Content related rights transmission with MPEG-21 in the educational field

Joaquim Marques[1], Carlos Serrão[2], José Metrolho[1]
[1]Instituto Politécnico de Castelo Branco, Castelo Branco, Portugal
[2]ISCTE-Instituto Universitário de Lisboa, Lisboa, Portugal
[1]{marques, metrolho}@ipcb.pt, [2]carlos.serrao@iscte.pt

Abstract: One of the main issues affecting educational content distribution and sharing is to ensure that the terms and conditions defined by the content owners are respected by the others, such as distributors and consumers. Authorship and the content integrity are the most basic rights that authors want to preserve in the educational field. To ensure that content and associated rights are protected, cryptographic techniques and mechanisms are applied to content, rights, protection keys and related metadata that are packaged in a digital object. ARMS is a new platform that was developed to preserve author rights in the educational field applying the MPEG-21 standard concepts. A web based services interface is established with the educational Academic Management System of the Academic institution in order to verify the user eligibility in this domain. After obtaining the usage license the user can send the license to other users, if that privilege has been granted. Our proposal uses MPEG-21 concepts in order to enable rights transmission among the main participants in the educational environment but with a mechanism where the inheritance rights established by the author are uphold. Through the integration between ARMS and the Academic Management Information System hosted in the educational institutions, user academic data can be retrieved in order to verify his eligibility.

Keywords: DRM, content protection, security, Intellectual Property, educational content

1. Introduction

Learning and education have specific requirements in terms of rights management such as attribution/authorship rights and content integrity authorship – these are the most important in the educational content distribution. A content owner can grant permission to use its content as long as he is properly acknowledged and with the assurance that the content ownership is properly expressed and correctly interpreted. The main intentions of the content owners and creators (teachers, researchers, and others) in the educational domain are oriented to the preservation of mainly two basic intellectual properties rights: the authorship and content integrity (Gadd, et al., 2007). Digital Rights Management (DRM) systems provides techniques and mechanisms, which congregates hardware and software to ensure the rights preservation of content providers against illegal usage (Ku W., Chi C., 2004). Modern DRM provides protected content to consumers adopting a license-based schema, which separates the protection keys from the encrypted content (Hwang, S. O., 2009). When a user wishes to perform some particular operation over governed content, the DRM Client checks that the user possesses a license that grants that permission, and that any constraints associated with that 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. A license is an aggregation of permissions awarded by some rights-holder to some beneficiary that can only be issued with the permission of the rights-holder (Sheppard, N. P., & Safavi-Naini, R., 2006). Rights issuers only generate licenses according to some policy set by the main content holder that provides content. Once a content is distributed to a distributor the owner loses its control over the content distribution and cannot enforce his rights requirements (Li et al., 2010) (Sachan E. et al., 2011). Not only it 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 and transmitted to users that are in a controlled domain. In the educational area this is a concern because many times the content owner not only wants to preserve their basic rights (authorship and content integrity) but also maintain the content usage controlled in this domain. Traditionally DRM systems focuses mainly on the transfer of rights between the copyright holders and the users, having less attention to the sharing of rights among users (Zhang ZY, 2011). In fact, the ability to support rights sharing has significant meanings in the DRM technology and educational field needs that.The MPEG-21 standard specifies mechanisms to enable controlled distribution of multimedia content through the complete digital value chain. The MPEG-21 Rights Expression Language (MPEG-21 REL, 2005) and Rights Data Dictionary (MPEG-21 RDD, 2004), specify the 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 verify 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. Rodríguez, E., & Delgado, J., (2007) propose some verification algorithms 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 generated license to be distributed obeys initial terms and conditions defined by the content owner. This paper, presents one DRM system, called Academic Rights Management System (ARMS), adapted from another proposed generic open DRM system, called OpenSDRM (Serrão C. et al., 2005), intended for sharing access to content based on the controlled domain concept. ARMS allows access to content to be shared amongst a pool of academia users, within the limits defined by the content provider through the insertion of control modules in the license server that verifies if the user is eligible when requesting a specific usage license. In order to do this, a major external component is introduced in the ARMS architecture enabling the exchange of information with the license server. This component is the Academic Management System (AMS) that controls and regulates all academic activities in the educational institution (Figure 1). ARMS followed an approach based on a web-based API that makes possible the integration of this external component and the integration level only depends on 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.

