From OPIMA to MPEG IPMP-X

A standard's history across R&D projects

Carlos Serrão*, José Miguel Salles Dias*, Panos Kudumakis**♦

* ADETTI/ISCTE, Associação para o Desenvolvimento das Telecomunicações e Técnicas de Informática, Edifício ISCTE, 1600-082 Lisboa, Portugal, www.adetti.pt

{Carlos.Serrao Miguel.Dias}@adetti.iscte.pt

**inAccess Networks S.A.

95A Pentelis Av., GR 152 34 Halandri, Athens, Greece

panos@ieee.org

Abstract

This paper describes the work performed by a number of companies and universities who have been working as a consortium under the umbrella of the European Union Framework Programme 5 (FP5), Information Society Technologies (IST) research program, in order to provide a set of Digital Rights Management (DRM) technologies and architectures, aiming at helping to reduce the copyright circumvention risks, that have been threatening the music and film industries in their transition from the "analogue" to "digital" age. The paper starts by addressing some of the earlier standardisation efforts in the DRM arena, namely, OPIMA (Open Platform Initiative for Multimedia Access). One of the described FP5 IST projects, OCCAMM (Open

♦ Panos Kudumakis from 1998 to 2004 was with Scipher-Central Research Laboratories (former EMI), Dawley Road, Hayes, Middlesex, UB3 1HH, UK

Components for Controlled Access to Multimedia Material), has developed the OPIMA vision. The paper addresses also the Motion Pictures Expert Group - MPEG DRM work, starting from the MPEG Intellectual Propriety Management and Protection - IPMP "Hooks", towards the MPEG IPMP Extensions, which has originated the first DRM related standard (MPEG-4 Part 13, called IPMP Extensions or IPMP-X) ever released by ISO up to the present days[1]. The paper clarifies how the FP5 IST project MOSES (MPEG Open Security for Embedded Systems), has extended the OPIMA interfaces and architecture to achieve compliance with the MPEG IPMP-X standard, and how it has contributed to the achievement of "consensus" and to the specification, implementation (Reference Software) and validation (Conformance Testing) of the MPEG IPMP-X standard.

1. Introduction

While digital technology has enabled new and more flexible means to create, exchange, store and consume multimedia content, when compared to the "analogue era", it has eliminated many of the barriers which have been implicitly granting value to the content, allowing, for example, an easy sharing of digital material over networks with no loss of quality even after an unlimited number of copies. In this context, the modern content distribution business models such as the Internet download and super distribution (through Peer to Peer - P2P networks), have proven to have considerable flaws and drawbacks. This has lead to the need of reassessing and modifying, traditional approaches of content protection. This change in the value chain has affected mostly the music and film industries. Mass storage and copy systems have become cheaper, Internet bandwidth at the final user home has increased, as prices for maintaining it

[1] MPEG IPMP-X was released in 2003 and is currently the single ISO standard in the DRM arena.

have fallen, and the content compression technologies have evolved in such a way, that it has created an increased interest for potential illegal use.

Currently the content industry is trying to identify illegal copiers who are using file sharing systems. Internet providers are forced by court to open their user logs and allow externals to prosecute their illegal users. On the one hand, the principle of anonymity and the protection of personal information have become highly questionable. On the other hand, this approach will have difficulty in coping with the complete number of illegal distributions, since the number of users that are taking part in these systems (in the order of millions and growing on a daily basis [1, 2]) are diminishing the probability of being caught and consequently the prevention of illegal media distribution. Other approaches must be found. These can only work by controlling either the distribution of the content via trusted channels or the protection of the content with access control, or the combination of both.

This paper provides both an overview of the development of new standards (from ISO and other bodies) and technologies which deploy a comprehensive framework for dealing with digital copyright protection and intellectual propriety rights as well as the description and achieved results of two EU IST RTD projects (OCCAMM [3] and MOSES [4]), that have addressed the implementation, benchmark and evaluation of such technologies and standards. This set of DRM technologies are currently enjoying world-wide support not only because they have been approved as International Standards (ISO/IEC JTC1/SC 29/WG11 14496-13 (MPEG-4) [5] & 13818-11 MPEG (MPEG-2) [6]), but also due to the fact that they provide the means for achieving interoperability among different manufacturers of devices, independently of the way that content is protected. The paper is organised as follows: First, a definition of DRM is given, which has the agreement of the Networked Audio-Visual Systems and Home

Platforms projects of the 6th Framework Programme of the European Union. Afterwards, the OPIMA initiative [7] is introduced, where most of the concepts currently supported by the IPMP-X standard were originated. The IST project OCCAMM, which implemented for the first time the OPIMA vision, is then described, focusing in the developed architecture and achieved results. The MPEG community own efforts of creating a DRM related standard are then introduced, starting from the IPMP "Hooks", that evolved into the current MPEG IPMP-X ISO standard, which is also described in a concise way. The FP5 MOSES RTD project is then introduced, since it aimed at extending the OPIMA implementation (from IST OCCAMM) to achieve compliance with MPEG IPMP-X and, at the same time, to contribute to the development of this ISO standard. This was achieved with success and two of the technological results, that have integrated with the MOSES MPEG IPMP-X implementation, are then described, namely the open-source DRM platform, referred to as OpenSDRM - Open Secure Digital Rights Management and Music-4You, a digital music B2C e-commerce site, which were developed to prove the technological concepts behind MOSES, namely, the MPEG-4 IPMP-X implementation integrated into the OpenSDRM platform integration.

