Rights and Trust in Multimedia Information Management

Jaime Delgado, Víctor Torres, Silvia Llorente, and Eva Rodríguez

Universitat Pompeu Fabra, Passeig de Circumval·lació, 8, 08003 Barcelona, Spain
{jaime.delgado, victor.torres, silvia.llorente, eva.rodriguez}@upf.edu

Abstract. Multimedia information management, which implies all steps from creation and production to distribution and consumption, is a complex and challenging research area. To have a secure and trusted system we need to take into account aspects such as digital rights management (DRM), certification, control and security. As current solutions rely on proprietary architectures and tools, we propose an open architecture, as general as possible and not restricted to a specific standard, which provides trust and rights management in multimedia information systems. We analyse how the elements of the architecture provide trust to the whole value chain by managing multimedia content and digital rights represented using current standards, such as MPEG-21 and OMA DRM, and we compare it with an alternative approach. Then, we illustrate the system operation through a content composition use case, and finally, we present the software tools that we have already developed and the future work.

1 Multimedia Information Management Architecture

In [1] we proposed an architecture for a system capable of processing multimedia information structured as defined in the MPEG-21 standard [2]. This architecture was refined in [3] and [4] to be as general as possible, considering the requirements from several standards, initiatives and projects like the Open Mobile Alliance (OMA) [5], MPEG-21 [2], Digital Media Project (DMP) [6], FP6 NAVSHP DRM [7] and AXMEDIS European project [8]. Figure 1 shows the basic modules that constitute the new architecture.

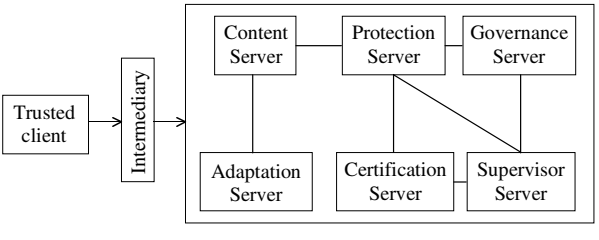

Fig. 1. DMAG-MIPAMS architecture

J. Dittmann, S. Katzenbeisser, and A. Uhl (Eds.): CMS 2005, LNCS 3677, pp. 55 – 64, 2005.

The architecture, called DMAG Multimedia Information Protection and Management System (DMAG-MIPAMS), whose name is after our group acronym DMAG [9], consists of several modules, where each of them provides a subset of the whole system functionality needed for managing and protecting multimedia content. The following list briefly describes the modules of the architecture:

- **Content server.** It provides the content that final users may request.
- **Protection server.** It is responsible for protecting the content or digital objects, which become protected objects, mainly using encryption techniques and managing the encryption keys.
- **Governance server.** The governance server includes several functionalities: license generation, license storage, authorisation and translation support.
- **Certification server**. It includes registration, authentication, certification and verification of users, tools and devices.
- **Adaptation server**. It performs the adaptation of content and its associated metadata, depending on transmission, storage and consumption constraints.
- **Supervisor server.** It receives reporting messages that include information about different aspects of media usage and stores them for future access.

It is worth noting that currently the architecture does not try to be complete, and some possible modules, such as a payment solution, are deliberately ignored.

2 Provision of Trust

After introducing our architecture, we are going to analyse the elements in the proposed system that provide trust from a business user or a final user point of view.

To provide trust to users it is important to take into account privacy aspects. In the presented system, information regarding content usage must be tracked. Nevertheless, this information will only be accessible to authorised parties. This authorisation will be done by means of party certification, which will provide the authentication in front of the service giving access to the information.

2.1 Use of Licenses

Digital Rights Management (DRM) enables the association of rights and conditions of usage to digital content, written in a digital license that can be embedded together with the content or stored in a separate way.

Digital licenses can be seen as digital documents that establish a contractual relationship between two parties: the license issuer and the granted party. That is, licenses can be used to establish contractual relationships in an e-commerce environment not only for final users (B2C scenario) but also between content creators/providers and distributors (B2B scenario).

