A Mobile Scenario for Electronic Publishing based on the MIPAMS Architecture[1]

Jaime Delgado, Silvia Llorente, Eva Rodríguez *and* **Víctor Torres-Padrosa**

Departament d'Arquitectura de Computadors, Universitat Politècnica de Catalunya, C/Jordi Girona, 1-3, 08034 Barcelona, Spain. Email: {jaime.delgado, silviall, evar, vtorres}@ac.upc.edu

Abstract: *This paper describes several scenarios for the management of digital media, focusing on electronic publishing from mobile environments. The solution proposed in those scenarios is based on MIPAMS (Multimedia Information Protection And Management System), a service-oriented Digital Rights Management (DRM) platform, which enables the creation, registration and distribution of multimedia content in a secure way, respecting intellectual property rights. The particularity of the mobile scenario with respect to others is the limited capability of mobile devices. A specific use case has been identified for the mobile environment and a new system, based on MIPAMS, has been designed for the electronic publishing environment.*

Keywords: *Content management; mobile environments; digital rights management.*

Introduction

This paper proposes a solution for the management of digital media in mobile environments. This solution is based on MIPAMS (Multimedia Information Protection And Management System) (Delgado, 2011), a service-oriented digital rights management (DRM) platform developed by the authors, which enables the creation, registration and distribution of multimedia content in a secure way, respecting the intellectual property rights. The proposed solution has been designed for mobile devices, which have limited capabilities, and applied to an electronic publishing scenario.

The paper is organized as follows: First, a set of content management scenarios is presented. In all of them DRM architectures facilitate the development of alternative applications. They include DRM-enabled content access control, content licensing and intellectual property registry with external licensing. Then, the MIPAMS architecture is presented. The MIPAMS section provides insights into the modules and services of the MIPAMS architecture that provide functionalities for the governance and protection of multimedia content. In order to illustrate the operation of this architecture, we present the results of some research and development projects in which the content management scenarios, previously described, have been implemented. Finally, a scenario for electronic publishing using mobile devices is presented. In this scenario the MIPAMS architecture is used for the registration and governance of digital information produced with smartphones.

Content Management Scenarios

Most of the literature refers to DRM as a means to restrict what users can do with content but in fact, DRM can be used in other contexts. For example, our research focuses on the "management" part; i.e., protection is not always necessary (for example in a trusted, or partly trusted, environment), but mechanisms to manage intellectual property are needed. We have identified several scenarios where DRM architectures enable the development of various kinds of applications on top of them, as detailed next.

DRM-enabled content access control. This scenario covers content registration, protection, search, licensing, authorization-based content access control, content storage and reporting. In this case, there is a need for an interface so that content creators can register and publish their content and determine and modify their offers. This functionality is provided by means of specific edition user

[1] This work has been partially supported by the Spanish Government through the project MCM-LC (TEC 2008-06692-C02-01).

applications or otherwise integrated in a web portal. Once content is registered, it can be linked from external sites so as to be able to license it through the mentioned portal, which means that the content promoted in external sites can include specific links towards the licensing portal. Moreover, apart from being linked from other sites, the portal itself would also be useful for promotion. In this business scenario, content is accessed by using DRM-adapted tools such as players and other rendering applications.

This scenario is illustrated in the following example. A news agency wants a solution for publishing, trading and distributing protected news. Content trade needs to support different licensing options, such as prices, time frames, territory, etc. Content access needs to be protected, controlled and reported. The news agency can make use of specific external services and a customized publishing and trading portal. Content access will be done through a DRM-enabled application.

Content Licensing. This scenario involves content registration, search, licensing and reporting. It is applicable to those cases where there are well established sites that deal with the promotion and collection of content, but for which licensing is not a part of their business model (e.g. Flickr, Picasa, Panoramio, YouTube, etc.). Although content can be directly accessed from those sites, it may be distributed under some restrictions that do not enable users to use it for free. This is the case when content is distributed, e.g., under copyright ("all rights reserved") or Creative Commons Non-Commercial models. In this scenario, there is a need for a trading portal, devised for formalizing the rights acquisition for personal or professional use. Content owners or rights holders are responsible for registering content in the trading portal and providing the link towards it. Content can be linked from external sites.

The following example describes the above scenario. A web portal dealing with specialized content (e.g., valuable medical images) wants to offer users the possibility to trade their content. The web portal defines some license templates that users can select when uploading their images. Content is automatically registered through external services and a link is provided from each image towards the trading portal for those users interested in licensing them for, e.g., publishing. Access to the images is managed by the web portal.

Content licensing and authorization-based content access control. This scenario involves content registration, search, licensing, authorization-based content access control, content storage (optional) and reporting.

