Protecting Notification of Events in Multimedia Systems

Eva Rodríguez, Silvia Llorente and Jaime Delgado

DMAG (Distributed Multimedia Applications Group)
Universitat Pompeu Fabra, Passeig de Circumval·lació, 8,
08003 Barcelona, Spain
Universitat Politècnica de Catalunya, Jordi Girona, 1-3,
08034 Barcelona, Spain

Abstract. Protection of multimedia information is an important issue for current actors in the multimedia distribution value chain. Security techniques exist for protecting the multimedia contents itself, like encryption, watermarking, fingerprinting and so on. Nevertheless, at a higher level, other mechanisms could be used for the protection and management of multimedia information. One of these mechanisms is the notification of events of actions, done by the different actors of the multimedia value chain (from content creator to final user), for the different delivery channels. It is possible to describe event notifications by standard means by using MPEG-21 event reporting. However, the current standard initiative does not take into account the security of the events being notified. In this paper we present a possible solution to this problem by combining two different parts of the MPEG-21 standard, Event Reporting (ER) and Intellectual Property Management and Protection (IPMP).

1 Introduction

Piracy is a key problem for current actors in the multimedia value chain, since available security techniques are currently not enough to provide full protection against it.

Something that could help in fighting piracy is the notification of events being done by users of multimedia systems. In this way, distributors of multimedia content can be informed of the usage of the multimedia objects they have provided through a web site, a downloading service for mobiles or whatever distribution mechanism used. Afterwards, users illegally distributing content could be prosecuted by means of these activity records. It is worth noting that privacy of users is preserved until an illegal action from a user is detected.

By means of the chain of licenses defining the contractual relationships between content creators, distributors and final users, not only distributors could be informed of the events occurred, but also the rest of actors in the value chain. In any case, they must have the appropriate permission to do so.

In the above situations, event notifications should be protected. We should guarantee access and modification only the users who have permission. In this sense, and

Rodríguez E., Llorente S. and Delgado J. (2006).
Protecting Notification of Events in Multimedia Systems.
In *Proceedings of the 4th International Workshop on Security in Information Systems*, pages 153-162

based on MPEG-21 standard we propose an approach to provide protection to events based on Event Reporting (ER) and Intellectual Property Management and Protection (IPMP).

This paper is organised as follows. First, we give some general information about MPEG-21 and the parts of this standard relevant to this research paper. Then, we make our proposal for protecting notification of events (or event reports), as known in the MPEG-21 world. After this, we describe some use cases where event reports are sent in different situations. Finally, we draw some conclusions and present some future work.

2 Multimedia Information Representation Using MPEG-21

The MPEG-21 [1] standard is divided into several parts, which deal with different aspects of multimedia information management. In the MPEG-21 context, the information is structured in Digital Items, which are the fundamental unit of distribution and transaction. Digital Items are digital documents written in XML according to a XML Schema.

A Digital Item is defined in [2] as a structured digital object, including a standard representation and identification, and metadata within the MPEG-21 framework. The rest of this section presents some parts of the MPEG-21 standard.

2.1 Digital Item Declaration (DID)

The two major goals of the Digital Item Declaration part within MPEG-21 are first to establish a uniform and flexible abstraction and interoperable schema for declaring Digital Items and also to be as general and flexible as possible, providing hooks to enable higher level functionality and interoperability. The Digital Item Declaration (DID) technology [3] is defined in three normative parts: DID Model, Representation and Schema. DID corresponds to part 2 of the MPEG-21 standard.

Within this model, a Digital Item is the digital representation of a work, and as such, it is the thing that is acted upon.

The different elements inside a DI provide different functionality for the organisation of multimedia information. The Container is a potentially hierarchical structure that allows Items to be grouped together with their descriptors, components and resources. The term “Item” should be understood as a declarative representation of a Digital Item.

Among all DI elements, the Statement one provides the possibility of inserting data in any kind of format, specially XML. This provides a wide field for including information used to protect and process multimedia data, such as rights expressions, intellectual property management and protection information or adaptation descriptors.

2.2 Intellectual Property Management and Protection (IPMP)

The Intellectual Property Management and Protection (IPMP), part 4 [4] of the MPEG-21 standard, deals with the standardisation of a general solution for the management and protection of Intellectual Property.

In this part of the standard an interoperable framework for Intellectual Property Management and Protection is being defined.

