revised along the downward chain through several creators to the end user. To enable rights distribution the license must include one special feature granting to the rights holder the privilege to issue a license. In MPEG-21 this can be done in several ways and one of that is related with the grant issue mechanisms ant the other is related with the delegation control mechanisms. One enables an authorized distributor with the privilege to issue usage licenses from a distribution license. The other enables users with the privilege to transmit rights to other users in controlled way. With these mechanisms is possible to control the issued license within the boundaries of the rights defined by the primary license which are inherited from the progenitor.

To enable this MPEG-21 introduces two special elements in his REL specification: the <issue> and the <*delegation control*>. With these elements MPEG-21 gives support to two types of granted controlled rights. The issue right may be used to specify that a given principal has the right to issue a given right, but the former principal does not necessary hold that right (e.g. the principal have the right to issue *right x* but can't use that *right x*). A license with an *issue* right, is a distribution license where the issuer authorizes the granted principal to issue another license with the right enclosed in the issue right. In this type of license the resource element is a grant issued by the principal (Figure 6).

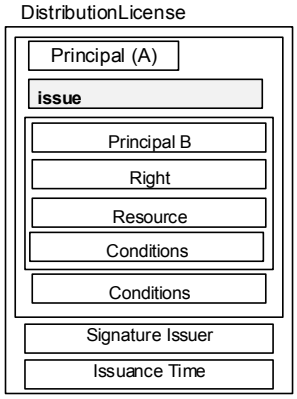

Figure 6 - MPEG-21 distribution license basic structure

3 DISTRIBUTION USAGE SCENARIOS IN THE EDUCATIONAL FIELD

In educational field the content lifecycle is not much different from other areas. The roles played by participants are more complex because sometimes they acts like distributors but sometimes acts like consumers. To grant rights to other participants the distributor must have the privilege to issue rights and these rights must consider the usage the consumer must have. Next we describe some simple scenarios white these privileges.

3.1 Issue rights control

Consider the following use case. Imagine that Teacher A issues a license to University ABC Publishing department with the right to issue a grant so users can read content PDFxyz file. As show in Figure 7 the license is issued by Teacher A with the issue right. Then, University ABC Publishing department can issue another license, which grants Student A the right to read *PDFxyz*.

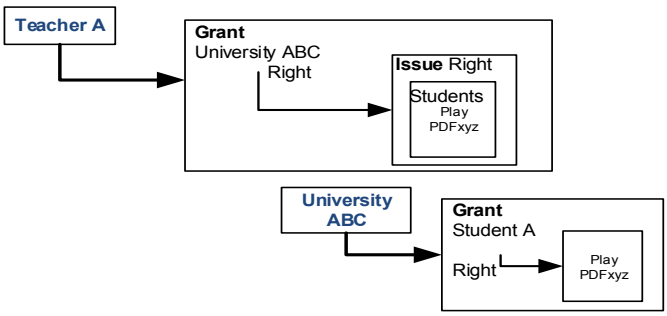

Figure 7 - PDF distribution scenario

In this case, University ABC Publishing department is authorized to issue the right to read *PDFxyz*, but it is important to note that Publishing Department is not authorized to read the PDF. In other words, Teacher A delegates to University ABC Publishing department the authority to issue the right to *read the PDFxyz*, and the University delegates to Student A (on behalf Teacher A) the permission to read *PDFxyz*. If Teacher A wants to restrict the usage of the content only for students in University ABC that are registered in current year he must apply additional conditions (Figure 8).