When dealing with content storage, this scenario is useful for applications where users need to handle or modify content without restriction or when users do not want to be limited to using some specific DRM-enabled application. Although access to content is authorization-based, content is given unprotected to the purchasing users so that they can enjoy it without further DRM restrictions.

The next example describes the above scenario. A content distributor wants a solution for trading and distributing unprotected audiovisual content. Content trade needs to support different licensing options, such as prices, time frames, territory, etc. Content needs to be delivered unprotected, since it is to be transformed by its recipient to adapt it to different online and offline publishing formats. However, the content distributor wants to be sure that only those clients who own a license can download content. That is, content access needs to be controlled and reported. The content distributor can make use of specific external services and a trading portal. Content licensing and access can be done directly from the portal, after checking user licenses.

When content storage is not used, this scenario is devised for content providers or distributors who want to use their specific protection mechanisms and content management systems so that content is never stored outside their well-established systems. In such a scenario, when registering content, specific proprietary identifiers are used for identifying external content. Once objects are registered, rights offers can be published and licenses issued without restriction. Regarding the applications that access content, such as players and editors, content providers or distributors will have to design their own applications to manage the access to encryption keys and content from their systems or otherwise provide an API so that their content can be accessed from third-party applications.

Here is an example that illustrates the above scenario. A TV broadcaster wants to license his/her own productions. The TV broadcaster may make use of specific external services to register the content and define different licensing options (offers). However, content will never be stored outside his system. The TV broadcaster may develop his/her own trading portal that interacts with specific

services to consult the available offers and formalize the acquisition of an offer by issuing a license. Specific services can be used to check whether a customer has an appropriate license and enable content download (authorization-based content access control).

DRM-enabled content access for mobile devices. This scenario involves content registration, protection, search, licensing, authorization-based content access control, content storage and reporting. It is devised for limited capability devices. In some cases, the encryption strength being used should be limited so as not to be detrimental to the device's performance. In such cases, if content is already registered and protected, content has to be re-encrypted to deal with device limitations.

The following example illustrates the above scenario. A content distributor who is already using specific external services for trading and distributing protected content wants that content to be available for mobile devices. Since the device's decryption capabilities are limited, content may not use the same encryption strength as for PC-devised content or may be adapted to fulfill the device's requirements.

Intellectual property registry with external licensing. This scenario involves content registration, search and reporting. It is based on the use of registration functionalities, leaving content licensing to be tackled by professional external sites or services. In this scenario, there is only need for an intellectual property registry, proving content ownership and offering the possibility to link content to external sites that deal with its commercialization, as in, e.g., YouLicense, Getty Images, etc.

The next example describes this scenario. A web portal dealing with specialized content (e.g., valuable breaking news images) wants to offer users a powerful means for proving authorship. The web portal integrates external services into its registration process and automatically registers user content. A digitally signed document is available in the portal to certify authorship. The web portal may reach further agreements with specialized portals for offering licensing solutions to users.

The MIPAMS Architecture

MIPAMS (Multimedia Information Protection And Management System) is a service-oriented content management platform, developed by the DMAG (Distributed Multimedia Applications Group) (DMAG, 2011). It is mainly intended for applications where management of rights is needed.

The MIPAMS architecture is based on the flexible web services approach, as it consists of several modules and services which provide a subset of the whole system functionality needed for governing and protecting multimedia content. One of the advantages of having service-oriented DRM functionality is the possibility of decoupling it into different subsystems depending on the needs of the application that is going to be implemented, while being able to share the same common services between different applications with different requirements, thus reducing costs. MIPAMS encompasses an important part of the content value chain, from content creation and distribution to its consumption by end users.

Figure 1 depicts the MIPAMS architecture, for which we now provide a general overview of its components and the different services being offered.

The Content Service (CS) enables applications to upload and download digital resources such as audio or video files, text documents, etc. Those resources can be optionally encrypted on request, according to the available encryption mechanisms it provides. If encryption is selected, the protection keys will first be requested from the Protection Service and then registered through the same service, once encryption is performed. Content upload requires content to be uniquely identified. Since MIPAMS deals with single resource objects, the identifier associated to content will be the same one used for the object that contains it, and must be used as input argument. This identifier can be requested from the Object Registration Service prior to the content upload, or obtained from an external application using MIPAMS (depending on the scenario).

The Object Registration Service (ORS) enables applications to request a digital representation of content and metadata (i.e., digital objects) to be generated and registered in the system. Content and metadata are packaged together following the MPEG-21 Digital Item (ISO/IEC, 2005) approach. Once registered, objects are digitally signed by the ORS so that they can be checked for authenticity and

integrity. The ORS also provides unique identifiers for those applications that need to upload content to the CS, as already explained.