In IPMP the expression and enforcement of rights that are associated with digital item distribution, management and usage by all members of the value chains is also included.

2.2.1 IPMP DIDL

IPMP Digital Item Description language (IPMP DIDL) [4] is defined to provide protection and governance to any part of a Digital Item, from a complete Digital Item to a specific asset.

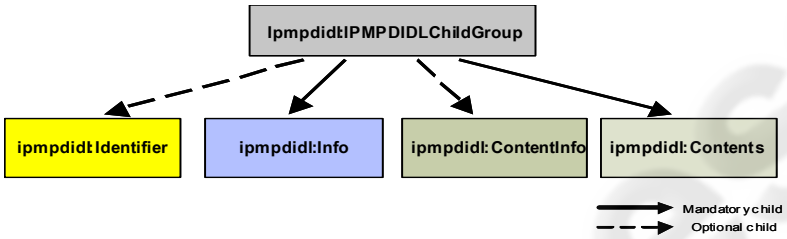

Fig. 1. Structure of IPMP DIDL elements for the DID model.

Digital Item hierarchy is represented in the Digital Item Declaration Language (DIDL) [3], which is defined by an XML schema [3]. The IPMP DIDL encapsulates and protects a part of the hierarchy of a Digital Item, and associates appropriate identification and protection information with it. For each entity in the DID model, an IPMP DIDL element is provided as a protected representation of that entity, derived from the abstract DID model types as defined in the DID model schema in ISO/IEC 21000-2. As both IPMP DIDL elements and DIDL elements extend abstract types defined for the DID model, they are interchangeable within a Digital Item Declaration.

Each of the IPMP DIDL elements has the same semantics as its DIDL counterpart and contains the elements Identifier, Info, ContentInfo and Contents. The Identifer element contains a unique identifier for the protected representation of the DIDL element. The Info element contains information about the protection tools and the rights expressions that govern the element. The ContentInfo element acts as a placeholder for the protected contents. Fig. 1 presents the structure of IPMP DIDL elements.

2.2.2 IPMP Information

The information related to protection of a Digital Item falls into two categories. The first is information that pertains to the whole Digital Item, including collections of general Licenses and a list of tools used in the Digital Item. The second category is information about the specific protection applied to a certain part of Digital Item

hierarchy protected with IPMP DIDL – i.e. specific tool applied, keys, licenses specific to that content, and so on. In the IPMP Info schema [4], these two categories of information are expressed with two top-level elements: IPMPGeneralInfoDescriptor and IPMPInfoDescriptor respectively.

The IPMPGeneralInfoDescriptor element contains general information about protection and governance related to a complete Digital Item. IPMP tool lists and licenses packaged in a Digital Item can be included under this element. The IPMPInfoDescriptor, on the other hand, is designed to contain information about governance of a specific section of Digital Item hierarchy, and has to be attached to that section through the use of IPMP DIDL.

The IPMPGeneralInfoDescriptor has two purposes: to allow a Digital Item author to provide a list of IPMP Tools used in governance that can then be referred to from IPMPInfoDescriptors; and to provide a container for Licenses carried in the Digital Item.

On the other hand, the IPMPInfoDescriptor contains information about governance that applies to a specific piece of content – generally a part of the Digital Item hierarchy. The Tool child element specifies a tool, which can be used to unprotect the content; the RightsDescriptor child element contains licenses governing the content. A digital signature for the entire element may also be attached.

2.3 Event Reporting (ER)

Event Reporting [5] is required within the MPEG-21 Multimedia Framework to provide a 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.

Event Reporting could be useful when monitoring of the usage of copyrighted material. The provider offering Digital Items for download would specify in an Event Report Request that, whenever a Resource within a Digital Item is rendered (e.g. played), he would receive an Event Report enabling him to manage his royalties. Upon rendering, the Peer will generate an ISO/IEC 21000 Event Report which will be delivered to the rights holder specified, in an Event Report Request, containing information about the Digital Item, the Resource, and the conditions under which it has been rendered. In this sense, a core experiment has been contributed to MPEG-21 standard, for studying in which cases event reports should be generated [6].

Fundamentally, Event Reporting will facilitate interoperability between consumers and creators, thereby enabling multimedia usage information to be both requested and represented in a normalised way. Examples where Event Reports may be requested include usage reports, copyright reports, financial reports and technical reports.