Another interesting functionality of digital licenses together with the Governance server is the possibility to keep track of the identity and correctness of the actions performed by any of the value chain players, from the content creator to the final user. The authorisation algorithms use the licenses stored in the Governance server to

determine if all the parties (content provider, distributor, final user) use the contents in the right way, according to the rights they are granted by their authorising party.

As we have seen, DRM can be a key element to provide trust in a content management system. In the proposed system, the Governance server provides this functionality through its license creation and authorisation facilities.

2.2 Protection

Protection mechanisms over digital content make it possible to deploy a business model to ensure the accomplishment of the license terms, so that protected objects are safe from unauthorised access, providing trust to the DRM system.

The delivery of protection keys must be performed in a secure and trusted way. On one hand, keys must be delivered through a secure channel. Moreover, they must be inaccessible in the client side. This can be achieved by providing the keys to certified and hence trusted tools in the client side.

2.3 Users and Tools Certification

Any tool in the user side must be trusted and must perform some checks in the server side to resynchronise the local information with the server side in every reconnection. Every time a user tries to do an action over a protected and governed object, the client side module must send the necessary information to the server side so that it can verify not only the user and the device, but also the tool integrity to ensure that the module has neither been modified nor corrupted. By ensuring the tool integrity, we can be sure that it is still trusted from the system point of view. If we want to provide trust from the user perspective, we must trust on the party that is performing the certification, which can be more easily achieved in a B2B scenario than in a B2C scenario. Whereas in a B2B scenario each party usually has a previous knowledge of the rest of the players and even also of the system, which could be formalised in a contract, in the B2C scenario, users usually need to trust on some tools without a real knowledge on how they work or manage their personal information.

The Certification server provides the mentioned functionality to verify the user, device and tool integrity. The tool in the user side must be trusted and must perform some checks in the server side to resynchronise the local information with the server side in every reconnection. Every time a user tries to do an action over a protected and governed object, the client side module must send the necessary information to the server side so that it can verify not only the user and the device, but also the tool integrity to ensure that the module has neither been modified nor corrupted. By ensuring the tool integrity, we can be sure that it is still trusted.

2.4 Supervision and Tracking

Transaction and operation supervision and tracking is another feature that can provide trust in such a system. The Supervisor server is responsible for collecting and interpreting the reporting messages generated by different modules and storing the appropriate information into a specific database. As we have already explained, the information in the reports can be notified to the corresponding party or used to block the access to a user, for accounting purposes or statistical analysis.

3 Existing Standards and the MIPAMS Architecture

As we have already mentioned, our intention is to define the architecture as general as possible so as not to be restricted to a specific standard, but to be able to align it to as many standards as possible. With this aim, we are going to present how it can operate with current standards, such as MPEG-21 [2] and OMA DRM REL [10]. However, in order to have a fully interoperable architecture capable of managing different multimedia formats at the same time, common interfaces for the identified modules should be defined.

MPEG-21 standard defines different mechanisms and elements needed to support multimedia information delivery and management, and the relationships and operations supported by them. In the seventeen parts of the MPEG-21 standard, these elements are elaborated by defining the syntax and semantics of their characteristics.

In the MPEG-21 context, the information is structured in Digital Items, which are the fundamental unit of distribution and transaction. A Digital Item [11] is constituted by the digital content, plus related metadata, such as adaptation information (DIA, Part 7) [12], information related to the protection tools (IPMP, Part 4) [13], rights expressions (REL, Part 5) [14], information to automatically report some actions exercised over the digital content (ER, Part 15) [15] and others.

In the following list, we describe how our architecture has the necessary functionality to cover the different parts of this standard:

- **DID.** Digital objects can have the structure of Digital Items, as defined in the DID part of the MPEG 21 standard.
- **IPMP, REL and RDD.** In MPEG-21 standard the protection and governance of digital content are specified in MPEG-21 IPMP Components, REL and RDD parts. MPEG-21 IPMP Components provides mechanisms to protect a digital item (DI) and to associate licenses to the target of their governance, while MPEG-21 REL specifies the syntax and semantics of the language for issuing rights for users to act on DIs while MPEG-21 RDD [16] comprises a set of terms to support the MPEG-21 REL.
- **ER.** Event Reporting is required within the MPEG-21 Multimedia Framework in order to provide standardised means for sharing information about Events amongst Peers and Users. Such Events are related to Digital Items and/or Peers that interact with them. In the MPEG-21 context, the reporting messages that include information about different aspects of media usage are called Event Reports. In our system, the functionality that involves the management of the event reports is provided by the Supervisor.