The License Service (LS) deals with rights offers and the issuance of licenses. Rights offers are set up by content creators or rights holders after registering content. They include the rights being offered for acquisition by other users and the conditions applicable to those rights. License issuance refers to the process by which a license is generated as the result of a rights purchase, acquisition or the direct grant by a rights holder to a user of a set of rights. Licenses are expressed using MPEG-21 Rights Expression Language (ISO/IEC, 2004).

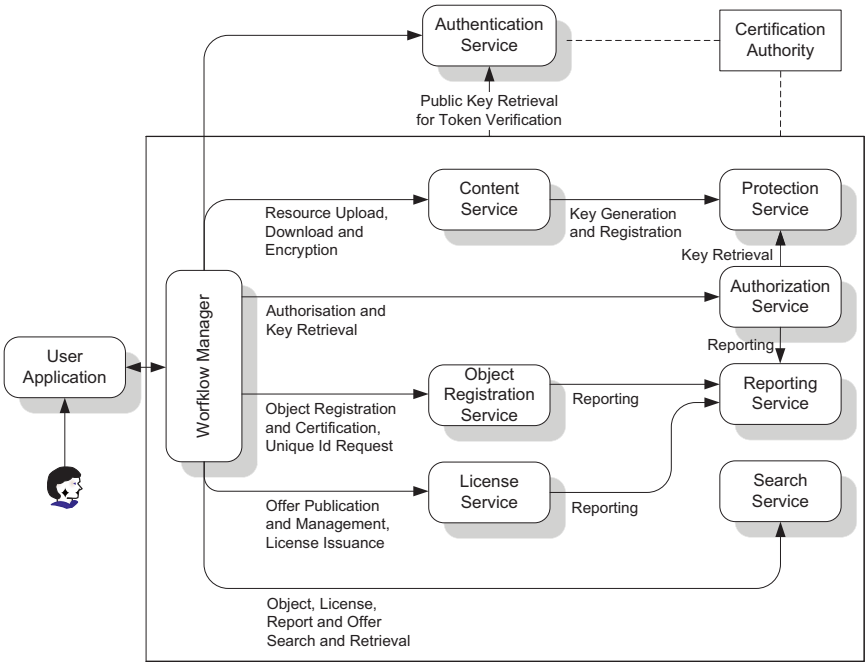

Figure 1. MIPAMS architecture

The Authorization Service (AS) checks whether a user owns any appropriate license that grants him the right to perform a requested action (e.g., play) on a digital object. The authorization is based on the mechanism defined in (ISO/IEC, 2004). The AS shares the access to the license repository with the LS. If the user is able to perform the action and the requested content is encrypted, the AS will retrieve the encryption keys from the Protection Service and return them to the requesting application. This is the only means for accessing encryption keys, which is performed as an atomic operation.

The Protection Service (PS), as introduced before, generates encryption keys upon request, registers encryption keys associated to uniquely identified content and provides the encryption keys for protected content to the AS. When using MPEG-21 Intellectual Property Management and Protection (ISO/IEC, 2006-1) scheme and descriptors, the PS also offers the possibility to download the protection tools being used by those applications that might be out-of-date.

The User Application (UA) is the player, edition tool, browser or any other means managed by the user to deal with the DRM functionality, such as registering and accessing protected contents. The UA may have an internal trusted module or intermediary to enforce DRM, which could consist of a secure local repository for licenses, protection information, offline operation reports and other critical data. It may be responsible for estimating tool fingerprints, require offline authorizations, unprotect content, track offline operations and manage content protection information.

The Workflow Manager (WM) may be an integral part of the UA or otherwise be located in the server part (e.g., web portal, brokerage service) to reduce the UA complexity. It can be seen as a broker whom the UA requests to perform different operations, such as object registration, content upload, rights offer management, license acquisition, authorization, etc.

The Search Service (SS) enables applications to perform accurate searches amongst metadata in the MIPAMS system. That is, it is the front-end for requesting any information present in MIPAMS

services databases. Thus, it can be used for searching content, licenses, offers or reports or a combination of them.

The Reporting Service (RS) collects usage reports regarding the registration of objects, the issuance of licenses and the authorizations being performed. It is also capable of building standards-based representations of those reports, such as MPEG-21 Event Reports (ISO/IEC, 2006-2). Those reports may be used for computing statistics as well as for billing or tracking purposes.

The Authentication Service (ATS) is needed to authenticate the identity of users. It generates SAML (Security Assertion Markup Language)-based tokens (OASIS, 2005) that identify MIPAMS users. Any service in the MIPAMS architecture will require a token argument to be provided in order to authenticate users. Tokens are digitally signed by the ATS, so that they can be checked for authenticity and integrity by the receiving service. Moreover, the ATS deals with user registration and management (i.e., personal data modification, user account deactivation, etc.).

Finally, there is a need for having a recognized Certification Authority (CA), which issues credentials for the different Components and Actors in the system, such as X.509 certificates and private keys for the different architectural components.