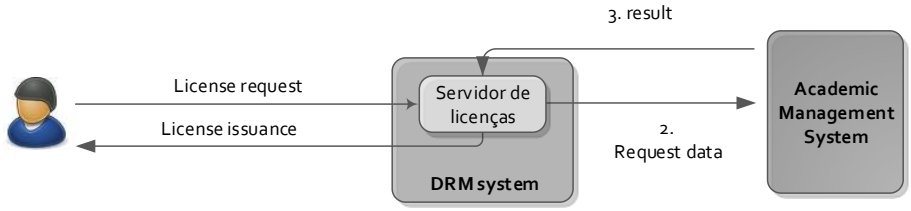

Figure 1 – License issue validation

The central component of the License Sever 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 it applies the mechanisms that verifies the legitimacy of the license requester inside the institution educational domain and verifies if the original terms and conditions are in accordance with the line of succession rights expressed in progenitor license.

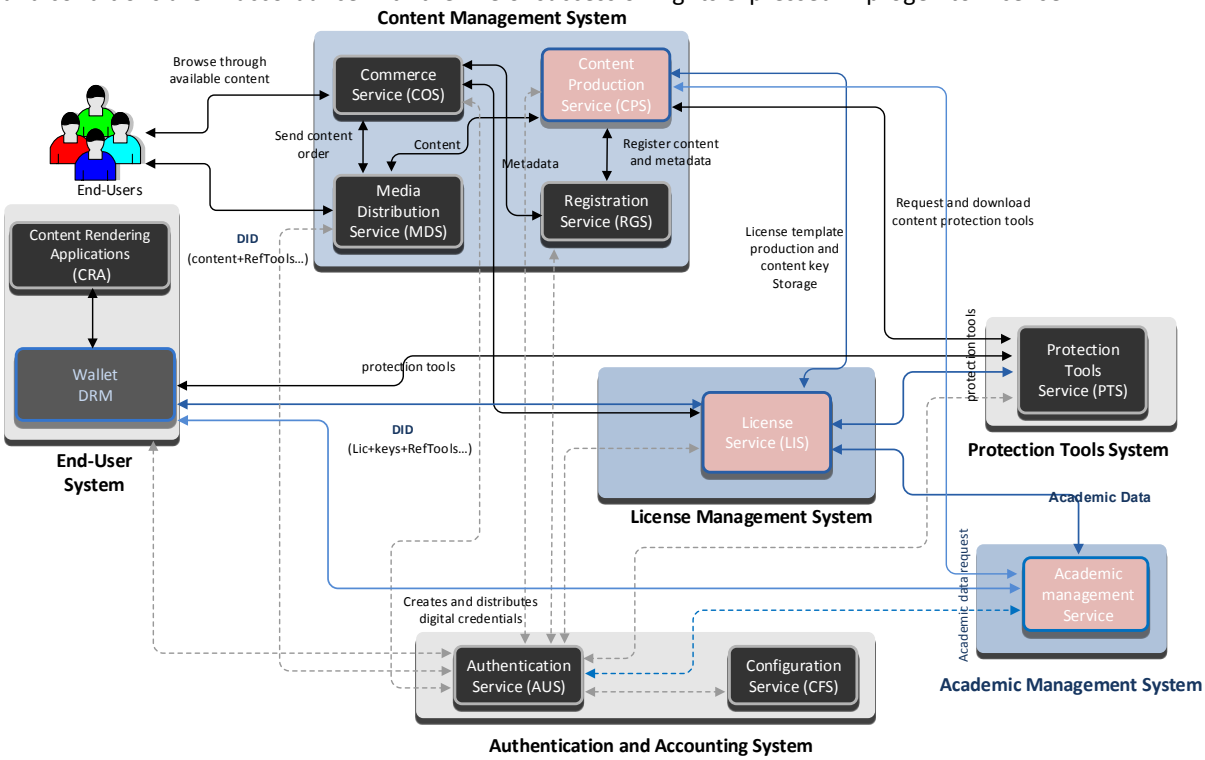

Figure 2 – ARMS main components interactions

In this paper we will describe some rights-sharing control mechanisms based in MPEG-21 standard that augments the control over a domain (the institution educational domain) through the validation of the license

generated in the ARMS system (Marques J. et al., 2015) (Figure 2). 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 content to be distributed to students in a specific course the mechanism will verify if the students satisfy that condition before generating and issue a usage license. 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 it is possible to make the license distributor act like a domain controller regulating the issuance of licenses in the educational context

2 Licensing

The technological enforcement of rights is one of the DRM systems common functionalities, to prevent unauthorized usage (Liu, Q., et al., 2003). Rights are expressed in a XML-based special purpose language, designed as Rights Expression Language (REL) that syntactically bounds a digital object identifier, an actor identifier, a content encryption key and set of conditions. The license is the most important concept in the 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, such as MPEG-21 REL (MPEG-21 REL, 2005), XRML (Alpern Y., 2008) and ODRL (ODRL version2.1, 2015), make use of XML due to its extensibility and flexibility. Basically the online DRM system is a set of content and rights management related services offered by the Content Provider (CP) to the Content Creator (CC) and Content Distributor (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.