2. A Definition of DRM

A precise definition of DRM, Digital Rights Management, from the technical and economical point of views, can be found in [8]: "DRM systems are means of assigning access to digital contents. In other words, DRMs are, first of all, technological tools designed for excluding consumers from information goods, which, otherwise, would be public goods. In that function, they supplement intellectual property rights whose economic role is to provide incentives in intellectual creation by giving the owner a

temporary monopoly on exploitation. This is why DRMs frequently refer to *rights models* as to define the range of accesses they grant. By doing so, DRMs should also be considered as versioning tools, providing to each kind of content, a pre-defined set of utilities that grant liberality of content use: right to view (hear), modify, record, excerpt, translate in another language, keep for a certain period, copy, distribute, etc.". DRM systems, which are in fact technical private measures protecting copyright, enforce a contractual agreement between parties (e.g. content owners and end-users or subscribers), that fix the width of their rights and that can sometimes override copyright law and especially limitations to copyright law as fair uses[2]

3. The OPIMA initiative

OPIMA (Open Platform Initiative for Multimedia Access), an initiative of the Industry Technical Agreement (ITA) program of the International Electrotechnical Commission (IEC), was established[3] with the purpose of enabling a framework [7] where, content and service providers, would have the ability to extend the reach of their prospective customers and, consumers, would have the ability to access a wide variety of content and service providers in a context of multiple content protection systems.

The OPIMA specification included its architecture and a description of the functions required to implement an OPIMA-compliant system. Furthermore it included also security protocols and a description of Application Programming Interfaces (APIs) and functional behaviours that enabled interoperability (Figure 1).

---

[2] By fair use (a concept valid in the United States and defined in the US 1976 Copyright Act, S 107), we refer to cases such as time shifting, private backup copying or uses for educational purposes.

[3] OPIMA had its kick-off meeting in Turin in March 1998.

The OPIMA specification was device and content independent. Content was perceived to include all multimedia types and executables. OPIMA introduced the Rules concept, referred to information that stipulates how content may be used on a given device; specifically, Rules determined how business models should be established. OPIMA also created the concept of IPMP (Intellectual Property Management and Protection). An IPMP system controls access and use of the content by enforcing the rules associated with it (Figure 1). Conditional access systems were considered as particular examples of IPMP systems. In the Optima's vision, protected content consisted of the following:

- A content set, which may be composed of different multiple media types;
- An IPMP system set, which may consist of multiple IPMP systems;
- A set of rules that could be applied under the given IPMP system.

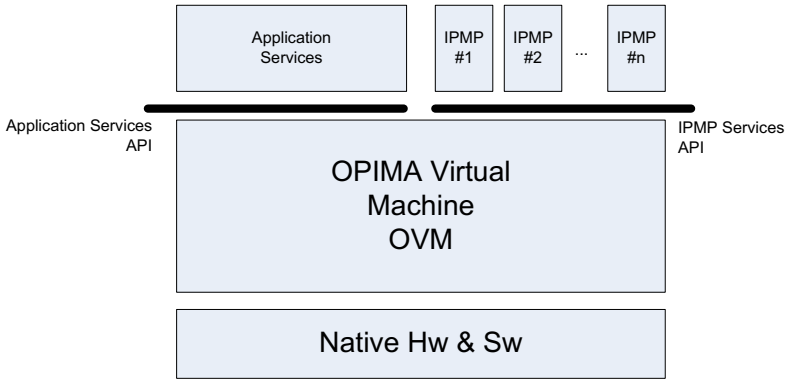

Figure 1 – The OPIMA architecture

OPIMA has finished its work in June 2000, by releasing version 1.1 of its specification [7]. In this specification, OPIMA defined the need for some building-blocks such as the OPIMA Virtual Machine (OVM) and the IPMP systems (Figure 1), as well as it recognized the need for back-end infrastructure and a set of trusted institutions (capable of credential issuance), but it did not specify how this back-end or institutions would have to be developed, how they have to work and how they interrelate with each other. The only normative part specified by OPIMA was the Application Services API and the IPMP Services API. Another normative part of OPIMA is the protocol definition

needed for the establishment of Secure Authenticated Channels (SACs) among OPIMA peers. One of the major components of OPIMA is the OVM. The OVM can be seen as a closed black-box that receives protected content and renders it. The only external communication points are service APIs.

4. Implementing the OPIMA vision

After the release of the OPIMA specification, the most active contributing organizations of the OPIMA initiative joined together and submitted an RTD project proposal to the IST programme in the EU FP5 framework. This proposal was named OCCAMM (Open Components for Access to Multimedia Material) and one of the most ambitious goals of it, was the implementation of the OPIMA vision and its specifications. This project was approved and started on January 2000 with the following objectives:

- The specification and development of a series of enabling tools and components, which were compatible with emerging standards and recommendations (MPEG, OPIMA, SDMI – Secure Digital Music Initiative), which would handle the controlled access, delivery, consumption, rights management and payment of multimedia content.
- The establishment of a number of commercially-driven applications that used the aforementioned tools, which would deliver the needs of all participants in the project.
- The definition and monitoring of performance levels in trial environments for such applications, pointing out additional actions needed for subsequent full and successful commercial exploitation.