Implementation of Content Management Scenarios with MIPAMS

In this section we present the results of some research and development projects where we have implemented the usage scenarios previously identified as using MIPAMS services and modules.

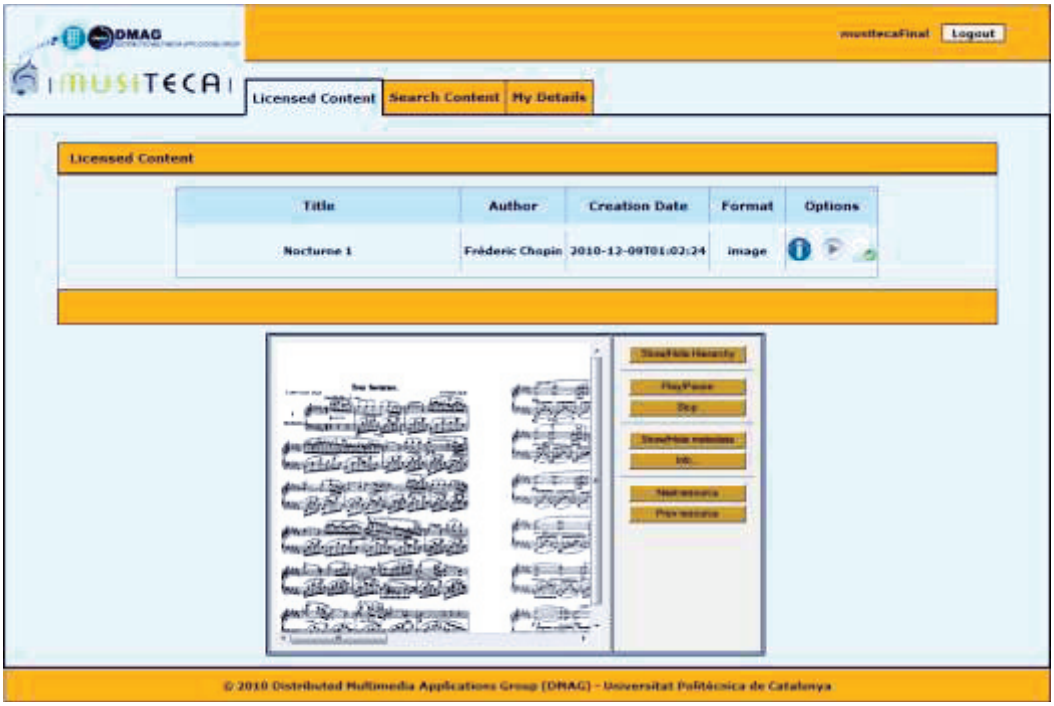

Figure 2. Protected rendering in a specific DRM portal in Musiteca

DRM-enabled content access control

This scenario has been implemented in Musiteca (Musiteca, 2008), a research project funded by the Spanish Administration. In this project, we have used some of the services making up MIPAMS (LS, RS, ATS, CS, ORS, SS and CA) to implement an electronic content publishing and trading platform. Access to the Musiteca repository is through a web portal that enables the registration of content, the definition of different licensing options (offers), the purchase of content (licensing) and access to the content purchased after checking whether the user is authorized. Content access is through a DRM-enabled application, while any action in the system is registered through the RS. Figure 2 shows a screenshot of the portal, where content is being rendered.

Content Licensing

This scenario has been also implemented in Musiteca. Figure 3 shows how content is linked from an external site, the Musiteca base on Freebase, which holds information about musical content in the Musiteca project, to a specific trading portal where content can be licensed and accessed.

