AXMEDIS: an MPEG-21 based solution for protected cross media content production and distribution

S. Chellini, T. Martini, P. Nesi
DSI-DISIT, Department of Systems and Informatics, University of Florence
Via S. Marta, 3 - 50139 Florence, Italy
nesi@dsi.unifi.it, http://www.disit.dsi.unifi.it

Abstract

The recent technologies for digital rights management, DRM, are mainly based on accounting events related to actions performed on the content by the final users like the exploitation of rights granted by means of licenses. This paper presents the solution for event reporting management related to the AXMEDIS project. The AXMEDIS is a research and development integrated project of the European Commission.

1. Introduction

In the evolving scenario of the digital content market, final users are asking to content distributors for more flexibility in exploiting the rights associated with the content acquired. The simple solutions at present provided on the market (e.g., Apple iTunes or Microsoft Windows Media) are mainly related to business models and DRM (Digital Rights Management) mechanisms that allow exploiting a number of limited rights, e.g., limiting the content usage on a specific platform or limiting flexibility in porting the content on different media (e.g. fixed number of CD/DVD burnings, of copies, etc.). In a similar way with the traditional usage of physical media (an analysis of the Traditional Rights Usage has been performed by DMP, http://www.dmpf.org/, [1]), users are becoming more and more interested in acquiring digital content they can make free use of, moving it from one device to another while at home, passing it to their children, transferring it into their mobile smart-phones or cars, collecting it in a house Media Center, etc.

To meet these needs there are several new challenges to be solved, such as flexible DRM, dynamic content adaptation, content modeling, content production on demand, content licensing, content interoperability, DRM interoperability, license processing, etc.

This paper describes the work performed in the AXMEDIS (Automating Production of Cross Media Content for Multi-channel Distribution) IST FP6 project, whose aim is to create an innovative technology framework for the automatic production, protection and distribution of digital cross-media contents over a range of different distribution channels with a flexible DRM. It means that DRM can be applied on every different distribution channel in different manners; this is possible thanks to the support offered by different distribution and protection models. AXMEDIS framework includes a large set of tools [2]. It has been designed to support the realisation of different distribution and transaction models. AXMEDIS tools are conceived to support the whole value chain, from content creation to content distribution and consumption under the support of the DRM.

This paper provides a description of the main aspects of the AXMEDIS framework related to the supported protection models and to the accounting tools provided in the AXMEDIS, while stressing the offered innovation.

2. Protection solutions in the AXMEDIS framework

The main aspects concerning the access to a protected content are the License (formal file or document which collects a list of rights that can be exploited for a given content by the user) and the Protection Information (i.e. data to get access to the protected content, for example a key to unprotect the digital resource and the algorithm type to perform the decryption).

Currently available solutions do not provide very flexible protection models. For instance, Windows Media DRM provides a model storing multimedia objects protection information inside the device hosting the tool. This information is stored on the device in an inaccessible appointed area for the so called licenses. In Windows Media DRM licenses contains both Protection Information and rules about multimedia content usage. Also Apple iTunes DRM provides a similar DRM model storing protection and licensing information along with the player.

In general Protection Information and licenses can be managed in several manners with respect to metadata and digital resources. Mainly, three different models are possible.

Open Model (see Figure 1) – the content is protected and the protection information is produced, while several different Licenses can be produced according to the business models. Protection information and licenses are kept separate.

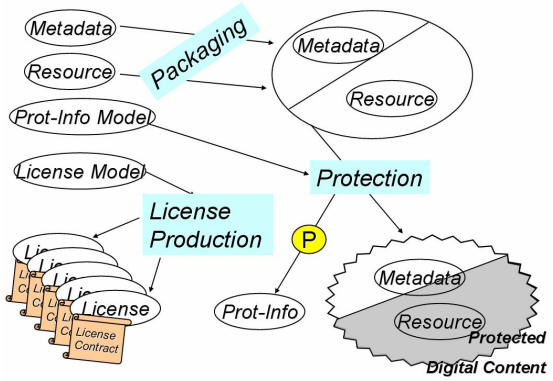

Figure 1 – The Open Model
(the copyrights of this figure is of DSI AXMEDIS)

In this way, if the Distributor has O objects to be distributed and U users as its distribution target, there may be O*U Licenses and only O Protection Information (in this example the hypothesis of only one resource for each object has been applied, while this restriction does not appear in the AXMEDIS). This model is suitable for P2P distribution since the digital Objects can be distributed freely and whenever the user is interested in opening/playing one of them, he/she has to acquire a License, being the only way to access the object Protection Information.