OCCAMM targeted specific innovative developments in the most diverse areas:

- Open, secure user environment based on the OPIMA Virtual Machine concept and its implementation on a general purpose PC platform;
- Encryption and scrambling, key management and authentication techniques assembled to constitute complete IPMP systems in conformance to OPIMA and MPEG-4 specifications, with the capability of automatically tracking content usage as well as usage of copyrighted content processing technologies;
- Watermarking technologies targeted to the audio and video domain of application in monitoring, copy/access control and fingerprinting, conformant with MPEG-4, OPIMA and SDMI requirements;
- Copy Protection (CP) techniques;
- Content metadata insertion and processing tools.

The other two components in the OPIMA Platform, implemented by OCCAMM, were two Application Programming Interfaces (APIs): the Application Services API and IPMP Services API.

1. The Application Services API intended to be used by applications, which normally have some user interface. With this API, now available, upon user request, an Application can call a set of API methods to: query the OVM, download a given Intellectual Property Management and Protection System (IPMPS) (which will be executed by the OVM), send messages to the IPMPS and send the OVM instructions for Content usage. The Application Services API is implemented by the OPIMA platform and provides the sole entry points to an Application. Based on the answer from the OVM, the Application can ask the User to select a previously downloaded IPMPS, or ask the OVM to download, install and run a new content specified IPMPS. Apart from the API, nothing else is specified by OPIMA for the

Application, which can have any type of User Interface (e.g. Internet browser, TV remote control).

2. The IPMP Services API intended to be used by IPMPS. This currently available API provides a set of methods that allow the IPMPS to: request Content Rules and/or User Rules, access to the OVM encryption/decryption, signature and watermarking engines, access to smart-card interfaces, communication with the user (directly), with the application, and with remote IPMPS. Content is handled only by the OVM, however it is the IPMP system that takes the decision if a User is entitled to perform the action requested. This decision is taken by the proprietary code in the IPMPS based on Content Rules and User Rights. If affirmative, the IPMPS will provide the OVM with the keys, or the means to obtain them, that will allow decrypting the Content. At a given time, several IPMPS may be running in the multi-tasking environment managed by the OVM.

OCCAMM endorsed the complex task of implementing the first set of PC OPIMA Virtual Machines, the external API interfaces, the necessary IPMP tools, demonstration applications and the needed support infrastructure. This was achieved with success.

4.1. OCCAMM main results

One of the most impressive results of the OCCAMM project was the implementation of the OVM. As it was referred previously, the OVM acted as a black-box that had the necessary capabilities and mechanisms to render protected content. Once closed, this box could only communicate with the outside world via the services (Application and IPMP) APIs. One of the options made by the OCCAMM project was the type of content that the OVM was capable of rendering. The choice resided in MPEG-4 content – Advanced Audio Coding (AAC) Low Complexity Profile audio files [9] with Advanced Simple Profile (Levels L4 & L5) video files [10], including JPEG still pictures, all

wrapped in MPEG-4 File Format [10]. OCCAMM's OVM implementation received protected MPEG-4 content from external sources and was capable of rendering such content. The following picture (Figure 2) depicts the OCCAMM implementation of an OVM. OCCAMM defined its implementation based on the OPIMA specifications and on the analysis work carried by the project.

Some of the most important components of the OVM implementation were (Figure 2):

- Scheduler: this component was responsible for managing all the OVM operations, assuring that these were executed as they were supposed to be;
- Secure Authenticated Channel (SAC): this component was used to establish secure and authenticated channels with other OPIMA peers (using the Secure Sockets Layer (SSL) protocol). The SAC was used for downloading IPMP tools and user licenses;
- IPMP System manager: managing the IPMP systems that were present on the system was one of the main goals of this component;
- Content Registry: this component was in charge of registering the content on the OVM;
- IPMP services: this component provided all the services indicated by the OPIMA specification to the IPMP systems;
- Application services: this component provided all the services indicated by the OPIMA specification to the Applications;
- MPEG-4 player: this component was responsible for decoding and rendering the MPEG-4 content;
- Protection tools: the encryption and/or watermarking algorithms that were used to either decipher or fingerprint the content were directly implemented on the OVM. On the OVM there was not the possibility to renew the protection tools.