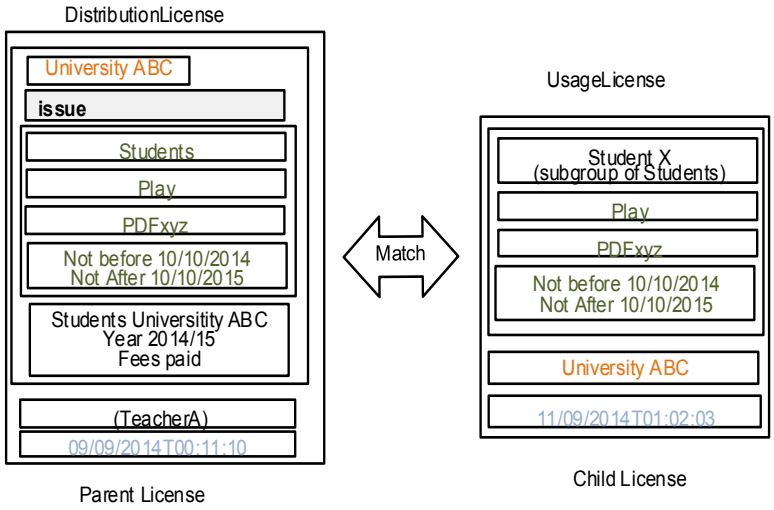

Figure 8 – Distribution issue control - licenses structure

A possible scenario can be devised in a situation where Teacher A grants to University ABC the right to issue licenses to students that attend a specific course at the University in the current year.

```
…
<r:license licenseID=”001”>
   <r:Grant licPartId=”issueGrant”>
       <r:forAll varName="studentX"/>
       <r:forAll varName=”cursoX”>
              <r:anXmlExpression>curso123<r:anXmlExpression>
       </r:forAll>
       <r:forAll varName="anoX">
              <r:anXmlExpression>2013<r:anXmlExpression>
       </r:forAll>
       <r:keyHolder>...University ABC...</r:keyHolder>
       <r:issue/>
              <r:grant licPartId=”UsageGrant”>
                     <r:keyHolder varRef="studentX"/>
                     <mx:play/>
                     <mx:diReference>urn:example:PDFxyz</mx:diReference>
                     <r:validityInterval varRef="anoX"/>
              </r:grant>
    </r:grant>
    <r:issuer>
       <dsig:Signature>
              <dsig:SignedInfo>...</dsig:SignedInfo>
              <dsig:SignatureValue> … </dsig:SignatureValue>
              <dsig:KeyInfo>...Teacher A...</dsig:KeyInfo>
       </dsig:Signature>
    </r:issuer>
</r:license>
….
```

Solving studentX to variable keyholder that identifies the student x and solving the yearX to variable valityInterval that identifies the year and doing the internal verification to confirm the student is enrolled in the current year, it is possible to issue a valid license for the student_111:

```
…
<r:license licenseID=”0001_1”>
   <r:Grant LicPartId=”usageGrant”>
       <r:keyHolder licPartId=”student_111”>
              <r:info>
```

```
                    <dsig:KeyValue>
                        <dsig:RSAKeyValue>
                            <dsig:Modulus>…</dsig:Modulus>
                            <dsig:Exponent>…</dsig:Exponent>
                        </dsig:RSAKeyValue>
                    </dsig:KeyValue>
                </r:info>
            </r:keyHolder>
            <mx:play/>
            <mx:diReference>
                <mx:identifier>urn:example:PDFxyz</mx:identifier>
            </mx:diReference>
            <r:validityInterval>
                <r:notBefore>2013-09-01T00:00:00</r:notBefore>
                <r:notAfter>2014-09-01T00:00:00</r:notAfter>
            </r:validityInterval>
        </r:grant>
        <r:issuer>
            <dsig:Signature>
                <dsig:SignedInfo>...</dsig:SignedInfo>
                <dsig:SignatureValue> … </dsig:SignatureValue>
                <dsig:KeyInfo>...University ABC...</dsig:KeyInfo>
            </dsig:Signature>
    </r:issuer>
    </r:license>
    …
```

When the student request a usage license a specific module in LS executes the verification mechanism in order to validate the compliance of the child license. Before this mechanism is applied the validation module in the license server verifies if this user belongs to the educational domain of the institution and if obeys the conditions defined by the teacher. The AMS is of primordial importance giving the information required by the LS validation module confirming the requester eligibility (figure 9). This validation module applies the rules adapted from [8] verifying this way two conditions: the eligibility of the license requester in the institution educational domain and the eligibility of the requester relatively to the specified conditions established distributor. This way is possible to verify if the inheritance rights are satisfied before the usage license is issued.