Our approach consists in separating content from the rights and embed them in a digital object conforming with MPEG-21 Digital Item Declaration (DID) (Bekaert J., Sompel H.,2006). The result consists in two objects: the content object (containing the metadata and the protected content) and the rights object (containing the metadata, the license and the content protection key). The generated digital objects have similar structures, however we propose a 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 (Marques J. et al.,2015). In our approach we use MPEG-21 IPMP standard (MPEG-21 IPMP, 2006) that considers them 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. The supported method of representation of a signature in the REL standard is the XMLDSig standard (Bekaert, J.,& Van de Sompel, H.,2005). The encapsulated signature signs all elements within the digital item (Bekaert J., Sompel H.,2006) with one exception - the annotation element.

The ARMS protection implementation is based on the application of different techniques and mechanisms resulting in an overall high protection level. When a user is authorized to perform an action over a given content, is possible to unprotect it using the corresponding mechanisms through the trusted tools at user side obtained from the ARMS system. These protection tools will be provided by the Protection Tools Server (PTS). To protect the resource, the MPEG-21 IPMP standard defines the notion of tool, which represents protection mechanisms that can be encryption algorithms capable of providing security services. This IPMP tool contains all required information about the type of algorithm and its parameters. The tool can be integrated at the level of the DID hierarchy, which is required to ensure the security of the content. The metadata can remain unencrypted so that any recipient can read this before take any action on content usage.

Our emphasis is the license structure itself in order to enable rights transmission. Our license management scheme considers the integration of rights management into the License Server of an existing DRM system adapted to support AMS interactions: the ARMS system. In this system, we adopt MPEG-21 REL to our scheme and apply it into the educational field. It is used in the rights managing model of the ARMS system to establish the progenitor requirements through the verification of the users' qualification when they request a license. The License Server holds a database of registered users and verifies them on behalf of the progenitors and qualifies them (obtaining related information from the AMS) before license issuance. Distribution and usage licenses are key elements. The distribution license is used to express transmitted rights to next part on the value chain. The usage license focus on the rights requested to the distributor and deliver a license to the final user. A parallel stream of rights produced between users when rights are shared and transferred from one to another could exist if the transmitted rights are enabled to do this.

In MPEG-21 a license contains the following parts:

1) Grant or grantGroup: each grant conveys to an identified party the right to use a resource subject to certain conditions. A grant consists in a minimum of 3 fragments: the "Principal" fragment containing the User ID (U_{ID}) and user public key ($Kpub^{U}$), the "Resource" fragment containing ResourceID and ResourceUrl, and the "Rights" fragment specifying the usage permissions and optionally conditions that limits content usage.

2) The license issuer digitally signs the license using his own private key (Kpri)v. In addition, the issuer may provide additional information about the issuance of the license.
3) Miscellaneous additional administrative information (Figure 3).

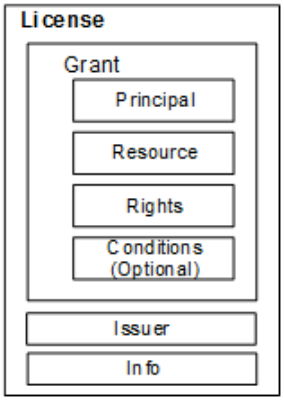

Figure 3 – MPEG-21 simple license structure

To check if a principal can exercise a right over a resource against a license, the interpreter installed in a module in the License Server needs to perform the following tasks (adapted from Wang X.,2005) before the license is issued,:

- verify if the issuer is trusted, and validate the signature (if any) associated with the issuer to ensure that the related information in the license is authentic,
- for each grant in the license,
  - if there is a principal in the grant, check if it matches with the requesting principal
  - check if the right in the grant is the requested right.
  - check if the resource in the grant matches with the requested resource (and if the resource is omitted, then the requested resource should also be omitted).
  - if there is a condition in the grant, check if the condition is satisfied.

When the issuer verification is successful, and there is a grant for which all the checks are successful, then the request to exercise the right is authorized. One of the concepts in ARMS that enables this verification is through the web services interface between the License Server and the AMS. With the returned information from the AMS the verification module can execute these checks and if they are valid then can issue the license.

2.1 MPEG-21 support to rights distribution

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 them is related with the grant *issue* mechanisms ant the other is related with the *delegation* control mechanisms. While one enables an authorized distributor with the privilege to issue usage licenses from a distribution license, the other enables users to transmit rights to other users in a 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 one. To enable this, MPEG-21 introduces two special elements in his REL specification: the "<issue>" and the "<*delegationControl*>". With these elements MPEG-21 gives support to two types of granted controlled rights.