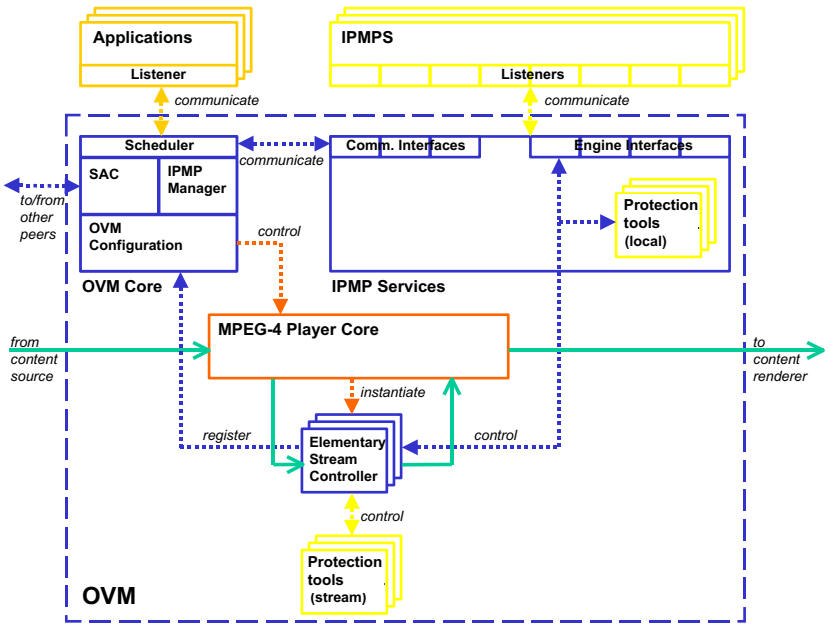

Figure 2 – OCCAMM's OVM architecture

Apart from the OVM implementation, OCCAMM also implemented two different IPMP systems, one smartcard-based and the other software-based. Also, a set of generic external elements that composed the supporting infra-structure were also developed: a License Server, an IPMP systems server and a Certification Authority. These latter components were suggested by the OPIMA specification but not specified. The License Server is the component that is responsible for issuing the licenses for content usage. The Certification Authority is used to issue the cryptographic credentials for the OPIMA peers, needed for the establishment of secure and authenticated channels between them. The IPMP systems server is the entity that supplies the needed IPMP systems to the OPIMA peers that need them to process the content. Additionally, for each of the trials performed within OCCAMM, a Content Preparation server and an E-Commerce platform were also developed.

4.2. OCCAMM tests and trials

The OCCAMM project consortium developed a series of trials in order to validate the OPIMA architecture. One of these trials was focused on the commercialisation of

protected digital music over an Electronic Commerce web-site and on controlling the access of such music content on the client platform.

OCCAMM provided a new mechanism for selling and distributing digital music recordings to consumers. This system combined the latest digital distribution technology, with developments in Internet multicasting, e-commerce and intellectual property management. The OCCAMM platform comprised five main components (Figure 3). These components were identified by OCCAMM as the necessary components to implement its business model and trials. The trials included the secure production, distribution and consumption of content along the value chain. The five components are as follows:

- The Electronic Commerce Platform (ECP) where orders for music products could be placed. It contained a full catalogue of all products for sale and enabled registered users to select products for distribution and authorise payment (note that payment facilities were dependent of the transaction model(s) deployed). Payment facilities included credit card payment, subscription management, micro payment and pay-per-view. The ECP also managed distribution scheduling for all products.
- The OCCAMM Service Centre contained all of the content available through OCCAMM in digital form. This centre also hosted the multicasting software required to distribute content to the users. The centre was located at the ground station of the satellite service provider used during the project. This removed the need for a high bandwidth link between this service centre and the ground station in order to distribute products following a user order. Instead, the centre was installed on the ground station LAN, facilitating rapid and economical delivery of the requested products via the satellite up-link facilities. Streaming software was also hosted on the OCCAMM Service Centre, which provided streaming services to

users. The services provided by OCCAMM were not limited to satellite delivery. It was envisaged that alternative distribution mechanisms would be also implemented for example, in ADSL and standard Internet distribution.

- A Client PC. Users wishing to use the OCCAMM service required a Client PC. This terminal facilitated the ordering, reception, management and consumption of digital content available via OCCAMM. Each consumer terminal required hardware (i.e. smart card reader) and software capable of performing the above functions. The OVM formed the core of the OCCAMM Client PC. Installed on the Client PC OVM were the IPMP Systems (IPMPS). The Content offered and distributed via the OCCAMM service was encrypted by an IPMPS. The IPMPS consisted of the server part (IPMPS License Server) and the client part. The server part was responsible for the creation, management and distribution of the licenses to the Client PCs. The Client part resided on the Client PC, which communicated with the IPMPS License Server via the OVM. All communications with the IPMPS (client and server parts) were secured using the OPIMA SAC.
- Production Station. This station consisted of a set of utilities, which prepared the content for distribution and use. These utilities included a watermarking encoder, an encryption system and an MPEG-4 audio/video encoder. All content prepared by the Production Station was transferred to the Multimedia Server Content Store via FTP (either standard internet connection, ISDN or Leased Line) for subsequent distribution to users. The music was encoded using AAC Low Complexity Profile [10] in MP4 File Format [11] which contained a scene composed by the music track and a JPEG image of the artist/album from which the music was originated. Therefore when the user opened the music track on the player, it also viewed the

image. Some video clips were also available encoded in Advanced Simple Profile, L4 and L5 Levels [9][11].

- Payment Gateway. This provided the OCCAMM system with the means to process payments for content purchased by users. For the purpose of the OCCAMM project, a Payment Gateway constituted either a bank/financial institution providing Electronic Commerce facilities, a Trusted Third Party providing payment services or a Micro payment system capable of processing transactions of small value. Any communication between the E-Commerce Platform and a Payment Gateway was secured via an SSL connection. This ensured any financial information being transferred between the two entities remained secure.