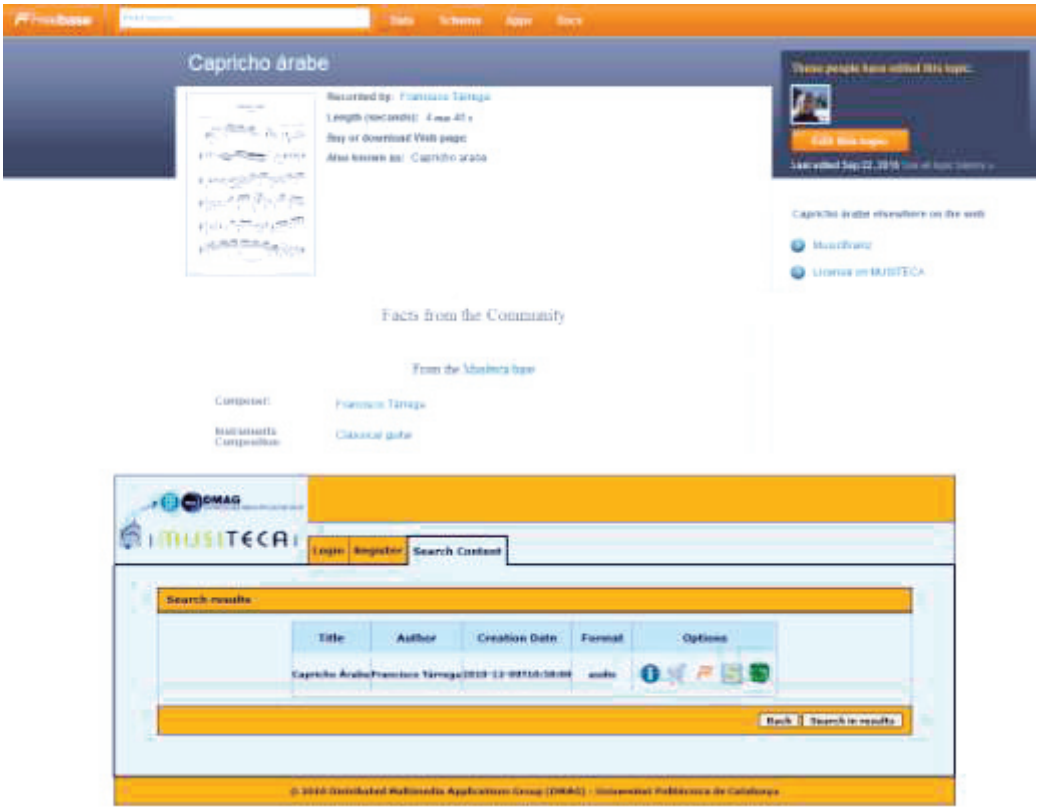

Figure 3. Licensing link from Freebase to a specific trading portal in Musiteca

Content licensing and authorization-based content access control

This scenario has been implemented in the Intellectual Property Operations System (IPOS) (IPOS, 2011), a content lifecycle management system resulting from several software developments carried out by the DMAG under different contracts with NetPortedItems (NetPortedItems, 2010), a Spanish SME company. IPOS provides content authors with the possibility of registering, publishing their work and defining how other users can license the work for deriving new content. This information is described using LS licenses, where we have added a special condition called Rights over Derivatives (ROD) (Torres, 2009). This condition indicates the percentage of the income that someone gets from a derivative work which will be owed to the original author. When an author creates derived content from an existing work and gets any revenue from it, IPOS follows the chain of work back, calculates the share for each author from the ROD condition in the licenses and creates a report for each author informing him of this fact. Reports can be consulted at established time periods to give each author the corresponding revenues. This system makes use of all MIPAMS services through a dedicated portal. Figure 4 shows a sample screenshot of the authorization-based rendering application.

This scenario has also been implemented in CulturaLive (CulturaLive, 2009), a research project funded by the Catalan Administration. In this project we have integrated, using Web Services, MIPAMS LS, AS and RS into an existing system offered by another project partner (VSN, 2011) that provides audiovisual content to be broadcast live through Digital Terrestrial Television (DTT) by televisions participating in the project. With our modules, content purchases can be tracked since we register each license acquisition and authorization result (positive or negative) into a reporting database. This database can later be consulted for billing purposes. It is worth noting that digital content to be broadcast is not managed by MIPAMS but directly by the different TV channels and

SMEs in the project consortium. This gives an idea of the integration capabilities of the MIPAMS platform.

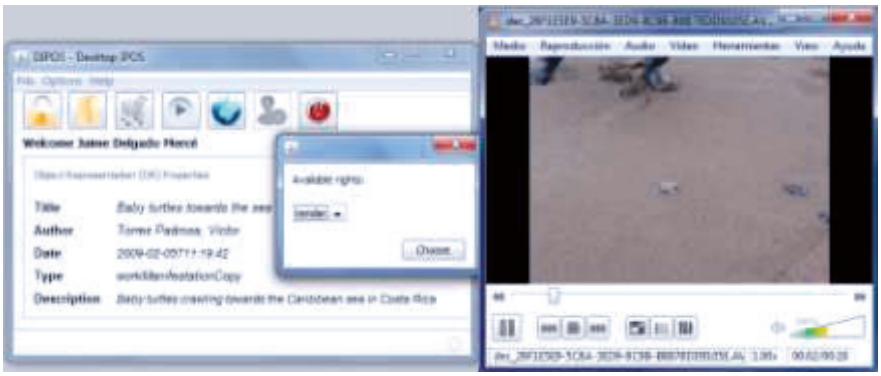

Figure 4. Content access and unprotected rendering in IPOS

DRM-enabled content access for mobile devices

This scenario has been implemented in some projects of our research group (e.g. AXMEDIS (AXMEDIS, 2004), but also in other projects) in a slightly different way. In such projects, the modules involved in the authorization of user actions were located inside the mobile device. In this way, when the user wanted to consume some content, the license for authorizing this action was inside the mobile. This was done to avoid calling external services, as it involved a phone call or data transaction that might involve a non-negligible cost for the user. Moreover, mobile devices used a specific licensing schema (OMA DRM, 2010) addressed to devices with limited processing and communication capabilities. Currently, since smartphones and high capacity mobile devices are gaining relevance and current telecommunications companies are adopting competitive pricing policies for mobile users (e.g., flat data fees), the solutions being implemented might be reconsidered.