Governed Object Model (see Figure 2) – the Content is protected including the License inside it. In this way, each object should be produced for every specific user and it can be accessed only by the specific user it is produced for.

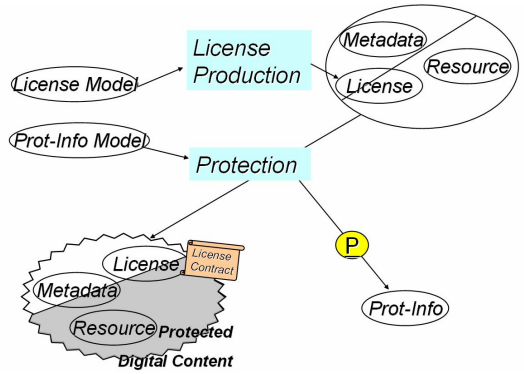

Figure 2 – The Governed Object Model
(the copyrights on this figure belongs to DSI AXMEDIS)

Therefore, if a Distributor has N objects to be distributed and U users as its distribution target, it has to produce N*U Objects and Protection Information. This solution is very expensive to be realized since the N*U Objects take much space and are expensive both at creation and management level. In this case, for managing the same number of objects in a solution using the Open Model, a space larger U times is needed. If the needed number of different objects per user is not produced, the License is not associated with the User, thus its scope being larger and less precise and allowing the Objects to be passed to other Users of the same group. This decreases the security level. This model is not suitable for P2P distribution, since the objects contain personal information about the purchaser.

Augmented License Model (see Figure 3) – the Content is protected and the Protection Information is produced, while several different Licenses can be produced according to the business models. Each License contains the Protection Information.

The Distributor produces a License for each final user or group of them. If the Distributor has O objects to be distributed and U users as distribution target, it may have O*U Licenses. This model is suitable for P2P distribution since the Objects can be distributed freely and whenever a user is interested in accessing one object, he/she has to acquire the License. This model presents more risks than the Open Model since the License contains the protection information and often the License has to be visible and accessible to the final user.

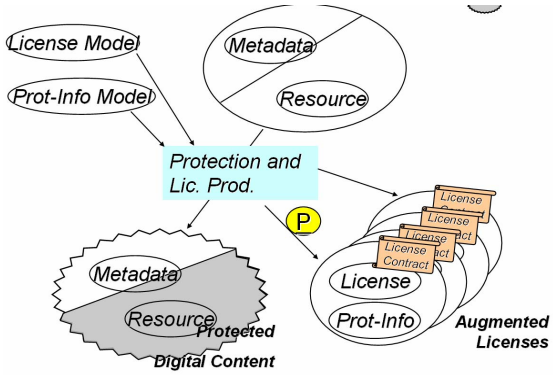

Figure 3 – The Augmented License model
(the copyrights on this figure belongs to DSI AXMEDIS)

In the AXMEDIS distributors, and more generally speaking, producers of protected objects are let free to decide to adopt the model they prefer according to their business and transaction models. The Open Model is the most flexible and allows managing independently the chain of licenses and the Protection Information.

3. Protection Architecture

The protection architecture used in the AXEMDIS system has been conceived in order to be flexible enough to support all three protection models previously reported. In the AXMEDIS, all the framework components have

been designed and realized in order to be MPEG-21 compliant, from the object model and metadata structure to log record organization.