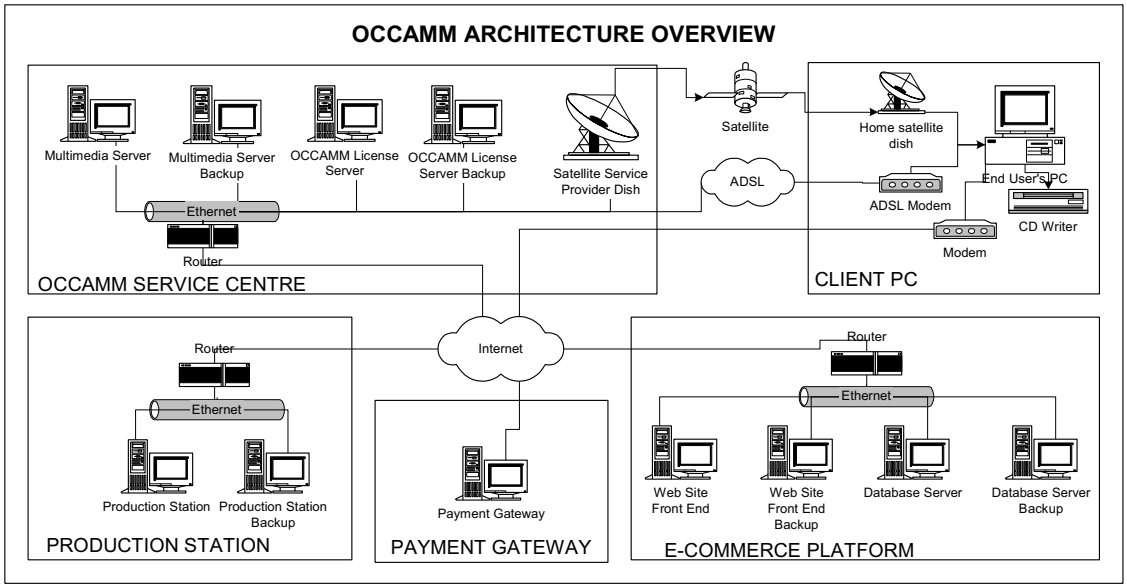

Figure 3 – OCCAMM trials architecture

5. MPEG IPMP

This section describes the standardisation work, carried under the MPEG auspices related to DRM. It starts by describing the initial efforts carried by MPEG, referred to as MPEG IPMP "Hooks" [12]. The section then presents the definition of the new standard, MPEG IPMP eXtensions [13][5], an evolution from MPEG IPMP "Hooks",

which shows a much higher level of interoperability than the “Hooks” specification in terms of both protection tools and business models.

5.1. MPEG IPMP “Hooks”

Meanwhile, almost at the same time that OPIMA released its first version of the specifications[4], the MPEG finalised its work on the IPMP “Hooks” [12, 14, 15].

In the IPMP “hooks”, a set of points in the decoding chain called Control Points were normatively defined; in each of them, a protection mechanism (called IPMP Systems) could be plugged in, to perform IPMP processing on the media data flowing from the decoding buffer down to the renderer (Figure 4). The time-varying information such as decryption keys, sync info, etc. could be delivered to the IPMP System through a dedicated stream called IPMP Stream [16].

The “IPMP hooks” provided the Intellectual Property Identification Data Set (IPIDS). This IPIDS could be used to associate various content identifiers with the audio-visual objects (AVO) contained in an MPEG-4 bit stream. The association of an IPIDS with AVO was accomplished through its addition into the AVO elementary stream descriptor. The MPEG-4 IPMP provided the “IPMP hooks” themselves which allowed proprietary DRM systems to be used within an MPEG-4-compliant terminal by associating the ID of an IPMP system with each AVO [16]. The uniqueness of this identifier was regulated by a registration authority. This identifier indicated which IPMP system governed the AVO. In addition to the IPMP system ID, MPEG-4 IPMP provided space for “private” data that IPMP systems could use to transmit any data they would need for its operation. The IPMP system ID and the private data for the IPMP

[4] The OPIMA specification v1.0 was published in 1999, while the second and final version v1.1 of the specification was published in 2000.

system could be associated with the AVO using the same mechanism used for linking the IPIDS to the AVO.

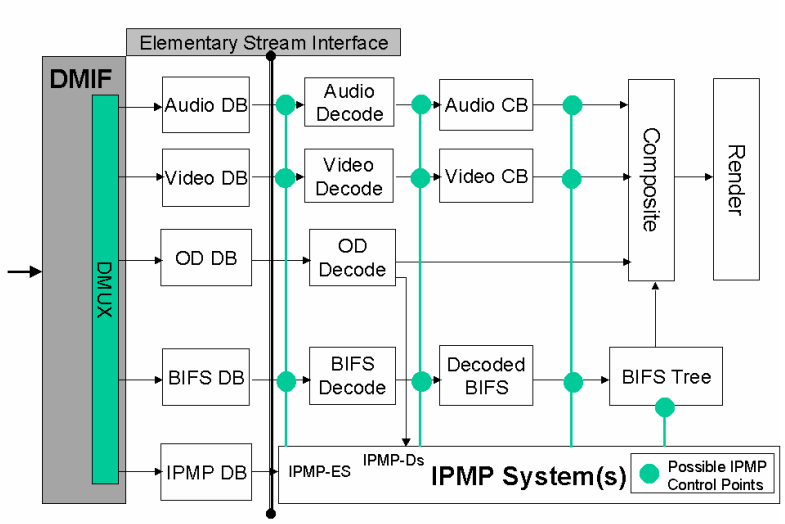

Figure 4 – MPEG-4 "IPMP hooks" architecture

The specification provided a second mechanism for associating IPMP system IDs and private IPMP data with AVO: adding an IPMP elementary stream into the bit stream allowing the synchronization of IPMP data with AVO. This was useful when using MPEG-4 streaming where IPMP information needed to be repeatedly sent to allow devices to start receiving and decoding content from arbitrary points within the bit stream. This mechanism also enabled a service provider to regularly change keys to the content, providing additional security levels [16].