OMA Digital Rights Management (DRM) v2 [17] defines mechanisms to enable the consumption of digital content in a controlled manner. The content is consumed on authenticated devices per the usage rights expressed by the content owners. The OMA DRM work addresses the various technical aspects of this system by providing appropriate specifications for content formats, protocols, and the rights expression language based on ODRL [18]. ODRL and MPEG-21 REL are currently the two most important rights expression languages and, although they have a different syntax, their semantics is quite similar.

We have been working for some time in this interoperability issue. After an initial proposal of a simple syntactic mapping [19], [20] we have proposed a specific subset of MPEG-21 REL that is interoperable with the first version of OMA DRM REL [21], [22], [23] and also with version 2 of OMA DRM REL [21], [24], [25], [26]. This work could lead to the specification of an MPEG-21 REL profile, as it is being discussed in the MPEG group after our proposals.

Our architecture enables the use of whatever rights expression language the content creators, providers or distributors want to use, associated to digital objects. Internally, our system can work with a predefined rights expression language and provide some translation mechanisms for converting licenses expressed in other languages to the predefined one. This translation can only be performed under certain conditions, which can be grouped to define rights expressions languages profiles, as stated before.

We have also studied the workflow of OMA DRM in order to provide a generic workflow for DRM systems [27].

4 Relationship of the Architecture with Other Initiatives

Other architectures exist for the management of protected multimedia content. Nevertheless, they correspond to proprietary systems and it is difficult to compare our architecture with them, as they do not follow any standard. Among projects funded by public administrations, the MOSES project [28] developed the OpenSDRM [29] architecture, with which DMAG-MIPAMS has some common points.

The main differences between MIPAMS and OpenSDRM are the following:

- OpenSDRM provides a Wallet, the middleware that requests and manages licenses and performs the authorizations locally. A single wallet can be used on the same device by different applications, whereas in MIPAMS we will have a trusted plug-in for each application or specific trusted application.
- OpenSDRM currently uses ODRL to express the licenses, while MIPAMS proposes different mechanisms, such as translation, to support ODRL and MPEG-21 REL at the same time.
- OpenSDRM provides a Content Preparation Server, which receives raw data and encodes it on a specified format, while adding metadata and protection. On the other hand, MIPAMS leaves this functionality for specific user-side tools, while providing protection, licensing and adaptation functionalities on the server side.
- MIPAMS performs the authorisation of users based on a licenses chain (from content rights holder to party or user), ensuring rights fulfilment in the whole value chain, whereas OpenSDRM uses a single license referred to the party.
- MIPAMS, through supervision and tracking functionalities, enables post-usage billing. OpenSDRM provides an interface for a pre-usage payment solution while, for the moment, MIPAMS leaves this point open for the involved parties.

5 Use Case

In this section we present a scenario to illustrate how the proposed architecture and the processing of protected and governed multimedia content are related.

The scenario we propose is about content composition. Imagine that a publisher has purchased a license that grants him the right to include a still image in one of his electronic publications. The mentioned user has installed in his device a specific editing tool or a plug-in for an already existing tool capable of managing the protected and governed objects of the system. For the sake of simplicity, the license creation for the new composite content has been omitted.

The use case begins when the user (publisher) downloads the protected and governed image and tries to include it in his publication using the editing tool. Figure 2 shows the steps involved in the content composition use case, which are:

1. The user opens in the editing tool the digital object that contains the image.
2. The user tries to include it in his publication ("embed" image).
3. The tool/plug-in connects to the Protection server in order to check if the user is authorised. It sends the following information: requested operation ("embed"), object identifier, user identifier, device identifier and tool/plug-in identifier.