The basic model of Event Reporting indicates that Events that need to be reported may be specified by interested parties through the use of an Event Report Request (ERR). An ERR is used to define the conditions under which an Event is deemed to have occurred. Events defined by ERRs trigger the creation of an associated Event Report (ER), which contains information describing the Event, as specified in the associated ERR.

The ER purpose is to indicate which Peer created it, define the data items that are to be included in such an Event Report(s), provide a reference to the originating ER-R, provide status information regarding its completion and creation, along with a free-form description.

3 Providing Protection to Event Reports

Event Reporting standard specification [5] at its current stage does not provide a way to ensure integrity and authenticity to the reported data (ER) neither to the request data (ERR). On the other hand, it is not possible to encrypt partially or totally ERs and ERRs.

This paper exposes how these goals can be achieved; it is based on the contribution [7] made by the authors to MPEG-21 in form of input document to the 74th MPEG meeting. This contribution presents mechanisms that ensure authenticity and integrity to Event Reports and Event Report Requests. Moreover, it also presents how to protect ERs and ERRs at any level, from a complete ER or ERR to specific elements or data within them.

3.1 Providing Data Integrity and Authenticity

In order to ensure authenticity and integrity for the data to be requested and reported, we propose the use of digital signatures for the appropriate elements within ERs and ERRs. We can use the dsig:Signature [8] element (see Fig. 2) to digitally sign all the metadata within ER and ERR elements, or if necessary the dsig:Signature element can be used to sign concrete elements within ERs or ERRs. For example, it can be useful to sign the reported data, that is metadata that describe the DI related operation performed by the user, or it can be useful to sign requested data.

Then, it is important to study for which elements within ERs and ERRs this will be useful. Then, we will add the dsig:Signature element as child element of each of them that will contain the digital signature for its parent element. Fig. 2 shows how the dsig:Signature element could be used to sign an ER.

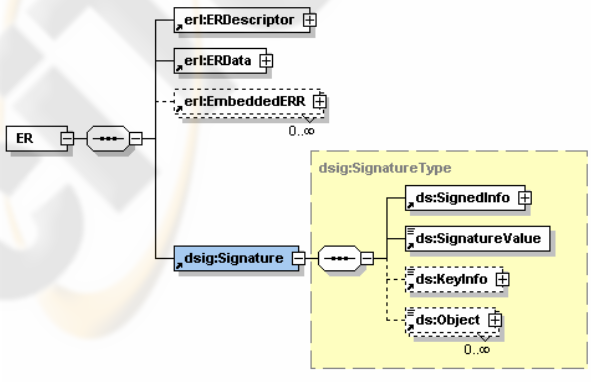

Fig. 2. ER element including dsig:Signature.

The ERData element is a clear example of an element that could be signed in order to provide authenticity and integrity of the data it contains. Nevertheless, further discussion is needed to determine the rest of elements for which authenticity and integrity will be provided.

In this way, once agreed the different elements within ERs and ERRs that will require to be signed, integrity and authenticity for the whole ERs and ERRs or for specific data within them will be guaranteed.

3.2 Data Encryption

If we want to protect, for example to encrypt, ERs and ERRs or elements within them, we can do that at least in two different ways.

The first option is to define the equivalent encrypted elements for ER and ERR elements and if necessary for other elements within them. Fig. 3 shows an example of how the encryptedER element can be defined using W3C XML Encryption recommendation [9].

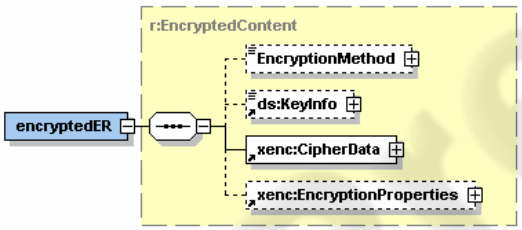

Fig. 3. encryptedER element.

In this case it is also important to determine for which elements it is useful to provide this functionality.

The second option is to define the equivalent IPMP ER elements as done in IPMP Components [4] standard specification for DIDL elements. This part of the standard defines the IPMP DIDL schema that facilitates the representation of a protected Digital Item structure within a DID document by encapsulating protected DIDL elements and linking appropriate IPMP Info to them, allowing for encryption and other forms of protection over DIDL hierarchy.

Then, it could be considered to define an IPMP ER schema, in order to provide protection to the whole ER and ERRs or to elements within them. Using this solution we can protect ER elements in different ways and it also allows to govern ER and ERRs or elements within them.