IPMP "hooks" allowed several IPMP systems to co-exist on the same Terminal. According to the chosen protected content, the IPMP System specified by the Content Owner at authoring time would be instantiated. The IPMP System itself was proprietary. However, the following issues were left open by IPMP "hooks":

- There was no standard way to specify how an IPMP System can be "hooked" in a MPEG-4 player without previous agreement between MPEG-4 player manufacturers and IPMP System providers;

- There was no standard mechanism to allow IPMP Systems to authenticate each other;
- There was not easy provision to replace a “broken” IPMP system.

The MPEG-4 IPMP-eXtensions [13, 5], which are described next, were designed to answer the above “open questions” and to provide a more complete DRM architecture within MPEG and to do so in a secure manner.

5.2. MPEG IPMP Extensions

MPEG, recognizing the value of content both for content owners and users, has been active since 1998 in defining standard solutions in the DRM (Digital Rights Management) arena to regulate the access to MPEG content. As a result of this activity, MPEG has recently developed the Intellectual Property Management and Protection eXtensions (IPMP-X) specification [13, 5], which has been one of the last available DRM solutions to govern MPEG content throughout its life, providing a secure framework that can host any number of proprietary protection algorithms thus granting interoperability in respect of allowing end users to get content from different service providers protected with different DRM systems. .

The MPEG IPMP eXtensions do not “break” or otherwise negatively impact existing implementations based on the original “Hooks” specifications [13, 17, 18]. An identifier is defined in order to specify which IPMP solution is being used. MPEG-4 IPMP “Hooks” protected content may be accessed by a MPEG-4 IPMP-X terminal. MPEG-4 IPMP-X protected content will be conceived by an IPMP “Hooks” terminal as being protected by an unknown IPMP system [13].

The MPEG IPMP eXtensions is delivered in two flavours: MPEG-2 IPMP-X (Part 11) [19, 6] and MPEG-4 IPMP-X (Part 13) [13, 5]. MPEG-2 IPMP-X [6] is designed to be

applied to MPEG-2 based Systems [19]; MPEG-4 IPMP-X [5] is designed to be applied to MPEG-4 based Systems [13].

MPEG-4 IPMP-X (Figure 5, Figure 6) can be used to host any type of media protection at a varied level of granularity and complexity, as required by the specific DRM system employed to protect a given content within MPEG-4 Systems. MPEG-4 IPMP-X may protect any kind of media content included in an MPEG-4 stream, as for example video, audio, computer graphics, text, interactive contents, etc.

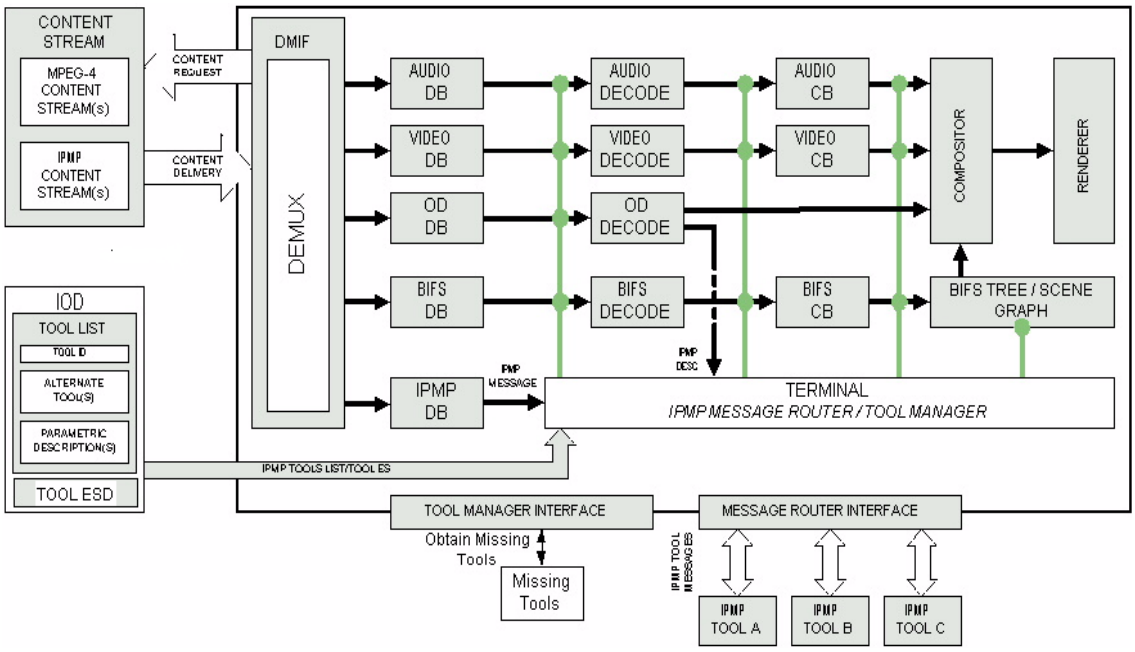

Figure 5 – MPEG-4 IPMP Extensions architecture

MPEG-2 IPMP-X [6] is provided in MPEG-2 Systems [19] with the same functionality and support as in MPEG-4 IPMP-X [13, 5]. MPEG-2 IPMP-X may protect any kind of content that can be inserted in an MPEG-2 transport stream, as for example video, audio, text, private streams, etc. IPMP-X can also be integrated in other non-MPEG based Systems easily, as long as these systems provide the appropriate integration APIs similar to MPEG IPMP “hooks”. Nevertheless this is something that the most popular media players (such as Windows Media Player, Apple iPod and other) don’t yet support

trying to monopolise the market by locking consumers and even governments into their proprietary DRM systems and trying to create “de facto” standards.