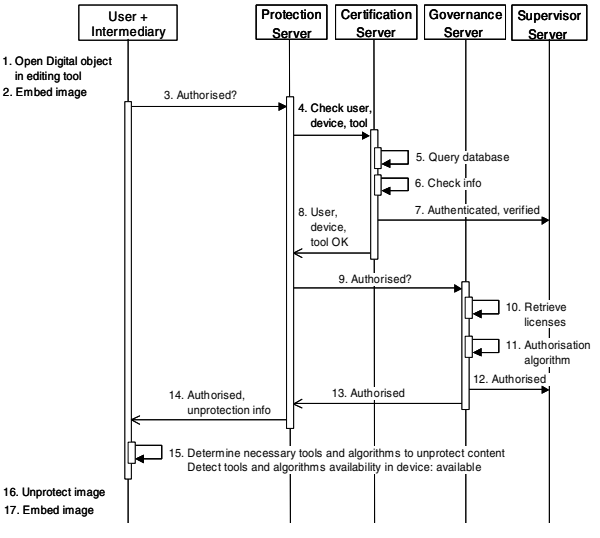

Fig. 2. Content composition use case

4. The Protection server sends the Certification server the received information.
5, 6. The Certification server queries its database and checks that the user and device are registered and the tool/plug-in integrity.
7. An event report is sent to the Supervisor server notifying the successful authentication of the user and verification of device and tool.
8. The Certification server notifies the Protection server that everything is OK.
9. The Protection server contacts the Governance server asking if the user is authorised. This authorisation consists on checking if the user is granted to exercise the right "embed" over the image according to a certain chain of licenses (going from the image creator (or rights holder) to the publisher).

10, 11. The Governance server searches in the database the licenses related to the user and runs an authorisation algorithm over the chain of licenses. The Governance server determines that the user is granted to perform the requested operation and that the distribution chain is correct (all the parties in the license chain were granted by their corresponding license).
12. An event report is sent to the Supervisor notifying the successful authorisation.
13. The Governance server notifies the right authorisation to the Protection server.
14. The Protection server notifies the object viewer that the user is authorised and sends the needed information for unprotecting the content.
15. The tool/plug-in determines the tools or algorithms that must be used to unprotect the object and detects that they are already available in the user device.
16. The tool/plug-in unprotects the image following the unprotection process steps and using the necessary tools and algorithms.
17. The editing tool finally embeds the still image into the electronic publication.In this section we present a scenario to illustrate how the proposed architecture and the processing of protected and governed multimedia content are related.

6 Development of Tools and Demonstrators

At the DMAG [9], we have been working in the MIPAMS trusted architecture and related standards, and have already developed several tools [30], contributed to the standardisation of MPEG-21 and included in the MPEG-21 Reference Software [31]. Some other tools have also been created to deal with ODRL licenses [32]. The tools we present in subsequent subsections are publicly available at [30] and [32].

The implemented tools offer independent and isolated functionality and will be extended and integrated with other modules in the context of the AXMEDIS European project [8] to develop several demonstrators, for several delivery channels. With these demonstrators we will verify the operation of the proposed modular architecture. Moreover, an AXMEDIS framework will be available for presenting the tools implemented in this project.

6.1 Rights Expression Languages and Rights Data Dictionary Tools

REL and RDD developed tools concern the creation and validation of digital licenses.

License Validators. These tools take a license as input and provide a verdict as the output. If the input license is not valid, a report explains the reasons why, according to the validation that has been performed. These tools, which have been implemented as Java APIs that can be run independently or integrated with other modules, include:

- **MPEG-21 REL Schema Checker**. It checks if an MPEG-21 REL license is valid against the corresponding XML Schemas.
- **MPEG-21 ODRL Schema Checker**. It checks if an ODRL license is valid against the corresponding XML Schemas.
- **MPEG-21 REL Validation Rules Checker**. It checks if a schema-valid MPEG-21 REL license is a valid REL License according to the MPEG-21 REL standard specification [14]. A license will be REL syntactically conformant if it complies with all the rules specified in the standard.

