Architectural solution for interoperable content and DRM on multichannel distribution

Pierfrancesco Bellini, Ivan Bruno, Paolo Nesi, Davide Rogai
DISIT-DSI, Distributed Systems and Internet Technology Lab
Dipartimento di Sistemi e Informatica, Università degli Studi di Firenze
Via S. Marta, 3, 50139 Firenze, Italy
www.AXMEDIS.org, nesi@dsi.unifi.it, http://www.dsi.unifi.it/~nesi
Office: +39-055-4796523, Fax: +39-055-4796363

Abstract

According to the new trends, final users are interested in acquiring content from different distribution channels and in using it on different devices/tools, while interchanging the content among devices and tools. This paper depicts the main scenario and reports a unified architecture supporting multichannel distribution and content interoperability. The paper presents the results produced in this area within AXMEDIS IST FP6, a research and development integrated project (Automating Production of Cross Media Content for Multi-channel Distribution) partially funded by the European Commission.

***Keywords**: e-commerce, multichannel distribution, interoperable DRM, iDRM, MPEG-21.*

1. Introduction

Final users are requesting more functionalities from content and content distributors. Content distribution services are grounded on a large set of technologies for content formats, connections and digital transmission, content processing and adaptation, content protection, and for Digital Rights Management, DRM. See for a general overview [Koushanfar et al., 2005]. In terms of content formats and DRM, many solutions are available on the market such as Apple i-Tunes, Microsoft Windows Media DRM, Adobe DRM, Intertrust, and OMA (Open Mobile Alliance, [Iannella, 2002]), and others see [Lin et al., 2005]. Most of these solutions have relevant limitations on the content formats and interoperability, since they support only a limited number of media formats, devices and distribution channels. Others have DRM mechanisms which allow exploiting/controlling only a limited number of rights on the digital content and therefore they allow establishing only a limited number of business models. Despite the large number of offered solutions, none of them seem to be generally accepted.

Business and final users are becoming more and more interested in using more complex digital content (e.g., interactive content with several kinds of media inside: audio, video, games, document, etc., SMIL, HTML, SCORM, etc.) [Bellini et al. 2006]. They expect to receive this kind of content from different distribution channels and to use it on different devices/tools, according to different business models (e.g., renting, pay per play, pay per use, all you can eat, passing the content to friends while receiving some bonus). The present state of the art is dominated by the lack of interoperability among different: content formats and DRM solutions (different licenses, protocols, protection models, etc.), distribution channels, devices and tools, accounting information, etc.

Attempts to solve this situation have been the creation of open DRM standards; such as those proposed by MPEG-21 [Wang et al., 2005], and/or by OMA [Iannella, 2002]. On the other hand, market standards such as i-Tunes, Microsoft DRM, can hardly be substituted by these new open standard solutions which suffer from a lack of interoperability among them. This is due to the assumption each of them make as to become the universally “Adopted Standard”. Among the emerging standards, the MPEG-21 is likely to be the most promising, it can deal with: license (formalized in some REL, Right Expression Language), event reporting for logging the actions/rights performed/exploited on the players, and the formats for content packaging called Digital Item Declaration (DID) [MPEG-21 DID] and the protection information called Intellectual Property Management and Protection (IPMP).

In this paper, the focus is on the problems lying behind any enabling of interoperability among multiple distribution channels. The studies and the solution reported in this paper have been worked out for AXMEDIS (Automating Production of Cross Media Content for Multi-channel Distribution) Integrated Project FP6 of the European Commission (http://www.axmedis.org), [Bellini and Nesi, 2005]. The

AXMEDIS consortium consists of: European digital content producers, integrators, aggregators, and distributors, collecting societies, together with information technology companies and research groups.

2. Digital Rights Management Scenarios

At present, there is a large number of content formats ranging from basic digital resources (documents, video, images, audio, multimedia, etc.) to integrated content packages such as: MPEG-21 [MPEG-21 DID], SCORM [Mourad et al., 2005], OMA. Packages can wrap digital resources with other related information (e.g., metadata, identification codes) so as to make them ready for delivery. Such solutions are more flexible, if compared with proprietary solutions where the DRM can be applied only to the single resources. The typical content production and distribution scenario, which synthesizes the most relevant phases from content packaging to content distribution, is shown in Figure 1.