In the content creation phase, the AXMEDIS framework provides tools supporting content editing [3] and automated production of multimedia objects based on a set of scriptable rules [4]. When a multimedia object is ready to be published, a unique identifier (called AXOID) has to be assigned and it can be protected through specific tools. When the object is protected, the protection information is generated.

Afterwards the object can be published. At this time distributors can acquire the desired object and deliver it to final users. It has to be stressed that users have to be registered in the system and tools have to be certified in order to let all phases be supported and supervised.

In the AXMEDIS architecture the AXOID is provided by a service of the AXCS (AXMEDIS Certifier and Supervisor), which has also the role of storing the protection Information. Moreover, a supervision activity over identification and certification of the involved actors is also needed to guarantee the correct exploitation of contents.

4. AXCS (AXMEDIS Certifier and Supervisor)

AXCS is the authority in charge of supervising all the activities in the system. Its own proper tasks deal with user, tool and device registration, certification and management, black lists management, identifiers generation and manipulation, object metadata and usage logs collection. It also stores the Protection Information of each protected object and resource and the list of actions performed on them, the so called Action Logs. Since AXMEDIS has to support multi-channel distribution, every single channel has to be supported by at least one or more AXCSs. All AXCSs in the AXMEDIS system are connected through a peer to peer network. In this way they can share information about AXMEDIS users, objects, licenses, protection information and so on.

4.1. AXCS support to protection

The AXMEDIS system has been conceived in order to provide a secure environment where multimedia resources can be safely distributed and consumed. Therefore it has to be able to identify all the entities involved in content exploitation without any ambiguity. AXCS provides a wide support to this aspect via registration mechanisms for users, tools and objects. Any entity is identified with an unique identifier assigned upon registration in the AXMEDIS and this piece of information is stored in appropriate certificates for users and tools.

Moreover, the system has to grant permissions only to trusted entities in order to guarantee that contents are exploited only by authorized users. To this aim, any tool has to be certified to access contents; this means that during the consumption phase user and tool credentials have to be provided to the system in order to let AXCS verify both user and tool identity and tool integrity. If these checks are passed, the PMS checks if the user has the right to perform the requested action and only then AXCS provides protection information useful to decode protected objects and consume them. For these purposes, all data about users, tools and objects are retained by AXCS.

Quite differently from what happens in other existent solutions like Windows Media DRM, in the AXMEDIS neither protection information nor licenses are usually stored inside tools, but a more complex and distributed model is used. As stated above, protection information are stored in AXCS, while licenses are stored in License Server called PMS (Protection Manager Support) or in the object itself, depending on the protection model chosen. In this way, there is a physical and logical separation between protection information and license. Objects can be distributed freely with no risk of deceitful usages, because protection information are retained by AXCS and provided only to certified users and tools.

4.2. AXCS support to accounting

The object usage accounting activity is a fundamental asset in the AXMEDIS system. Distributors, creators, integrators, collecting societies are interested in knowing which are the operations performed over their pertinent objects, in order to produce accounting and/or verify they received the correct fee from object usage according to the business models. In addition, this activity is also very relevant to provide statistical data and to guarantee that the usage respects the provided licenses. This is a vital activity if we want to guarantee that owner rights are respected. Moreover, collection of data concerning content consumption can be used to support AXCS supervision activity, thus allowing the creation of black lists of users, tools, objects and so on.

All the accounting needed information is collected and stored by AXCS in the form of Action Logs. Each Action Log registers an action carried out on a given content/ resource by a given user, on the basis of a given license, etc. An Action Log is automatically generated every time the system grants to someone the authorization to perform an action over an object. In fact, every single action performed is subject to an authorization request. Whether the device is connected to the system, the usage authorization is directly provided by the system itself. If not, the license for the requested object and for the user is temporarily cached locally by the tool (in a way that it cannot be accessed from the outside) and for each action performed the needed data are stored; in this way, as soon as the tool gets back on-line, these data can be communicated to the AXCS. The producer of the license

can either allow or not the caching of the license on the terminal. On such grounds, AXCS tracks the actions performed in both on-line and off-line object consumption scenarios.