License Creators. These tools have been implemented as web applications, formed by a web page containing an HTML form, a servlet for processing the information introduced in this form, a Schema Checker implementation and several auxiliary files, mainly used for formatting the information. The introduction of information is done by means of the HTML form. If all information has been filled, an XML file containing the license is created. Finally, the license syntax is checked with the Schema Checker and returned to the user, who can see the generated license and also store it locally. They include:

- **MPEG-21 REL License Creator**. It allows the introduction of the following information to create a license: Principal, Resource, Right, Conditions and Issuer.
- **ODRL License Creator**. It allows the introduction of the following information to create a license: Asset, Permission, Constraints and Party.

MPEG-21 Authorisation Tools. These tools determine if a user is authorised to perform an action over a resource according to the license terms. In this tools we have used the RDD term genealogy defined in MPEG-21 to determine if a term present in a license (e.g. Adapt) grants a user the permission to perform another action (e.g. Play). We have implemented a specific tool, as a Java API, that consults an RDD ontology placed in an external server, returning all the ancestors of an input RDD term.

- **License Interpreter**. It performs the authorisation according to a unique license and a simple, non-standardised query mechanism.
- **Interpretation Conformance**. It performs a standardised authorisation and query mechanism, which consists on checking not only if the user is authorised according to the source license, but also if the party that issued this license was authorised to do so, and so on, so that the whole licensing chain is checked.

6.2 MPEG-21 IPMP Tools

IPMP developed tools concern the validation and extraction of IPMP information from Digital Items, as explained next:

- **MPEG-21 IPMP Expressions Validator**. This tool parses and validates a set of IPMP Information documents against the XML Schemas specified in them.
- **MPEG-21 IPMP Information Extractor**. This tool obtains the IPMP Information associated to a protected DIDL document or parts thereof. First, the protected element(s) within the DIDL document are identified and presented. Then, the software module obtains and presents the relevant information related to the IPMP tools and the license(s) associated to each one of the IPMP DIDL elements previously identified.
- **MPEG-21 License Extractor**. This tool obtains the license(s) associated to a protected and governed DIDL document or parts thereof. It identifies the protected element within the DIDL document given as input, and obtains the license(s) that govern(s) it, if any.

7 Conclusions

We have presented a general architecture of a system for the distribution and management of protected and governed multimedia content, based on different requirements, not restricted to a specific standard and flexible enough to locate different functionalities in separate machines.

We have analysed the elements in the proposed architecture to describe how they provide trust in different aspects to the global system and the whole value chain.
On the other hand, we have shown how the presented architecture is flexible enough to support current standards such as MPEG-21 and OMA DRM. In the MPEG-21 context, we have described the relationship between MPEG-21 parts and the elements or functionalities of the architecture while, regarding OMA DRM, we have shown how the use of different rights expressions languages can be managed by translation mechanisms and profile definition. Moreover, we have compared MIPAMS with the OpenSDRM architecture.

Then, a use case has been presented showing the successive steps that the system will follow in a content composition scenario, considering authentication, verification and authorisation matters.

Finally, we have presented several tools that have been contributed to the MPEG-21 Reference Sofware part and we have introduced the AXMEDIS project, which will provide a publicly available framework.

Acknowledgements. This work has been partly supported by the Spanish administration (AgentWeb project, TIC 2002-01336) and is being developed within VISNET (IST-2003-506946, http://www.visnet-noe.org), a European Network of Excellence and AXMEDIS, a European Integrated Project, both funded under the European Commission IST FP6 program, and "Projecte Integrat" project, funded by the Catalan Administration (Fundació i2Cat).

References

1. Torres, V., Rodríguez, E., Llorente, S., Delgado, J.: Architecture and Protocols for the protection and management of multimedia information. MIPS 2004, LNCS, Vol. 3311. Springer-Verlag, Berlin Heidelberg New York (2004) 252-263
2. MPEG 21, http://www.chiariglione.org/mpeg/standards/mpeg-21/mpeg-21.htm
3. Torres, V., Rodríguez, E., Llorente, S., Delgado, J.: Trust and Rights in Multimedia Content Management Systems. The IASTED International Conference on Web Technologies, Applications, and Services (WTAS 2005). To be published
4. Torres, V., Rodríguez, E., Llorente, S., Delgado, J.: Use of standards for implementing a Multimedia Information Protection and Management System. AXMEDIS 2005. To be published
5. Open Mobile Alliance (OMA), http://www.openmobilealliance.org
6. Digital Media Project (DMP), http://www.dmpf.org/
7. Digital Rights Management (DRM) Coordination Group of the European FP6 Projects in the area of Networked AudioVisual Systems and Home Platforms (NAVSHP), http://www.rose.es/navshp