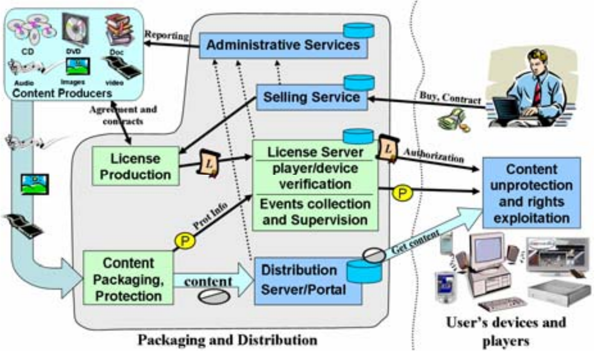
CD
DVD
Doc
Audio
Images
video
Content Producers
Reporting
Administrative Services
Selling Service
Buy, Contract
Agreement and contracts
License Production
L
License Server
player/device verification
Events collection and Supervision
L
Authorization
P
Content unprotection and rights exploitation
Prot Info
P
Content Packaging, Protection
content
Distribution Server/Portal
Get content
User's devices and players
Packaging and Distribution

Fig.1–A simplification of a typical DRM based Content Production and Distribution solution.

The distributor establishes a contract/agreement with the Content Producer (this is a simplification). The distributor may protect the produced content package to keep a certain level of control about the exploitation of rights. The content distributor may make business by allowing consumers to access the content through specific licenses. The latter ones describe the set of rights granted to the consumers (the rights are the actions that can be performed on the content, e.g., play, print, copy, etc.). The digital resources are packaged in order to get a package for the distribution which is protected by using some algorithms. The protection information (P) has to reach the final user in order to allow him to unprotect/open digital resource and/or the package, when the user is authorized to do it. This kind of information is typically called Protection Information or IPMP as in MPEG-21. Both license and protection information is needed to exploit the rights on the content. They can reach the content via different paths or together. If they arrive together, the protocol from the License Server to the Player/device results to be simplified; and license production cannot be delegated to third parties.

Once the content package has reached the consumer's player, he/she may exploit the acquired rights, e.g., "a play". In order to permit the performance of authorized actions only, the player/device has to verify if it can be authorized according to the license, for example contacting the License Server. The License Server processes the license database to verify if the authorization can be granted to the player. In alternative, a copy of the license can be sent to the player. Every time a right is exploited, the involved distributors/ producers may need to have back an evidence for their Administrative Services (e.g., for sending the bill). This information can be easily recovered in solutions that constrain the player/device to contact the License Server for each grant authorization. In those cases, a sort of Action Log record (Event Report in MPEG-21) can be produced by the player/device. The information on the user Action can be used for recovering statistics about content usage, to adjust the service, to make market analysis, etc.

According to the above short presentation of the typical scenario, it can be stated that: content formats, license, protection information, and action log, strongly influence the architecture and protocols of the distribution channel, thus creating differences which may limit the interoperability among the different channels and DRM models. The difficulties are mainly due to the differences among the different DRM solutions and devices, to the information transferred among the involved entities and to the related protocols used to perform authentication, granting the authorization, accessing to the license, accessing to the protection information, requesting license production, reporting actions log, etc. All these details are strongly relevant for the interoperability among different DRM distribution channels even if they are based on different tools, formats and protocols.

3 AXMEDIS Distribution Services

A description of the AXMEDIS architecture can be recovered from [Bellini et al, 2005] and the full specification from the AXMEDIS portal. The following AXMEDIS architecture for multichannel distribution of interoperable content and DRM is supported by a number of service tools for: Authorizing and Managing Licenses, Supervising and controlling activities, as well as for User and Tool Authentication. The models and tools mentioned in the scenarios can be adopted by any actor of the value chain without any limitation; therefore "producer" and "distributor" have to be intended as roles