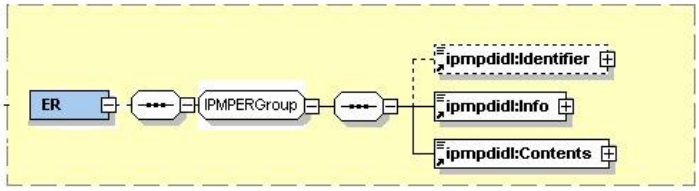

Fig. 4. IPMP ER element.

Fig. 4 shows the ER IPMP element. The elements that form the IPMPERGroup are Identifier, Info and Contents. The Info element contains information about the mechanisms and licenses involved in the protection of the ER data and the access of this data. This element may link directly to an existing rights expression or contain an IPMPDescriptor from the IPMP Info schema presented in section 2.2.2. Finally, the Contents element contains the protected ER data.

4 Event Reporting Usage Use Cases

In this section, we describe how event reporting can be applied to a real scenario where a user wants to make use of multimedia content. In this scenario, several servers are involved. This scenario will be explained with two use cases. They are described in detail in [10, 11, 12] in the context of the MIPAMS architecture.

In the MIPAMS architecture, the server mainly involved in event reporting is Supervisor Server. This server keeps track of the actions or events occurred in the system. We will describe here the generation of some events related to user actions, especially content consumption, but others are possible (network/server errors, etc.).

Events stored by the Supervisor Server can be later analysed in order to extract billing information, usage statistics, errors, blocking because of illegal actions, etc.

We will present this scenario with two use cases, one where the user is not allowed to make use of content and other where user is authorised to perform the action.

To describe the two use cases we will make use of other servers from the MIPAMS architecture [11]. They are Protection, Certification and Governance servers.

Fig. 5 shows the first use case, where the user is not authorised to perform the action because it is blocked in the system for example because he performed a previous illegal operation. The steps involved in this use case are as follows:

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 action).
3. The user tool 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 identifier.
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 not blocked and the tool/plug-in integrity.

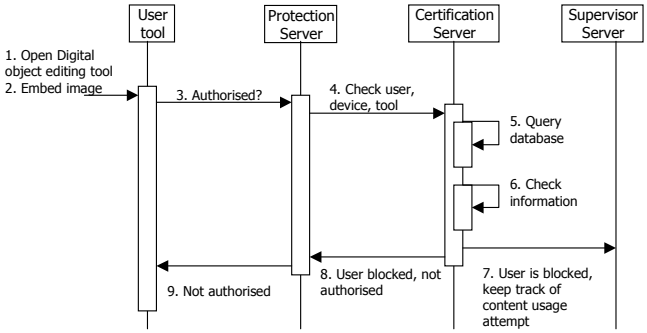

Fig. 5. Unsuccessful content usage.

7. An event report is sent to the Supervisor server notifying that the user is blocked, thus it cannot be authorised.
8. The Certification server notifies the Protection server that user is blocked.
9. The Protection server returns a negative response to the user tool. The action cannot be done, so the embedding of the image will not be performed.

Fig. 6 shows the second use case, where the user is authorised to perform the embedding action. The steps involved in this use case are as follows:
1, 6. The same as the previous one.
7. The user is authorised, protection server is informed.
8. 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 trying to embed the image).
9, 10. 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).
11. An event report is sent to the Supervisor notifying the successful authorisation.
12. The Governance server notifies that authorisation is OK to the Protection server.
13. The Protection server notifies the object viewer that the user is authorised and sends the needed information for unprotecting the content.

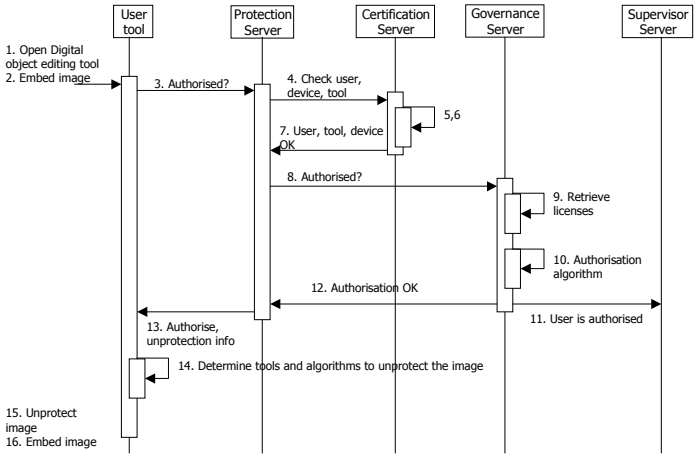

Fig. 6. Successful content usage.