8. Automatic Production of Cross Media Content for Multi channel Distribution (AXMEDIS), IST 2004 511299, http://www.axmedis.org
9. Distributed Multimedia Applications Group (DMAG), http://dmag.upf.edu
10. OMA, DRM Rights Expression Language (OMA-Download-DRMREL-V2_0-20041210-C). December 2004. http://www.openmobilealliance.org
11. ISO/IEC, ISO/IEC 2nd Edition FCD 21000-2 – Digital Item Declaration
12. ISO/IEC, ISO/IEC FDIS 21000-7 – Digital Item Adaptation
13. ISO/IEC, ISO/IEC CD 21000-4 – Intellectual Property Management and Protection
14. ISO/IEC, ISO/IEC IS 21000-5 – Rights Expression Language
15. ISO/IEC, ISO/IEC WD 21000-15 – Event Reporting
16. ISO/IEC, ISO/IEC IS 21000-6 – Rights Data Dictionary
17. OMA, DRM Specification (OMA-DRM-DRM-V2_0-20040716-C), July 2004, http://www.openmobilealliance.org
18. Open Digital Rights Language (ODRL), http://odrl.net
19. Polo, J., Prados, J., Delgado, J.: Interworking of Rights Expression Languages for Secure Music Distribution. In: Delgado, J., Nesi, P., Ng, K. (eds.): WEDELMUSIC 2004 Proceedings, IEEE Computer Society (2004) 78-84
20. Polo, J., Prados, J., Delgado, J.: Interoperability between ODRL and MPEG 21 REL. ODRL International Workshop (2004)
21. OMA, DRM Rights Expression Language (OMA-DRM-REL-V1_0-20040615-A). June 2004. http://www.openmobilealliance.org
22. Delgado, J., Prados, J., Rodríguez, E.: Interoperability between MPEG-21 REL and OMA DRM: A Profile? ISO/IEC JTC 1/SC 29/WG 11/M11580. January 2005. http://dmag.upf.edu/DMAGMPEG21Tools/m11580.pdf
23. Delgado, J., Prados, J., Rodríguez, E.: Profiles for interoperability between MPEG-21 REL and OMA DRM. IEEE CEC 2005, IEEE Computer Society, to be published
24. Delgado, J., Prados, J., Rodríguez, E.: A subset of MPEG-21 REL for interoperability with OMA DRM v2.0. ISO/IEC JTC 1/SC 29/WG 11/M11893. April 2005. http://dmag.upf.edu/DMAGMPEG21Tools/m11893.pdf
25. Prados, J., Rodríguez, E., Delgado, J.: Interoperability between different Rights Expression Languages and Protection Mechanisms. AXMEDIS 2005. To be published
26. Prados, J., Rodríguez, E., Delgado, J.: A new Approach for Interoperability between ODRL and MPEG-21 REL. Second International ODRL Workshop. To be published
27. Llorente, S., Rodríguez, E., Delgado, J.: Workflow description of digital rights management systems. OTM 2004 Workshops. LNCS, Vol. 3292. Springer-Verlag, Berlin Heidelberg New York (2004) 581-592
28. MPEG Open Security for Embedded Systems (MOSES) project, http://www.ist-moses.org
29. Serrao, C., Dias, M., Delgado, J.: Using ODRL to express rights for different content usage scenarios. The Second International ODRL Workshop 2005. To be published
30. DMAG MPEG 21 Tools, http://dmag.upf.edu/DMAGMPEG21Tools
31. ISO/IEC, ISO/IEC FCD 21000-8 – Reference Software
32. DMAG ODRL Tools, http://dmag.upf.edu/ODRLTools