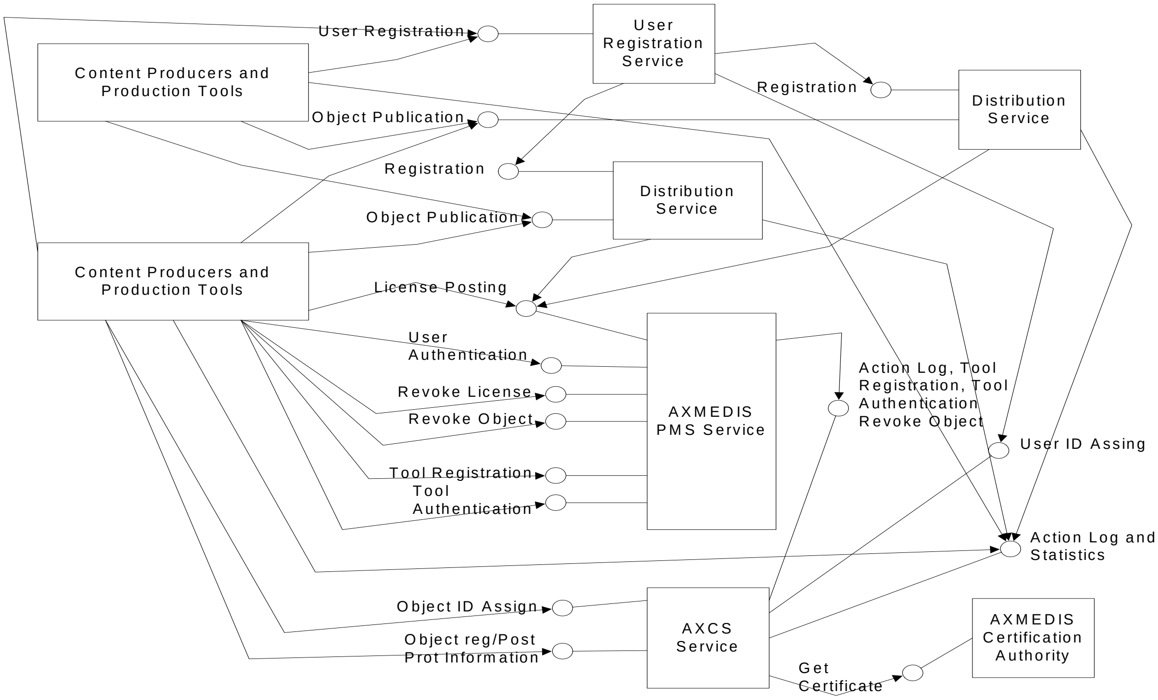

Figure 2 – DRM Services, Producer's point of view and its tools, a Business to Business case from Producers to Distributors. (Please note that for one of the Producer we have not depicted all possible connections)

rather than effective entities. The tools mentioned above refer to generic functionalities, as described below.

The main rationales which led to the definition of the AXMEDIS tools and web services are reported along with the presentation of the most relevant scenarios for B2B and B2C, respectively.

Authorizing and Managing License Service

The AXMEDIS PMS (Protection Manager Support) Service is mainly a License Server which allows granting the authorization to the players on the basis of the licenses. It is the primary access for a large set of capabilities exploited by the content producers such as: license posting, verification, revoking; revoke of objects, tools and users, etc. Some of these services are delegated to the AXCS (AXMEDIS Certifier and Supervisor). Most of the AXCS services are conveniently made accessible by the PMS since it establishes a secure communication channel with the Production Tools and Final User Tools. All the above services have information (such as certificates, protection information, grants, action logs, etc.) that should pass via a secure channel in order to avoid simple sniffing attacks.

Supervising and Control Service

The AXCS (AXMEDIS Certifier and Supervisor) Service provides a number of services for producers and distributors such as: object ID assignment, user ID assignment, access to Action Log reports and statistics about events and user usage.

In addition, the AXCS provides a number of services to the PMS such as: storing of the actions logs (grants, posting of licenses, and other events), tool registration and authentication, posting of protection information, revoke of object, tools and users. The AXCS collects and keeps the information regarding the registered objects, users, devices, etc., and therefore it allows the management of black lists. It also stores the Protection Information of each protected object, resource and the list of actions performed on them, the so called Action Log database. Each Action Log describes an action performed on a given content/resource, by a given user, on the basis of a given license, etc. The whole set of Action Logs allows to produce the reporting and the production of statistics.

Registration Portal and Service

It is used to register users (final and business) in collaboration with the AXCS and the AXMEDIS Certification Authority. The registration portal allows collecting information about the users, regardless of the assignment of their unique ID and provides certificates. The PMS and AXCS does not have any personal and private information about the user and see them only via their unique ID.

3.1 Business to Business Scenarios

In Figure 2, the point of view of the Producers with their production tools and two related Distributors is presented. The Producer typically performs the following operations as to the above mentioned services and tools.

User Registration for business users as content producers and distributors. The registration provides them a unique ID and a certificate released by a Certificate Authority.