To control the grant of permissions and constrains over governed content where the principal receiving the grant can delegate rights to other users in a controlled manner, a delegation control mechanism is used. With this mechanism, the rights holder can specify that the licensee can delegate the permissions that a "grant" or "grantGroup" conveys. A license issuer can define through a distribution license if the delegate can grant rights. A license that enables infinite redistribution shall have a "grant" that contains a "delegationControl" element, which enables the principal to whom that "grant" is issued to delegate it. When a principal delegates a "grant" the delegated license must contain a "delegationControl" compatible with the "delegationControl" element in the original license and it must be at least as restrictive as in the original one. Moreover, the license issuer can impose constraints on delegation, for example controls on adding or changing conditions during delegation, the allowable depth of the delegation chain and/or the principal to whom the "grant" or "grantGroup" may be delegated. In the MPEG-21 specifications the constraints can be specified by four delegation control elements: "<ConditionIncremental>", "<ConditionUnchanged>", "<DepthConstraint>" and "<ToConstraint>" (Figure 4). With these elements incorporated in a license distributors have the privilege to control the rights transmission on behalf of the owner and independently issue licenses to users. Using these

elements is possible to enable content sharing schemes where the distributors using their received redistribution licenses can generate new different types of redistribution licenses to their sub distributors and new usage licenses to users according to the permissions and constraints in their received redistribution licenses.

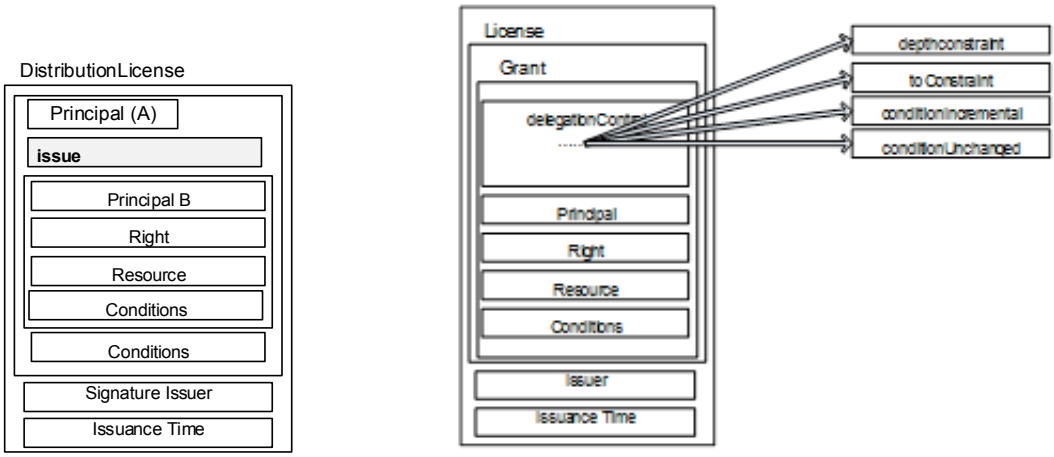

Figure 4 – issue and delegation control license structures

Basically, the issue right can enable an authorized distributor to redistribute licenses in a controlled way to final users. The DelegationControl can enable the final users to redistribute licenses among them. For the sake of space we will focus on delegationControl depth constraint element in this paper. Our focus here is how to control the distribution of rights between users in a way that enables license superdistribution, controlling the number of times a grant can be delegated.

The "delegationControl" depth constraint model allows the superdistribution of content in a controlled way. Using this mechanism content creators and distributors can state the maximum number of times that content can be redistributed controlling the tree depth. Obviously the child license that dependent from the parent license can't exceed the rights and conditions specified in the ancestor.

2.2 Distribution Usage Scenario in the educational field

In the educational field the content lifecycle is not different from other fields. The roles played by participants are more complex because sometimes they act like distributors while some other times they act like consumers (Marques et al., 2012). To grant rights to other participants the distributor must have the privilege to issue rights and these rights must consider the consumer usage. Also, these granted grants could give to the final user the privilege to distribute the license to others. Consider the following scenario: imagine that "Professor A" issues a license to "University ABC" publishing department with the right to issue a grant so users can read the content "Paper A". As show in Figure 6 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 "Paper A" and also including a grant to distribute it to other students. With the "depthConstraint" element specified in "Student A" license is possible to delegate his grants to "Student B". When "Student A" generates and transmits the new license to "Student B" the "depthConstraint" is reduced by one unit and "Student B" reduce it further (until it reaches zero). The "delegationControl" depth constraint model allows the superdistribution and use of content in a controlled way.