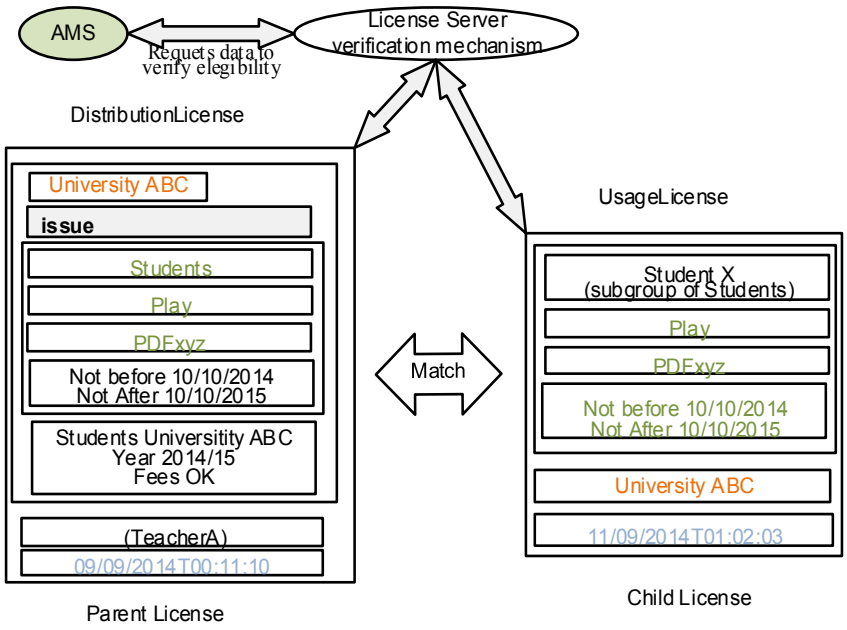

Figure 9 - academic scenario -issuance license generation

Another typical scenario occurs when a teacher wants to share a content with their colleagues and share this same content with their students registered in current year in University ABC. This is a typical situation in *elearning systems* where licensor consider two types of grantees: one for teachers and another for students. The licensor grants rights in license to University ABC with the issue privilege. The validation mechanisms will verify if it is possible to issue a license according the

requester profiler. When these conditions are satisfied the University ABC could then issue different licenses according the requester profiles (Figure 10).

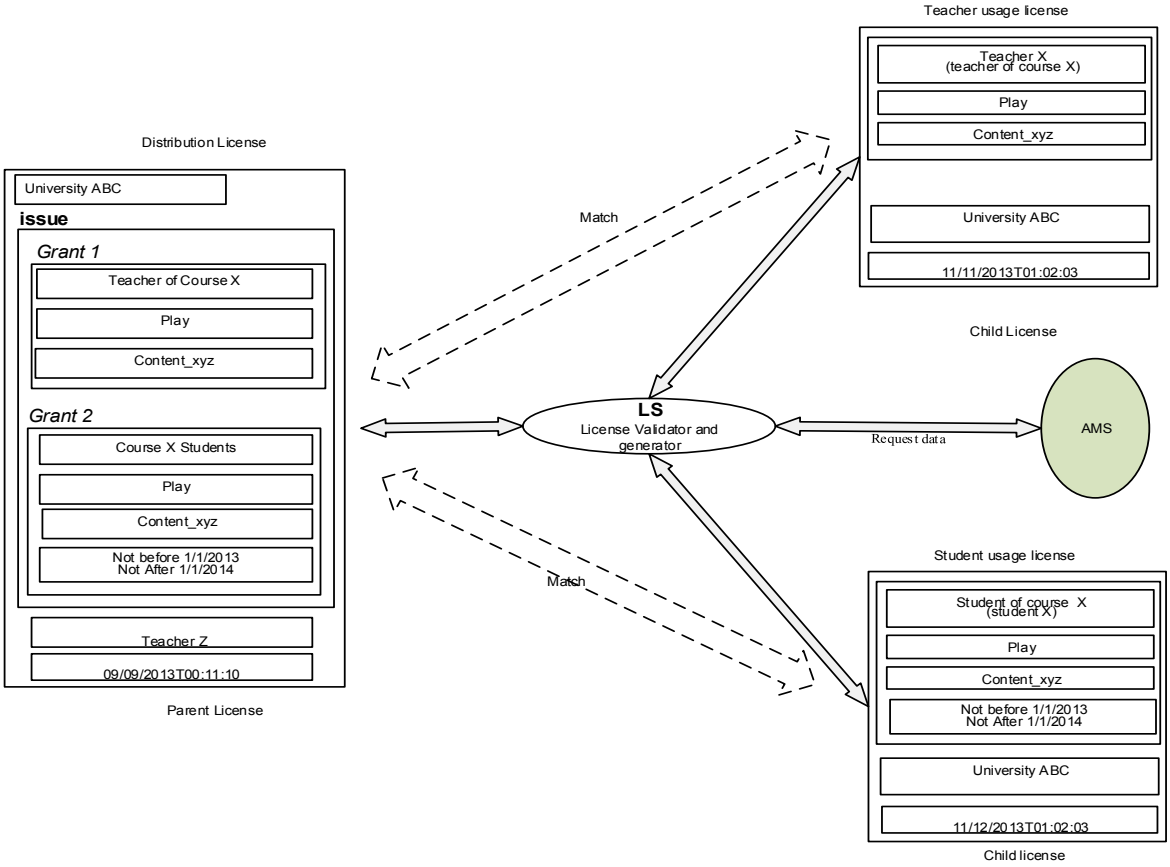

Figure 10 - academic scenario- multiple issuance license generation

4 VALIDATION RULES

In this section we will consider the scenario in Figure 9 as general example of application of validation rules. To verify if the requesting user obey the terms and conditions stated in the progenitor license the validation mechanisms implemented in the LS verifies if all of following rules are fulfilled before deliver the child license:

- The Issuer element (University ABC) of the child license is equal to Principal element (University ABC) of the Parent License,

- The Time of Issuance (11/09/2014T01:02:03) of the Child License is later than the Time of Issuance (09/09/2014T00:11:10) of the Parent License. Also the Time of Issuance of the Child License is within the interval specified in the conditions,

- The Right element (*issue*) of the parent License is the *issue* right,

- The elements included on the element resource of the grant on parent license are related with the granted elements on the child license this way:

- The principal on the parent license (students) covers anyone of the principal elements on the child license (student x).,
- Right element within the grant of the parent license (play) is equal to right element of the child License (play),
- The resource element (PDFxyz) within the grant of the parent License, is equal to resource element of the child license (PDFxyz),
- Conditions element within the grant of the parent license (validityInterval), are equal to the Conditions element of the child license,

- The conditions of parent license are satisfied (all students must be enrolled in current year at University ABC with all fees paid).

In this scenario the validation of the Principal (student X) in the child license and all parameters in the distribution conditions (Students University ABC, enrolled Year 2014/15, Fees paid) are very important because with this is possible to define to whom and which constraints are transmitted. Using these statements, the content owners (Teacher) and distributors (University ABC) can state the principal to whom the usage license will be designated having assurance the inheritance rights are respected when the child license is delivered. Applying these rules to previous scenarios is possible to observe that all are fulfilled and then the license can be delivered in a controlled way to requesting users in the educational domain.

5 CONCLUSIONS

In this paper we show how ARMS manage licensing among the participants in content DRM value chain The approach that ARMS brings when applying some of concepts of MPEG-REL, allows the rights transmission among participants in a way where the inheritance rights are followed in the delivered license. To enable the control over content users the interface between LS and AMS permits to get user data that will be used in the license validation process. In this process the usage license is only delivered if a set of rules are fulfilled ensuring this way the inheritance rights are maintained. With the data obtained from AMS the LS can act like a domain controller verifying if the user when requesting the usage license belongs to the educational domain and also if this user satisfies all the conditions stated on the distribution license, granting a new level of security to the content owner that wants to maintain the content usage inside the educational domain.

References

[1] Gadd, E., Loddington, S., & Oppenheim, C. (2007). A comparison of academics' attitudes towards the rights protection of their research and teaching materials. Journal of Information Science.

[2] Ku W., Chi C., (2004) “Survey on the Technological Aspects of Digital Rights Management,” Proc. of the 7th Information Security Conference, Vol. 3225, pp. 391-403, 2004

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

[4] Lee, W. B., Wu, W. J., & Chang, C. Y. (2007). A portable DRM scheme using smart cards. Journal of Organizational Computing and Electronic Commerce,17(3), 247-258.

[5] Sheppard, N. P., & Safavi-Naini, R. (2006, October). Sharing digital rights with domain licensing. In Proceedings of the 4th ACM international workshop on Contents protection and security (pp. 3-12). ACM.

[6] ISO/IEC. (2005). ISO/IEC IS 21000:5 - Part 5: Rights Expression Language

[7] ISO/IEC. (2004). ISO/IEC IS 21000:6 - Part 6: Rights Data Dictionary.

[8] Rodríguez, E., & Delgado, J. (2007). Verification algorithms for governed use of multimedia content. Online Information Review, 31(1), 38-58.

[9] 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.

[10] Wang X., “Design Principles and Issues of Rights Expression Languages for Digital Rights Management”, by ContentGuard Inc 2005, http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.115.1202&rep=rep1 &type=pdf

[11] ODRL Version 2.1 XML Encoding (2015), W3C ODRL Community Group, retrieved from https://www.w3.org/community/odrl/xml/2.1/

[12] Liu, Q., Safavi-Naini, R., & Sheppard, N. P. (2003). Digital rights management for content distribution, In *Proceedings of the Australasian information security workshop conference on ACSW frontiers 2003-Volume 21* (pp. 49-58). Australian Computer Society, Inc.

[13] (MPEG-21:DID, 2005) - ISO/IEC 2100:2 - Part 2: *Digital Item Declaration*

[14] MPEG-21 IPMP (2006). ISO/IEC IS 21000:4 - Part 5: Intellectual Property Management and Protection