Tool Registration to register the tools used by the producer for producing content object packages, licenses, and to revoke licenses. In general, different users may use the same tool, so that the certificate should be managed at the User's level, whether this distinction is needed by the control and/or revocation process and tools.

User and Tool Authentication operations performed to verify if the connection is established with the right user and tool. A simplification can be performed in the case of final users if User and Tool are considered a unique element, e.g., the Device. The authentication based on the certificate allows also storing the keys to establish a protected channel for exchanging sensible information.

Object Publication, Object ID Assignment, Object Registration/Posting of Protection Information. In most cases, the producer asks for the production of protected objects to the distributor, moving the not protected objects to the latter. In this way, the producer delegates also part of the control about the exploited rights. In other business cases, the activity of content protection is performed by some intermediate producer. The scenario reported in Figure 3 is more complete and offers several advantages. The protection is directly performed by the producer who can distribute the protected objects to more distributors (even with different DRM and protection models).

License Posting. The license provided by the Producer defines the rights that he has deployed to a distributor (also called distribution or mother license). These licenses typically include the possibility of (i) object reselling according to different business models, (ii) object adaptation to make the object suitable for different distribution channels and devices, (iii) object encapsulation, (iv) object interrupt for advertising, etc. Therefore, the licenses, that the Distributor produces (to enable the rights' exploitation for the final users), depend on the licenses the Distributor bought from the Producer. Once the license is posted on the PMS (License Server), the corresponding action should be communicated to the AXCS in the form of Action Log (reporting the event).

Revoke License. This operation can be performed to terminate the contract that the Producer has with a Distributor/User. The License Server, such as the PMS Service, has to manage a black list of revoked licenses.

Revoke Object. This operation allows invalidating a specific object by including its unique ID in a black list. This action disables the distribution of the Protection Information related to that object.

Action Log and Statistics Accesses allows getting detailed reporting and statistic information about the exploitation of rights and other events. The Producer is interested and it is authorized to have the detailed information about the exploited rights for the produced objects. The detailed reporting refers to the Action Log records which were produced according to some produced objects. The Action Log record for each exploited right includes also: content owner ID, Producer ID, Distributor ID, Object ID, User ID, right, device ID, date and time, etc. Some kinds of information (such as the User ID) cannot be delivered to the Producer, in order to respect the privacy.

3.2 Business to Consumer Scenarios

Figure 3 depicts the point of view of a DRM Client and Player with respect to the distribution of content performed by two Distributors and other DRM services. In this case, the activities are performed by means of the so called DRM Client and Player that includes the device/tool which the user performs all actions from. Any User may have/use one or more devices/tools supporting interoperability. The DRM Client/player typically performs the following operations.

User Registration and Authentication to register the user on the circuit of the Distributor(s). The Distributor needs to identify the User so as to provide him with the bill or to get the payment in advance (both models are possible). The second case allows the User to maintain anonymity with respect to the distributor, yet limiting the flexibility of the business model that can be agreed among these business actors. The registration in this case leads to produce a unique ID for the User and to deliver a Certificate in order to establish protected communication and authentications.

Tool Registration and Authentication to identify the tool used by the final user and to certify that they are trusting tools. The distinction between user and tool allows managing multiple users exploiting the same device for accessing content and exploiting rights such as in archives, schools, content factories, families, etc.

Query (browse, selection), Get Object and Set Contract. The final user may go to any Distributor to make some query for selecting the content objects. In order to enjoy the content object, some rights have to be acquired by the user setting a contract with the Distributor according to some business model. In any case, according to the established contract, the Distributor has to issue a corresponding License, and to post it on the License Server (PMS). Once the license is posted, the corresponding action may be logged into the AXCS in the form of Action Log record (reporting the event).

Do Payment, Dispose Payment, Delegate Get Payment. According to the business model, the Distributor starts the process to obtain the payment from the user. This is typically performed by delegating some external Payment and Compensation Service to get the payment from the User (Delegate Get Payment). The Distributor periodically verifies the status of the payment to enable the service to its client. A similar service can be used by the Colleting Societies to dispose the revenue sharing among the value chain actors involved in the rights sold by the Distributor (Dispose Payment).

Grant Authorization, Content usage, rights' exploitation. Finally, the user who obtained the content can try to exploit its rights, for instance making play on its DRM-enforced player. This action implies to contact the PMS to establish a secure connection in order to get the Grant Authorization. Once the grant is provided, the corresponding action is communicated to the AXCS in the form of Action Log record.