The whole set of Action Logs allows the production of reporting to distributors, to content providers, to collecting societies and so on, through a specific tool called Reporting Web Service provided by AXCS. In a similar way, AXCS provides a tool called Statistics Web Service designed to obtain anonymous data on content consumption, i.e. usage data without any reference to users.

Action Log mechanism allows also the creation of black lists, used to identify users to be blocked (if in any way they performed unauthorized actions) and/or object copies to be licensed no more (for instance, because the protection algorithm has been cracked).

4.2.1. AXMEDIS Action Log and MPEG-21 Event report

Since AXMEDIS has been designed to be MPEG-21 compliant, also AXMEDIS Action Log is based on the MPEG-21 Event Report, but at the same time it is somewhat different since it implements only a part of the standard. The main difference between ER (Event Report) and AL (Action Log) lies in the fact that ERs are always issued as a consequence of ER Requests, being the request included directly inside a digital item or taken by an application. Instead, AXMEDIS Action Logs are always generated without the need of a generation request. In fact, every action performed has either to be authorized by the system (on-line object consumption) or it generates data (which later are automatically sent to AXCS) needed to create the corresponding Action Log (off-line object consumption). In any case, there are no specific requests: the generation mechanism is completely automatic.

In the AXMEDIS it is not possible for users to perform actions over objects in mistrusted systems or with no AL generation. Actions can be performed only through a certified tool (thus granting that they do not manipulate illegally objects) and only after checking the integrity of both the tool and the device and the authorization of the user (even in the off-line consumption scenario, these checks have to be done before a license can be cached locally by the tool). So, actions are performed only in trusted environments and they always produce Action Logs. On the other hand, Event Reports can be generated also for mistrusted systems; moreover, in MPEG-21 general scenarios, it is also possible for users to perform actions without generating Event Reports under some conditions [5], even in a mistrusted system.

Action Log and Event Report schemas are quite different too. At present, there is not a strictly correspondence between each element in MPEG-21 Event Report and AXMEDIS Action Log. This is due to MPEG-21 not being completely standardized, while AXMEDIS Action Log has been already designed and implemented in order to be temporally lined-up with other framework modules.

5. Conclusions

This paper has presented mainly the protection solutions adopted in the AXMEDIS and described as three different paradigms providing a very flexible DRM model. It has also illustrated the AXCS component, explaining its role in protection and accounting supervising activity. Finally, it has reported a short comparison between AXMEDIS Action Log and MPEG-21 Event Report in order to make evidence of the differences and the similarities.

6. Acknowledgements

The authors would like to thank all the AXMEDIS project partners (ANSC, AFI, EUTELSAT, Giunti ILABS, HP Italy, FHGIGD, DIPITA, CRS4, TISCALI, XIM, ACIT, FUPF, CPR, EXITECH, Univ. of Leeds, etc.), the Expert-User-Group and all the affiliated members for their contribution, support and collaboration. The authors would also like to thank the EC IST FP6 for funding partially the AXMEDIS project.

7. References

[1]. AXMEDIS, *Comparing AXMEDIS, MPEG21 and DMP*, accessible at www.chiarigllione.org and on www.axmedis.org

[2]. AXMEDIS Use Cases, Official Deliverable of AXMEDIS project: www.axmedis.org.

[3]. P. Bellini, P. Nesi, D. Rogai, A. Vallotti, *AXMEDIS Tool Core for MPEG-21 Authoring/Playing*, Proc. of International Conference on Automated Production of Cross Media Content for Multi-channel Distribution, 30 November - 2 December 2005, Florence, Italy.

[4]. P. Bellini, I. Bruno, P. Nesi, *A Distributed Environment for Automatic Multimedia Content Production based on GRID*, Proc. of International Conference on Automated Production of Cross Media Content for Multi-channel Distribution, 30 November - 2 December 2005, Florence, Italy.

[5]. ISO/IEC JTC1/SC29/WG11, MPEG2005/M12299, *Core Experiment on use of Event Report Requests: Specification of Use Cases*, July 2005, Poznan, Poland