The Teacher acts as a content provider granting to the distributor (academic publisher) the right to distribute the license to students. The academic publisher has a distribution control license consisting of some elements that grants him (principal) the issuance of licenses to the final users in the same conditions (delegationControl =depthConstraint-1) (Figure 5)

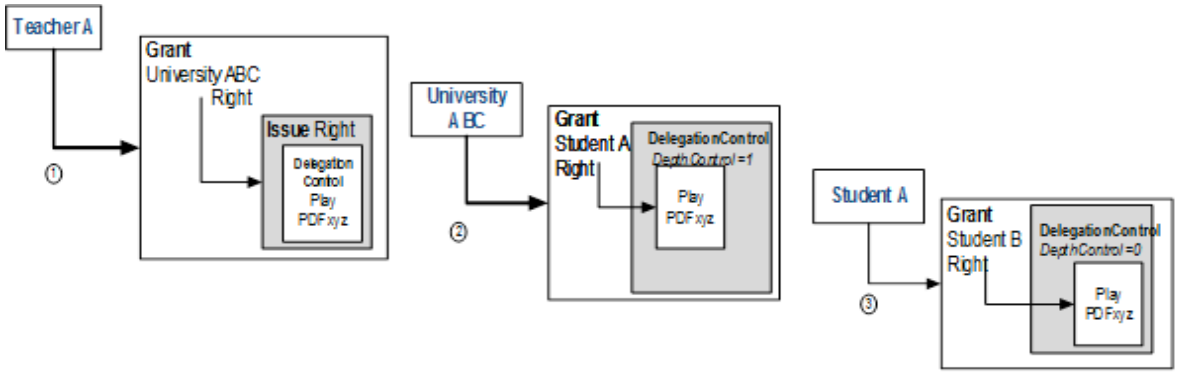

Figure 5 – Rights delegation with depthConstraint control

At initial stage is assumed that a user acquires content in the form of a Digital Item (DI) from a server. In Figure 6 is possible to see both licenses in the MPEG 21 REL format. In presented scenario the delegation control verification algorithm will be applied when the final user tries to obtain a usage license granting him the right to view the "Pdf_X". If other student tries to obtain a license from "Student A" he will be refused because the "depthConstraint" is zero and "Student A" cannot generate a new license. The corresponding obtained license permits to play and have a delegation control that permits issuing this license to other users with a "dcount=1". When the other user obtains this license, then "*dcount*" is reduced to zero. That means that delegation activity is over and he cannot transmit it to other users.

Parent license

```
<license>
...
 <grant>
    <delegationControl>
          <depthConstraint>
                <count>1</count>
          </depthConstraint>
    </delegationControl>
    <keyHolder licensePartId = "Teacher X">
        <info>RSA Information</info>
    </keyHolder>
    <mx:play/>
    <digitalResource licensePartId="PDF_x">
       <nonSecureIndirect URI=" http://arms.com/di/PDF_x.di" >
     </digitalResource>
 </grant>
 <issuer>
    <dsig:Signature>..Digital Sign Academic Publisher..</dsig:Signature>
    <details>
       <timeOfIssue>20013-10-01T01:25:00</timeOfIssue>
    </details>
 </issuer>
</license>
...
```

Child license

```
<license>
...
<grant>
    <delegationControl>
          <depthConstraint>
                <count>0</count>
          </depthConstraint>
    </delegationControl>
    <keyHolder licensePartId = "Student A">
          <info> RSA Information</info>
    </keyHolder>
    <mx:play/>
    <digitalResource licensePartId="PDF_x">
          <nonSecureIndirect URI="http://arms.com/di/PDF_x.di" >
    </digitalResource>
 </grant>
 <issuer>
    <dsig:Signature> ..Digital Sign Teacher X.. </dsig:Signature>
    <details>
          <timeOfIssue>20013-10-10T03:05:00</timeOfIssue>
     </details>
 </issuer>
</license>
...
```

Figure 6 – Parent and child license with depthConstraint delegation control

These licenses are generated obeying to some special rules and some elements must match to the progenitor license and child license. Is possible to see equivalences between some elements on the license in Figure 7 (see colors) when Student Y deliver is license to Student X. These equivalences must match some of the adapted rules stated in Rodriguez E., et al (2006) applied in the ARMS. There exists two licenses: a parent (Student Y) and a child license (Student X) generated from the parent. If the equivalences match them child licence is generated and delivered. The LS in ARMS system have a special module that do this (indeed his description is outside the scope of this paper)