4 Unique Backoffice DRM Interoperability

By using the AXMEDIS framework and tools, it is possible to set up a large set of different architectures and configurations, which allows managing at the same time and in harmonized manner several different distribution channels, while supporting also production and distribution on demand. The AXMEDIS solution allows realizing multichannel interoperable channels supporting both MPEG-21 and OMA for distributing content via satellite data broadcast towards PC and/or STB, via Internet towards IPTV and/or STBs, via mobile channel to moves, etc., as demonstrated by AXMEDIS demonstrators (www.axmedis.org).

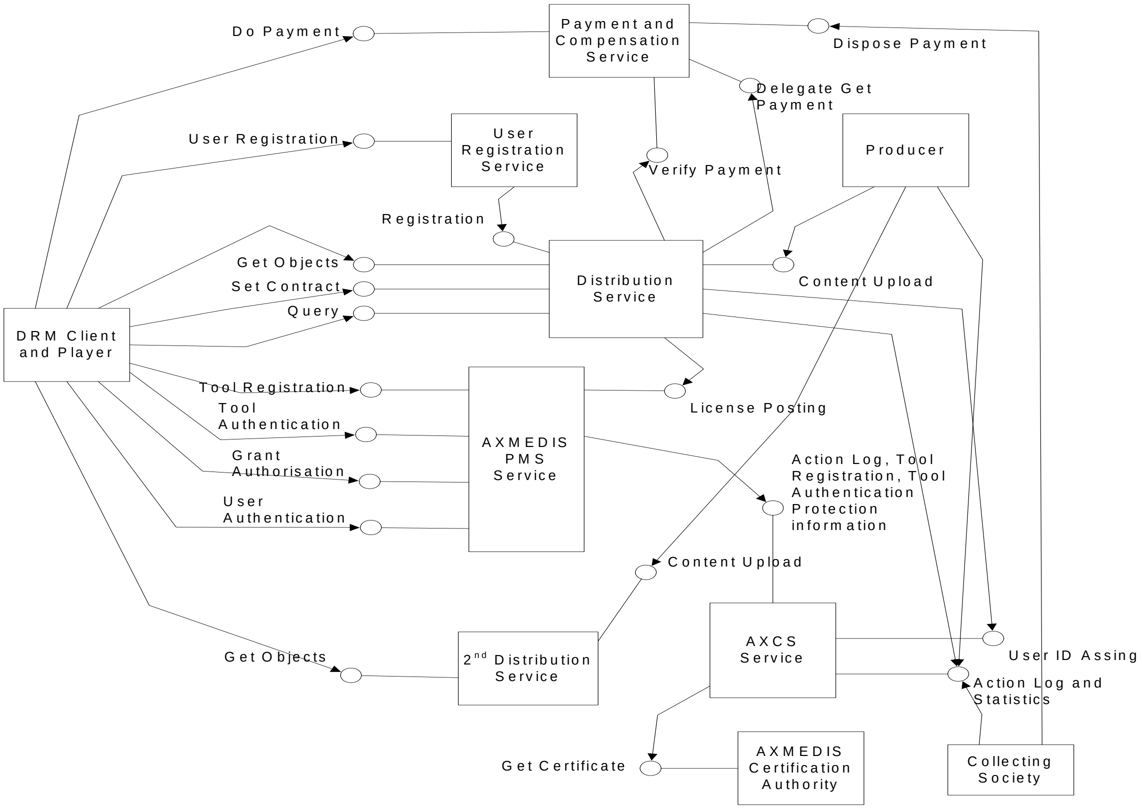

Figure 3 – Exploiting DRM Services, point of view of final user with its DRM client and player, a Business to Consumer Scenario. (please note that, for one of the distributor not all the connections have been reported).

The AXMEDIS framework allows automating the activities of production and distribution by scripting these activities and putting them in execution on the Content Processing GRID platform: the so-called AXMEDIS Content Processing. This solution allows setting up different interoperable distribution channels with a unified back-office. For example, (1) AXMEDIS/MPEG-21 content format distribution towards PC and STBs exploiting functionalities of both the AXCS and the AXMEDIS PMS; (2) OMA distribution according creating OMA packages and accessing to OMA license server according to the so called Separate Delivery; (3) a channel can be based on Microsoft Windows Media DRM, creating MS content and posting licenses on related License Server. These channels may have a unified or separate portal with services for content promotion and distribution in streaming and/or download. On the basis of the AXMEDIS back office tools and Rules [Bellini, Bruno and Nesi, 2006] specific services/adapters can be set up by intermediate business partners for transcoding content packages and/or licenses among different non interoperable channels, so as to make them interoperable (for example converting MEPG-21 REL license into OMA DRM license). The above mentioned rules may include adaptation of content, of metadata and of license. In some cases the content cannot maintain the same functionalities in all platforms and therefore some parts of the license have no sense for some devices.