14. 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.
15. The tool/plug-in unprotects the image following the unprotection process steps and using the necessary tools and algorithms.
16. The editing tool finally embeds the still image into the electronic publication.

We can see that event reporting can be differently used for keeping track of the actions occurring in a system where multimedia content is consumed. In the above use cases, we have used them for notifying that a blocked user wants to perform an operation which he is not allowed to and for notifying that an operation can be authorised based on the licenses a user owns.

5 Conclusions and Future Work

This paper has presented a way of protecting notification information generated in a system where multimedia content is consumed. The protection of the event reports is done by means of different parts of MPEG-21 standard: Event Reporting and Intellectual Property Management and Protection, following the ideas described in IPMP-DIDL, the way of protecting digital items in MPEG-21. Some parts of this standard have been described.

Moreover, some preliminary ideas regarding event reporting protection and posted as contributions to the MPEG-21 standard have been presented. They are based on the use of digital signatures for guaranteeing Event Report integrity and authenticity. Furthermore, two different approaches have been presented to provide integrity and authenticity to event reports. On the one hand, the encryption of Event Reports or some of its elements. On the other hand, the specification of IPMP ER elements to protect complete or partially Event Reports and to associate protection and governance information to them. These contributions were presented and discussed during 74th MPEG meeting. Finally, it was agreed that security issues regarding to Event

Reporting will be specified in an amendment to Part 15 of the MPEG-21 standard and will take as basis the presented contributions.

The use of event reporting in a real scenario has been described in two use cases.

Future work we plan to do around the presented is to deep into the description of event reporting protection, trying to include it as part of the standard and the implementation of the techniques proposed in order to check if its use is feasible. For more details about Distributed Multimedia Applications Group (DMAG), see [13].

Acknowledgements

This work has been partly supported by the Spanish administration (DRM-MM project, TSI2005-05277) and AXMEDIS [14], a European Integrated Project, funded under the European Commission IST FP6 program.

References

1. MPEG-21, http://www.chiariglione.org/mpeg/standards/mpeg-21/mpeg-21.htm. 2004.
2. ISO/IEC, ISO/IEC TR 21000-1 – Vision, Technologies and Strategy.
3. ISO/IEC, ISO/IEC 2nd Edition FCD 21000-2 – Digital Item Declaration.
4. ISO/IEC, ISO/IEC FDIS 21000-4 – Intellectual Property Management and Protection Components.
5. ISO/IEC, ISO/IEC FCD 21000-15 – Event Reporting.
6. Rodríguez, E., Cirera, M., Delgado, J. Core Experiment on use of Event Report Requests: Specification of Use Cases. ISO/IEC JTC1/SC29/WG11 MPEG2005/ M12299. July 2005.
7. Rodríguez, E., Delgado, J. Integrity and authenticity of Event Reporting information. ISO/IEC JTC1/SC29/WG11 MPEG2005/M12525. October 2005.
8. XML-Signature Syntax and Processing, http://www.w3.org/TR/xmldsig-core/
9. XML Encryption, http://www.w3.org/TR/2002/REC-xmlenc-core-20021210/
10. Torres, V., Rodríguez, E., Llorente, S., Delgado, J. Use of Standards for Implementing a Multimedia Information Protection and Management System. 1st International Conference on Automated Production of Cross Media Content for Multi-Channel Distribution (AXMEDIS 2005). http://www.axmedis.org/axmedis2005. November-December 2005.
11. Delgado, J., Torres, V., Llorente, S., Rodríguez, E. Rights and trust in multimedia information management. Conference on Communications and Multimedia Security (CMS 2005). http://cms2005.sbg.ac.at/. September 2005.
12. Delgado, J., Torres, V., Llorente, S., Rodríguez, E. Trust and rights in multimedia content management systems. Web Technologies, Applications and Services (WTAS 2005). http://www.iasted.org/conferences/2005/calgary/wtas.htm. July 2005.
13. DMAG, http://dmag.upf.edu
14. Automated Production of Cross Media Content for Multi-Channel Distribution (AXMEDIS). http://www.axmedis.org