In 1997, MPEG issued a Call for Proposals for technology in the area of Intellectual Property management and Protection (IPMP). After receiving the proposals and the ensuing discussions, MPEG and the experts drawn to MPEG by the Call decided, in 1998, that it would not be appropriate to standardise complete systems, but that just providing the right interfaces (or ‘hooks’) would be were standardisation should stop. At that time it was believed that only a few IPMP Systems would emerge in the market, thus interoperability among them could take place using the “hooks” and complemented by bi-lateral agreements signed among the different IPMP System providers and players’ manufacturers. In 1998 and 1999, IPMP technology has matured, requirements for these systems have become clearer, and also MPEG’s understanding of the role of IPMP technologies in building interoperable devices and services has evolved. Also, it became clear that not all parties represented in MPEG were convinced that only providing the interfaces would be enough. Particularly, some parties were concerned about interoperability between different products, often for similar services, as developed within the IPMP framework of the MPEG-4 Standard. Also, with convergence becoming a reality, e.g. through the deployment of broadband Internet access and the start of new services on mobile channels, interworking between different types of devices and services becomes a more important requirement. It was the belief of these parties, that the existing MPEG-4 IPMP “hooks” Framework - with its demand for bi-lateral agreements among IPMP System providers and players’ manufacturers - did not provide the necessary infrastructure to meet their interoperability requirements. It is MPEG policy to support legitimate requests to standardise on a technology,

knowing that those not interested in that particular standard technology have no obligation to adhere to it because of conformance obligations [20].

In the eXtensions, a more mature level of technology and a clearer understanding of the role of IPMP technologies made the MPEG group come out with a solution which does not need bi-lateral agreements, granting far much more interoperability between different IPMP modules (called IPMP Tools) [5], by defining a message-based interface supporting the co-existence and communication between any pair of IPMP Tools and between them and the MPEG-4 player (Figure 5, Figure 6). Using normative messages, IPMP Tools can interchange any kind of information, including mutual authentication data, in order to ensure that the plugged-ins are the ones they claim to be and not "malicious", thus granting a secure operating environment [5].

When users request access to IPMP-X protected content, the MPEG-4 terminal processes the IPMP Tool List (Figure 5), a structure which specifies the IPMP Tools meant to govern the access to the content [5]. These are then located, (if not present locally can be downloaded from a supplied location), and instantiated by a conceptual entity within the Terminal: the Tool Manager. Another conceptual entity, the Message Router, takes care of routing information between Tools and terminal. This communication takes place by means of normative and user-defined messages (Figure 6). If mutual authentication succeeds, and all the conditions the IPMP Tools require are fulfilled, a Rights Management IPMP Tool checks the validity of the license associated to the content, and then processing of the individual elementary streams starts. As an example, a decryption Tool decrypts the content and sends it to the media decoder for that particular content. Then the media decoder decompresses the stream and passes it on to a watermarking Tool, which reads or writes the payload from/into the content and finally, passes it on to the renderer which will present it to the user (Figure 5).

Communication between the IPMP-X framework and IPMP Tools, or between any pair of IPMP Tools, is based upon a messaging framework (Figure 6). The specification defines a set of normative messages, which the IPMP Tools need to generate and send or interpret upon receipt, in order to be able to communicate with the other entities in the framework. These can be grouped in the following categories [5]:

- IPMP Tool Connection and Disconnection Messages: Used to instantiate and destroy logical instances of new Tools, and to allow Tools to find out information about other Tools;
- Event Notification Messages: To provide the IPMP Tools the ability to request and get notified of events such as connection or disconnection of other Tools, watermark detection, etc;
- IPMP Processing: Defined to be used in the IPMP process covering a wide range of scenarios, like conveying keys, usage rules, to communicate with an audio or video watermarking Tool, to configure selective encryption, and so on;
- Authentication Messages: Defined to verify the trust relationships existing between two entities (Tools or Terminal), and to determine or create secure channels of communication as needed, based on the application;
- User Interaction Messages: To allow information to be exchanged between the user and an entity requiring information from the User;
- Consumption Messages: To allow an IPMP Tool to notify the terminal about its consensus to process content or not;

In summary, the key advantages brought by IPMP eXtensions can be summarized as the following [21]:

- Interoperability: Thanks to the set of normative messages, interaction between different IPMP Tools is allowed;

- Security: Normative mutual authentication negotiation mechanisms are provided to ensure a secure operating environment;
- Flexibility: Free choice in choosing the algorithms (mutual authentication, protection such as encryption and watermarking, management, etc.) to govern the content;
- Renewability: Easy replacement of weak or old IPMP Tools.

IPMP-X, has finalized its specification in Oct 2003 [13, 5] [19, 6], and its reference software [17][22] and conformance testing suite [18][23] were ready by March 2004 [22, 17, 18]. Currently is being already adopted and supported by an increasing number of companies [24] and consortiums [25, 26], all over the world. The core technology of IPMP-X (Message router and Tool Manager) is also under discussion and consideration for adoption by MPEG-21 IPMP Components [27], Digital Media Project - DMP [28, 29], DVB TM-SEC and Audio-Video Coding Standard Group of China - AVS China. The key benefits brought to content owners, end users and industry, are believed to be able to revolutionize the whole experience of access to protected content.