To implement this scenario with MIPAMS, if content is already registered and protected using a protection mechanism not compatible with the device, the intermediary would be responsible for decrypting content and re-encrypting it to deal with the device limitations. Otherwise, if content is only to be used by limited capability devices, it should be encrypted using the suitable protection mechanism when uploaded to the CS.

Intellectual property registry with external licensing

Figure 3 (the lower part) shows how content could be linked from the MIPAMS-based intellectual property electronic registry developed in the Musiteca project towards external specialized licensing portals. Some examples (not used in this project) are YouLicense (YouLicense, 2011) or Getty Images (Getty Images, 2011). Content would be registered and accessible to search, while the shopping cart icon would redirect the user to a specialized and external licensing service.

Scenarios where Mobile Devices are needed

Among the different scenarios presented in the previous section, there is one specifically for limited capability devices. Inside this category of devices we include smartphones and other similar devices with internet connection that usually have an integrated camera. The difference between those devices and personal computers is mainly their dimensions (smaller), their processing capabilities (lower) and, maybe the most important, that they do not have a qwerty keyboard or mouse to interact with the user, but a touch screen or a keypad.

In this case, if we want to register new content for publishing it electronically, using one of these devices could be a laborious and slow process. Nevertheless, it could be interesting in some specific cases that we are going to describe in this section. We will make use of the MIPAMS architecture to offer these services for smart devices.

First of all, the user application has to be prepared for use in those devices. For the case where the application is a web portal, there is not much problem, as current devices have integrated browsers

which are able to manage web forms and show web pages. The only restriction in some cases is the screen size, but this can be avoided with a suitable design.

There is a scenario where mobile devices can be useful for electronic publishing, although the quality of the recorded images or videos is obviously lower than those produced with professional devices. In this scenario, what is most important is the "opportunity" of the content in the image or the video, that is, to be at the right place at the right moment, independently of the content quality. This is especially true for sudden events, for example a building collapse, a natural disaster or some celebrity being caught in an embarrassing or funny situation. In such cases, the images may even have economic relevance, as they could be published in online newspapers or in the gossip news. Therefore, the author may register the content for different purposes: to try to get some revenue or just for later attribution.

MIPAMS modules involved in this scenario and their interaction are depicted in Figures 5 and 6. Figure 5 shows the registration of the content, image or video in the registration portal. Figure 6 shows how the author can create some offers of the content to get revenue. If the author only wants to be able to prove authorship, registering the content would be sufficient. In this case a Creative Commons attribution license would be suitable as long as the author waives his right to any potential future revenues (Creative Commons, 2011).