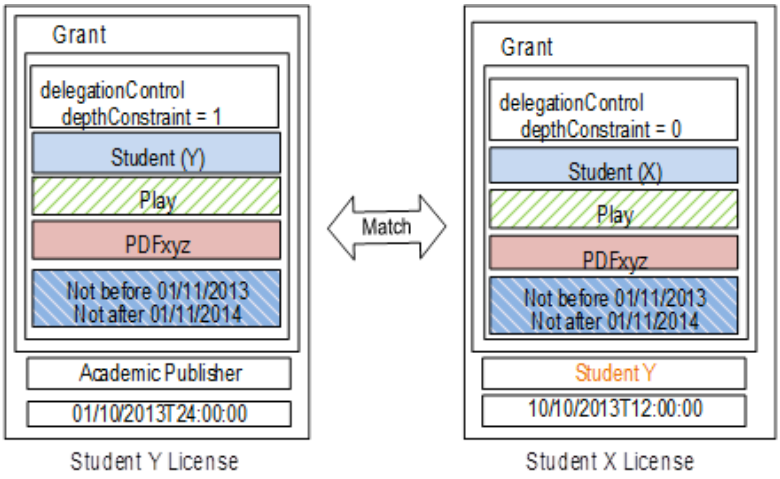

Figure 7 – depthConstraint delegation control rules verification

In a simplified manner is possible to see in these licenses that Student (X9 belongs to Students (Y) group, the delegation control decreases by one, the right is the same and resource is also the same resource on both licenses. Also the child license was delivered after the parent license. If the actual time is inside the time interval them the usage license can be generated. Applying these simple rules in a delegation control depth constraint is possible to control the inherited rights among final users.

2.3 Description of the validation process

In order to understand some of the concepts on this paper, the license validation process is described. The main steps on the validation process are detailed next and Figure 8 depicts the main interactions between user devices and some core DRM components:

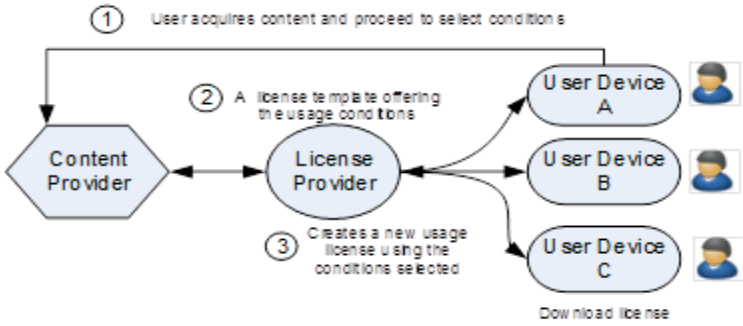

Figure 8 – Content acquisition and usage license creation

a) Parent license elements are extracted;
b) XML license file is created based on extracted license elements;
c) XML license elements are extracted;
d) Verification of all rules begins;
e) If all rules are fulfilled then the child license is generated and stored;
f) The requester can download the child license.

A key point that allows the verification if all rules match is the web services interface between License Server (LS) and the AMS. With this interface is possible to obtain academic user related data. With the obtained data returned from the AMS is possible to verify the eligibility of the user inside the institution academic domain whenever a new license is requested. Appling some processing control mechanisms in the LS it is possible to validate the new license and transmit it to the requester. The LS obtains the requester user academic data from the AMS and apply the verification mechanism. If all the rules are fulfilled then the LS signals the issuer that he can issue a license in the specified conditions. If a “delegationControl” “depthConstraint” element is present in the license then the new generated license to be issued by the final user is decreased by one unit.

2.3.1 License processing and generation

When a user requests a license generation, an initial process needs to occur on the user device. The client device application verifies if the license exist internally. If not, it then requests a license lookup on the LS

corresponding to the "ResourceID" and "UserID". If it is found then the user can proceed and download it from the LS and use the associated content. If the License is not found at the LS, the application on the client device requests the generation of a new one.
When the user requests a new license, it activates the license generation mechanism. This module establishes contact with the AMS and verifies if the user belongs to the educational institution domain. This mechanism initializes a license lookup, searching the internal registry license database in LS and verifies if a license related with the resource exists. If the license is found it is loaded in a special module, the License Processing Module (LPM) residing in the License Server and following steps take place:
A) License validation
Before a license can be generated, the license needs to be valid. There are three reasons for a license to be invalid:

1) It is malformed: when the license does not meet the specifications detailed in the data model or if there are permissions granted by the agreement that are not present in the permission set associated with it;
2) The constraints for the license cannot be met. When the license has constraints that apply to the entire license, that can no longer be satisfied (eg time limit or number of play counts);
3) The license is legally invalid. The license could be revoked or the licensor not having authorization to issue licenses.