5. Conclusions

This paper has presented the architecture of AXMEDIS for multichannel interoperable content production, protection and distribution. The architecture has been defined as a result of an analysis of a large set of different content models, distribution solutions and DRM architectures, and supports the harmonization of the MEPG-21 with OMA and Windows DRM. The analysis has been performed to define common bases for their interoperability and to define a unified architecture supporting different models and solutions of interoperability, thus supporting and facilitating the transition from the present status and solutions to a possible unified and standardized model.

The paper reported an overview of the AXMEDIS architecture and tools which are a solution to automate, accelerate and restructure production and protection processes. AXMEDIS architecture supports multichannel and interoperability by allowing to set up services for the migration of content from different formats (by setting up some adaptation services), among different channels and from different DRM formats [Bellini, Bruno and Nesi, 2006]. Such different channels may have their specific devices and business models and their specific DRM solutions. This paper described only a part of the whole AXMEDIS framework and architecture which is addressing many other problems and critical points. AXMEDIS solution is mainly based on MPEG-21 and OMA models and it provides and stimulates the usage and the exploitation of the developed features for creating many AXMEDIS compliant tools and solutions, while making the core aspects and solution accessible in the form of AXMEDIS Framework. The full specification of AXMEDIS tools and WSs can be accessed on the AXMEDIS portal.

6. Acknowledgements

The authors would like to thank all the AXMEDIS project partners (ANSC, AFI, EUTELSAT, Giunti ILABS, HP Italy, FHGIGD, TISCALI, XIM, ACIT, EXITECH, University of Leeds, University of Cataluña, University of Reading, BBC, TEO, ELION, TIM, SDAE, etc.), the Expert-User-Group and all affiliated members for their contributions, supports and collaborations. The authors would also like to express their thanks to the European Commission IST DG-INFSO FP6 for partially funding AXMEDIS.

7. References

1. Bellini P., Bruno I., Nesi P., ``A language and architecture for automating multimedia content production on grid", Proc. of the IEEE Int. Conf. on Multimedia & Expo (ICME 2006), IEEE Press, Toronto, Canada, 9-12 July, 2006.
2. Bellini P., Nesi P., “An architecture of Automating Production of Cross Media Content for Multi-channel Distribution”, Proc. of the first Int. Conf. on Automated Production of Cross Media Content for Multi-channel Distribution, 30 Nov - 2 Dec 2005, Florence, Italy, IEEE Computer Society press.
3. Bellini P., Nesi P., Ortimini L., Rogai D., Vallotti A., ``Model and usage of a core module for AXMEDIS/MPEG21 content manipulation tools", Proc. of the IEEE Int. Conf. on Multimedia & Expo (ICME 2006), IEEE Press, Canada, 9-12 July, 2006.
4. Iannella, R., “Open Digital Rights Language (ODRL)”, Version 1.1 W3C Note, 19 September 2002, http://www.w3.org/TR/odrl .
5. Koushanfar, F., Inki Hong, Miodrag Potkonjak, “Behavioral synthesis techniques for intellectual property protection”, ACM Trans. on Design Automation of Electronic Systems (TODAES), Vol.10, Issue 3, ACM Press, July 2005.
6. Lin, E.T., Eskicioglu, A.M., Lagendijk, R.L., Delp, E.J., “Advances in Digital Video Content Protection”, Proceedings of the IEEE, Vol.93, N.1, pp.171-183, January 2005,
7. Mourad, M., Hnaley, G.L., Sperling, B.B., Gunther, J., “Toward an Electronic Marketplace for Higher Education”, Computer of IEEE, pp.58-67, June 2005.
8. MPEG Group MPEG-21 DID, “Introducing MPEG-21 DID, Digital Item Declaration”, www.chiariglione.org/mpeg/technologies/mp21-did/
9. Wang, X., De Martini, T., Wragg, B., Paramasivam M., Barlas C., "The MPEG-21 rights expression language and rights data dictionary", IEEE Transactions on Multimedia, Vol.7, N.3, pp.408-417, 2005.