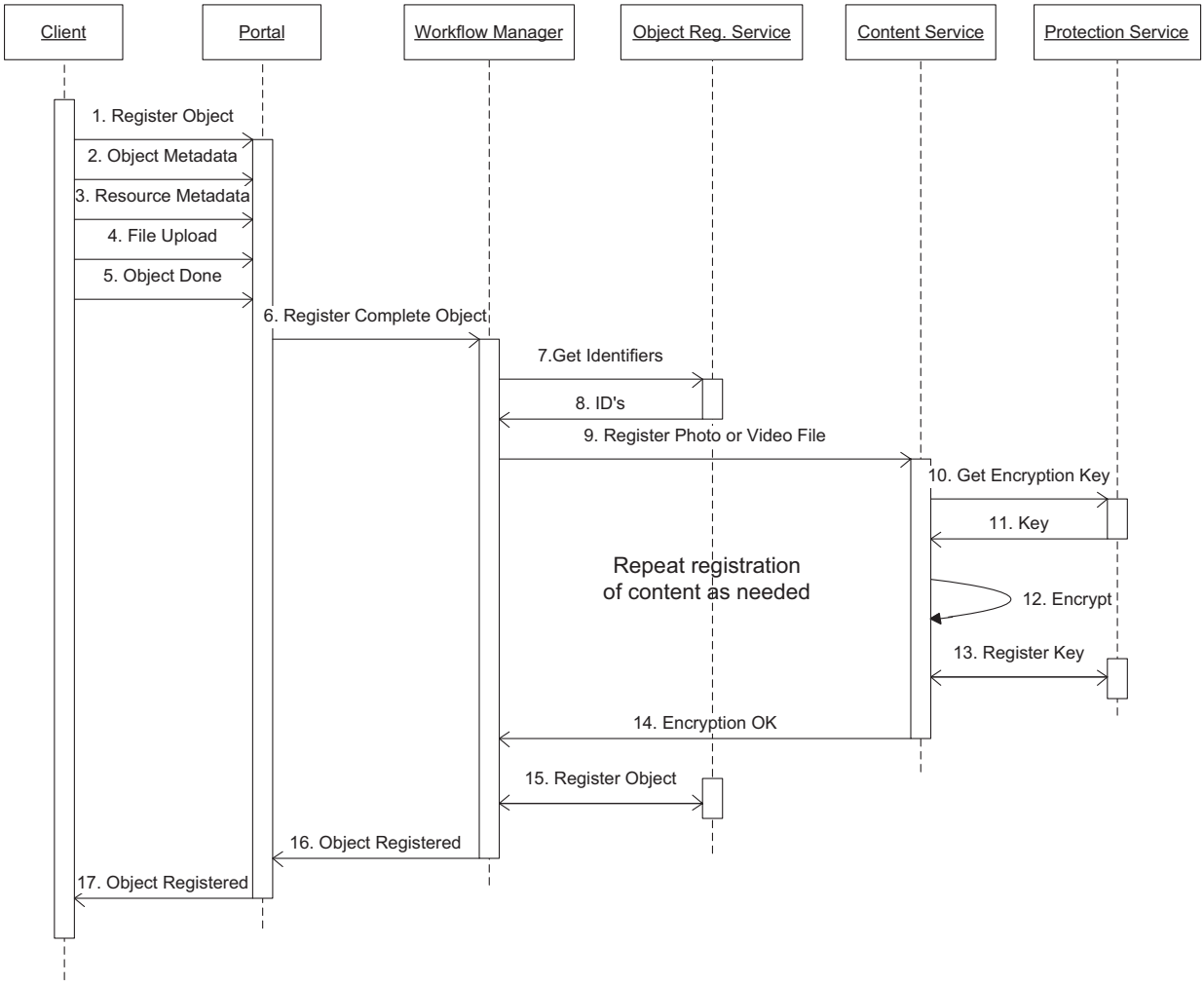

Figure 5. Registration of photo or video

The steps involved in content registration shown in Figure 5 are the following:

1. User starts registration of content in the portal by means of the client application. The client application can be a browser or a specific application for mobile devices, where some information could be predefined to facilitate the registration.
2. User fills out a form with all metadata associated to the complete digital object.
3. User fills out several forms (one for each image or video, that is, each resource) with metadata associated with each resource.
4. User uploads the file containing each resource.
5. User indicates that all object information has been inserted and the registration process needs to continue.
6. The portal sends all information to the Workflow Manager (WM) module, which will call the corresponding service for storing the object.
7. WM requests identifiers from the Object Registration Service (ORS).
8. ORS sends the identifiers requested to the WM, one for the object and one for each resource file (even if they have not yet been uploaded).
9. WM sends resource to the Content Service (CS)
10. If user has requested encryption of the resource, CS asks for encryption keys from the Protection Service (PS).
11. PS returns the keys for encryption algorithm and key length specified by CS.
12. CS encrypts and stores the file with the given key.
13. CS registers the encryption key in the PS for permitting later decryption.
14. CS sends WM notification of correct content storage and encryption. Steps 9 to 14 are repeated for each resource uploaded by the user. If no resources are uploaded, these steps can be done later.
15. When all resources are properly uploaded and encrypted, WM requests from ORS registration of the complete object, which is digitally signed to guarantee digital object integrity. The format used for storing the object is the MPEG-21 Digital Item.
16. WM sends notification of object registration to the portal.
17. Portal informs the user that the object has been properly registered.

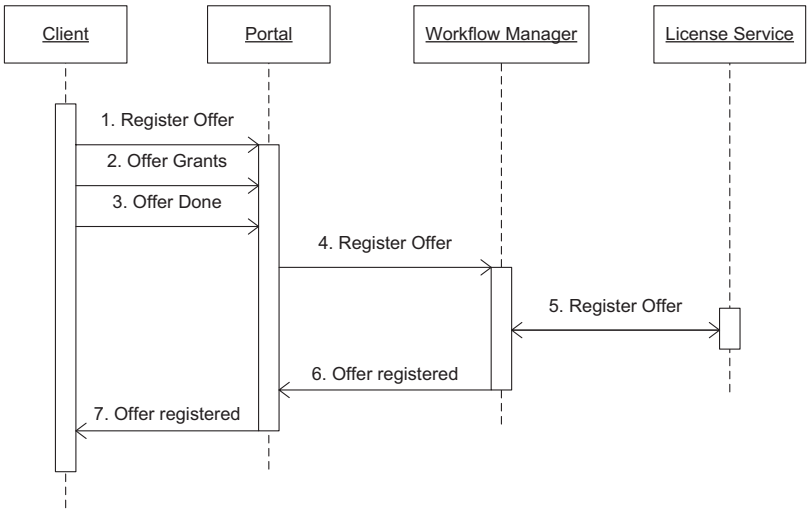

Figure 6. Creating some offers to get revenues

After object has been registered, the user can create some offers to profit from the images or videos she has registered. The steps involved in offers creation shown in Figure 6 are the following:

1. User asks Portal for offer registration.
2. User has to insert the different sales conditions offered for the registered object. These conditions include what can be done with the content (play, print, etc.) together with conditions such as territory, number of times one can perform the action or terms of payment.
3. User indicates to the Portal that the offer is complete.
4. Portal sends the offer to the WM.
5. WM sends offer information to the License Service (LS) which checks whether everything is correct and stores the offer.
6. WM informs the portal of offer registration.
7. Portal informs the user of offer registration. From that moment on, the registered content can be sold with the purchase conditions indicated by the user. It is possible to create an offer saying that the digital content is free, just to guarantee author's attribution.

Once registered, other users are able to purchase the object. At that moment, a license is created based on the selected offer. This part of the scenario corresponds to the *Content licensing and authorization-based content access control with content management and without protection* business model already described in the scenarios section, since content needs to be further processed prior to being published.

Conclusions

Mobile devices may become crucial when they are the only available means for recording information (e.g., taking a photo or recording a video) of an unexpected event of any type.

In this context, we have presented the MIPAMS architecture, developed by DMAG, devised for the management and secure distribution of multimedia content. The operation of MIPAMS architecture has been presented by means of the results of research and development projects in which different content management scenarios have been implemented.

We have illustrated different scenarios where MIPAMS has proved to be useful for copyright preservation and electronic publishing, some of them beyond traditional DRM applications.

Finally, we have focused on limited capability devices, including a detailed description of how MIPAMS registration, licensing, trading and authorization-based access control functionalities may help to protect the author's copyright, ensuring attribution and easing the exploitation of his economic rights. A detailed analysis of the interaction between different components of the architecture has been also provided.

References

AXMEDIS (IST-2004-511299). (2004-2008). Automating Production of Cross Media Content for Multichannel Distribution. Retrieved May 2, 2011 from http://www.axmedis.org.

Creative Commons licenses. (2011). Retrieved May 2, 2011 from http://creativecommons.org/licenses/.

CulturaLive Research Project (2009REGIÓ 00024). (2009). Generalitat de Catalunya.

Delgado, J., Torres, V., Llorente, S. & Rodríguez, E. (2011). Rights management in architectures for distributed multimedia content applications. *Trustworthy Internet*. Heidelberg: Springer. Publication pending.

Distributed Multimedia Applications Group (DMAG). (2011). Retrieved May 2, 2011 from http://dmag.ac.upc.edu

Getty Images. (2011). Retrieved May 2, 2011from http://www.gettyimages.com/.

Intellectual Property Operations System (IPOS). (2011). Retrieved May 2, 2011 from http://dmag1.ac.upc.edu/IPOS

ISO/IEC. (2005). ISO/IEC IS 21000:2 – Part 2: Digital Item Declaration.

ISO/IEC. (2004). ISO/IEC IS 21000:5 – Part 5: Rights Expression Language.

ISO/IEC. (2006-1). ISO/IEC IS 21000:4 – Part 4: Intellectual Property Management and Protection Components.

ISO/IEC. (2006-2). ISO/IEC IS 21000:15 – Part 15: Event Reporting.

Musiteca Research Project (TSI-020501-2008-117). (2008). Ministerio de Industria, Turismo y Comercio (Subprograma Avanza I+D). Retrieved May 2, 2011 from http://musiteca.freebase.com/.

NetPortedItems S.L. (2010). Retrieved May 2, 2011 from http://www.digitalmediavalues.com/.

OASIS. (2005). Security Assertion Markup Language (SAML). Retrieved May 2, 2011 from http://saml.xml.org/

OMA DRM: Open Mobile Alliance Digital Rights Management. (2010). Retrieved May 2, 2011 from http://www.openmobilealliance.org/technical/release_program/drm_v2_1.aspx.

Torres, V., Delgado, J., Maroñas, X., Llorente, S., & Gauvin, M. (2009). A web-based rights management system for developing trusted value networks. In *Proceedings of the 18th International World Wide Web Conference Developer's Track, April 20-24, 2009, Madrid, Spain* (pp. 57-59). New York: ACM. Retrieved May 2, 2011 http://upcommons.upc.edu/e-prints/bitstream/2117/7776/1/www09dev_proceedings.pdf.

Video Stream Networks (VSN). (2011). Retrieved May 2, 2011 from http://www.vsn-tv.com/es.

YouLicense. (2011). Retrieved May 2, 2011 from http://www.youlicense.com/.