After a valid license is loaded in the LPM the License validation process begins. LMP supports license signature validation and license status checking. License signature validation is done to ensure its integrity and authenticity. Also, the license status checker verifies if the license is malformed and inspects a revocation list to find if the identified license is active and if the distributor is authorized to issue licenses.
B) License generation
When the user request the license to be generated, he interacts with a form where he can select the available license templates and related conditions pre-defined by the original content owner and sends the request. User data like registered "userID" and some academic data are sent to LS. We must distinguish two types of licenses:

- Distribution License. A distribution License is a special kind of license where rights are offered to the requester under predefined conditions. In the distribution license the principal element is the entity that have a specific role that will grant rights to the content, but before was issued by another parent entity. To generate this type of license the LPM verifies (e.g against data returned by the Academic Management System – AMS via web services) if the user (principal) is eligible verifying if is registered in the educational institution. The other elements must be conformant with the original. The verification algorithm validates conditions and if successful generates a XML document with the conditions associated with the original matching grants, which can be stored on the license server. This license is generated according to the MPEG-21 REL specification. The Distribution license is issued by the content owner or other entity, such as the University, on behalf of the rights owner. The distribution license is created in the LS using one of the templates the content owner has selected when he made the content upload. This distribution license is issued to the distributor (e.g University) granting the right to issue a license to final users.
- Usage License. A usage License is derived from one of the distribution licenses stored previously on the LS. The final user selects one of the distribution licenses that are automatically loaded by the LPM. The final user selects a set of available conditions compatible with the ones extracted from the distribution license. A temporary MPEG-21 usage license based on the distribution license is then created and loaded into the LPM. Before this license is delivered to the requester the *license interpretation and verification* process is executed.

C) License Interpretation and Verification
After the temporary license is loaded in the LPM, the License Interpreter Module (LIM) receives it and makes some dynamic queries extracting remarkable data elements from the license and executes these queries against the pre-loaded distribution license elements to verify if matching rules are observed. Then the LIM applies the validation algorithm to verify if the result conflicts with terms and conditions given by the original matching grants. If the matching fails, the requester will have no usage rights and the issuance is terminated. If for some reason delegation control is zero in the distribution license, the activity of delegation will be, also terminated and the requester user will not get the usage license. If the result of the validation algorithm is successful then the next step is executed.

D) *License Storage and Delivery*

If a usage license is requested by the final user then this license is registered and stored in the internal database and prepared to be sent to the requester embedded in a MPEG-21 Digital Item (DI). This license database works for saving, searching and retrieving licenses using the Unique IDs to reference resources (resourceID) and users (UserID). Finally, the usage license, the encrypted content protection key and some related metadata are embedded in a DI. The final user is then presented with a temporary link where he can download the DI containing the license and sent to the user device where rights will be enforced.

The usage license is sent embedded in a Digital Item (IPMP DIDL) to the user device where rights will be enforced. The previously described license generation process is depicted on Figure 9.

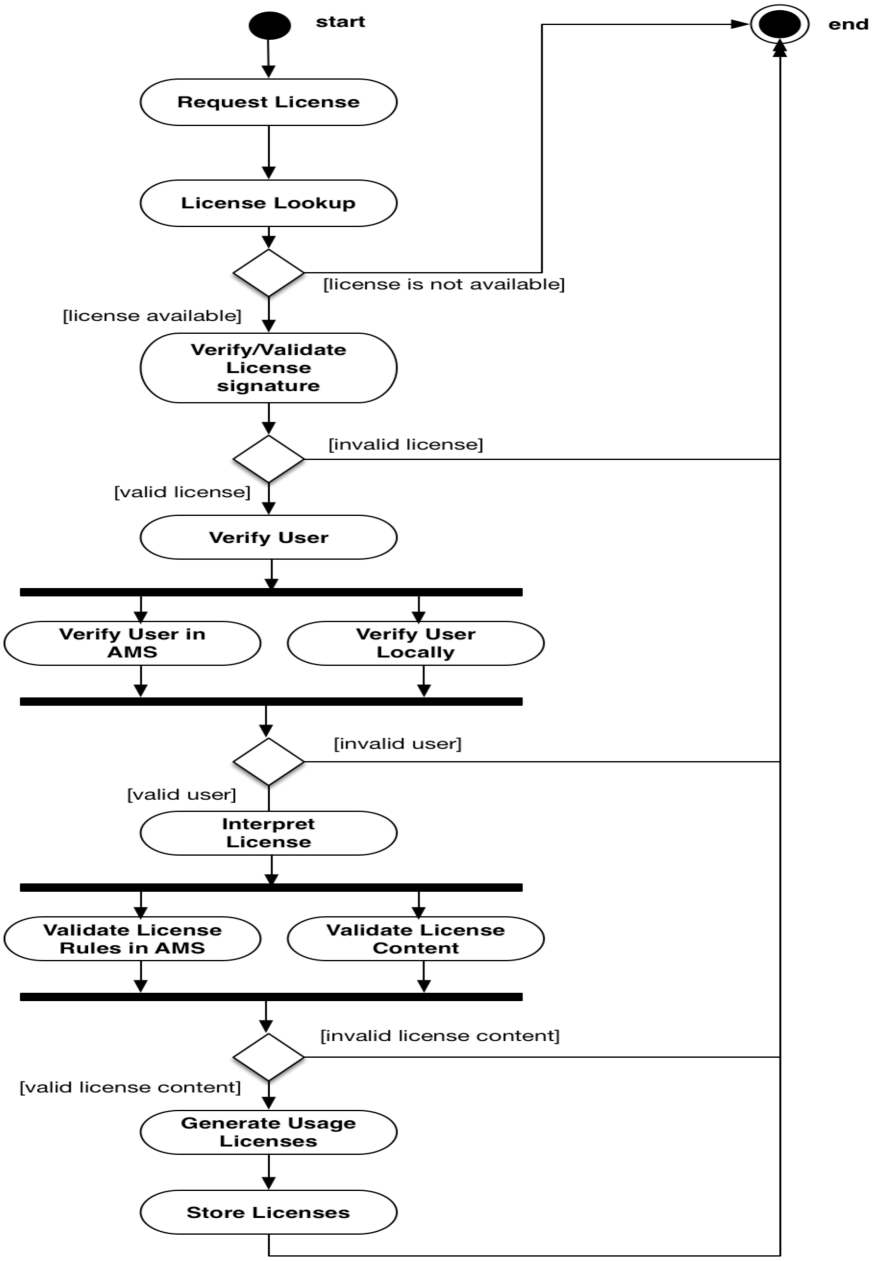

Figure 9 -License generation management flow

3 Conclusion

Ensuring that the terms and conditions stated by content owners on licenses are observed and enforced on other participants of the content value chain, such as distributors (eg. teachers) or consumers (eg. students) is an overall concern, valid also for digital educational content. The assignment of licenses is a requirement in order for the distributor in the DRM system to unambiguously communicate the licensing of the content giving an enhanced user experience. The educational domain is not an exception. Not only is important to validate the issued license, verifying if the terms and the conditions stated in the parental license are observed in the

child license, but also is important to verify if this license is generated to users that are in a controlled domain in the educational context. This way it is possible to control rights transmission when a distributor wants to share content having the assurance that the content will be used in the context he wants. With our license scheme, resource owners can specify restrictions on who can use their academic learning resources under specific constraints, while peer consumers also can deliver and delegate rights to other peers.
Rights sharing control mechanisms based in MPEG-21 standard that augments the control over a domain (the institution educational domain) were presented and described. Through the validation of the license to be generated in a specific designed DRM system (ARMS) is possible to content owners control which users can obtain a license within the constraints previously defined, giving them the power to control rights transmission and usage control in the educational domain. With the verification mechanisms implemented in LS it is possible to control the distribution of licenses making the license server act like a domain controller that regulates the issuance of licenses in the educational context.

4 References

Bekaert J., Sompel H. (2006) *Representing Digital Assets using MPEG-21 Digital Item Declaration*, Int. J. on Digital Libraries Vol. 6 No. 2 Pg. 159-173

Bekaert, J., & Van de Sompel, H. (2005) *A standards-based solution for the accurate transfer of digital assets*. *D-Lib Magazine*, *11*(6), 1-24.

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. *33*(6), 686-701.

Halpern, J. Y., & Weissman, V. (2008) *A formal foundation for XrML*, Journal of the ACM (JACM), 55(1), 4.

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

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

Li H, Zhao L, Wang C, Ma F., (2010) *DRM system for multiple cascaded business operators*, In: IEEE International Conference on Multimedia and Expo (ICME), Singapore.

Liu, Q., Safavi-Naini, R., & Sheppard, N. P. (2003, January) *Digital rights management for content distribution*, In Proceedings of ACSW frontiers 2003-Volume *21* (pp. 49-58). Australian Computer Society, Inc.

Marques J., Serrão C., Metrolho C. (2015) *Enabling Content and rights transmission in the Educational field with ARMS*, to be published in proceedings ICWI15

Marques J. Serrão C., (2012) *Rights Management and Technological Protection Measures in Educational Field*, in Proceedings ECEL2012, Gronningen.

MPEG-21 RDD. (2004). ISO/IECISO/IEC IS 21000:6 - Part 6: Rights Data Dictionary.

MPEG-21 REL (2005). ISO/IEC IS 21000:5 - Part 5: Rights Expression Language

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

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

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

Sachan, A., & Emmanuel, S. (2011) *Rights violation detection in multi-level digital rights management system*. *computers & security*, *30*(6), 498-513.

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.

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.

Zhang ZY (2011) *Digital rights management ecosystem and its usage controls: a survey*, Int. J. Digital Content Tech. Appl 5(3):255–272

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