6. MOSES and the IPMP-X Framework

MOSES (MPEG Open Security for Embedded Systems) was the natural evolution of the work already achieved in the IST OCCAMM project. Most of the organizations present in the MOSES project had already participated on the IST OCCAMM project. One of the MOSES goals was to extend the OPIMA interfaces and architecture to achieve compliance with the emerging security standards such as MPEG IPMP-X, helping to consolidate the integration of research and concertation of the projects in the field of Networked Audiovisual systems and Home Platforms and to develop visions and recommendations so as to foster consensus among the various stakeholders

(broadcasters, telecom operators, content and service providers, research and academic and users at large) on future industrial and research initiatives. Another aim of MOSES was to contribute to the specification [13, 5][19, 6], implementation (Reference Software) [17][22] and validation (Conformance Testing) [18][23] of the MPEG-2/4 IPMP-X concepts. The Reference Software and Conformance Library were developed in close collaboration between MOSES and Panasonic Singapore [30, 31].

The OCCAMM extension, through the MOSES project took place in three axes (download ability, secure environment and target applications) as can be seen in the following table (Table 1). This extension resulted in the MPEG-4 reference implementation of IPMP-X and is included in the MPEG-4 reference code [31].

Features	OPIMA	MPEG IPMP-X
Ability to download:	Rules/licenses & policy	Rules/licenses, policy and protection algorithms (encryption, WM, etc).
Secure environment based on:	Tamper resistance/ OPIMA compartment	Mutual Authentication allowing Tools to be linked together.
Targeting applications:	STB and mobile devices	Military, Government, D-Cinema to STBs and mobile devices.

Table 1 – Comparing OPIMA and MPEG IPMP-X

The OPIMA solution was the first to recognize the need to make content access rules (licenses) as much portable as possible but did not recognize the need of downloading protection components into the terminal, since was based on the assumption that only a few would emerge as “de-facto” standards and thus, it would be possible to accommodate them in an OPIMA “compartment” achieving interoperability. Another reason with respect to the latter issue was the consideration that the most security sensitive components were not the protection algorithms themselves but the key

management mechanisms. Thus, OPIMA also adopted the operation in a tamper resistance environment, assuming an environment capable of resistance against internal or external modifications by third parties, never allowing clear text content to be exposed outside of it.

Differently from OPIMA, MPEG IPMP Extensions was designed not only to be able to download protection components into the terminal, but to perform it in a secure way as well. This has been achieved by introducing Mutual Authentication negotiation mechanisms in the standard, allowing different protection components from competing vendors to co-work and interoperate. By not relying any more in tamper resistance environments, MPEG IPMP-X has also increased the number of application domains where the standard can be used, which has been also in line with the diverse range of applications that MPEG covers.

Due to the aforementioned reasons, the MOSES goal of extending the OPIMA vision to MPEG IPMP-X has been achieved in a such way that has not invalidated OPIMA, and can be seen as a conceptual profile of MPEG IPMP-X suitable for limited resources (portable) devices.

Comprehensively the main goals of IST MOSES can be synthesised in the following:

- Extension of the OPIMA interfaces and architecture to achieve compliance with the most recent ISO security standards;
- Extension of current business models to encompass operational scenarios where the full set of functionalities pertaining to IPMP systems have been implemented and tested;
- Porting the end-to-end MPEG-4 IPMP-X compliant secure infrastructure to devices other than the PC, addressing typical Consumer Electronic (CE) platforms based on open development suites.

6.1. MOSES main results

MOSES can be viewed as a success case in the scope of EU projects [32] since, according to its final review panel, it has achieved all the initially established objectives and has indeed addressed standardisation issues beyond the initial aims of the project. In fact, MOSES has established a strong relation with standardization activities, in particular MPEG and its stakeholders (broadcasters, telecom operators, content and service providers, research and academic and users at large), in order to help in achieving the development and implementation of the MPEG IPMP-X standard, the first Digital Rights Management related standard ever released by ISO (in 2003) and the single one published by ISO in the DRM arena, up to the writing of this paper[5].

MOSES has brought some differences, from the technological point of view, when compared with the previous OCCAMM project, both in terms of terminal-side technology and in the support of server-based DRM technology. Some of the new topics developed by MOSES were:

- The usage of IPMP Tools rather than IPMP Systems. While an IPMP System is a monolithic IPMP protection scheme which requires implementation dependant access to protected streams at required Control Points and must provide any intra-communication within an IPMP System on an implementation basis, the IPMP Tools are modules that perform (one or more) IPMP functions such as authentication, decryption, watermarking, etc. Conceptually the use of one or more IPMP Tools is combined to perform the functionality of an IPMP System. IPMP Tools, as opposed to IPMP Systems, are normatively identified as to which control

[5] ISO/IEC JTC 1/SC 29/WG 11 – MPEG-21 has issued a Call for Proposals in March 2004 "Requirements for MPEG-21 IPMP". Answers to the call were submitted [32] and the work on this new standard is on-going. The standard is in Committee Draft (CD) stage, at the time of writing of this paper.

points they function at as well as are provided normative methods for secure communications both within as well as outside of a given IPMP Tools comprised functional “IPMP System”. An additional difference between IPMP Tools and IPMP Systems is that IPMP Tools, or a combination thereof, may be used for the protection of Object streams.

- Better defined IPMP descriptors and associated system syntax structures;
- The existence of a Messaging Framework instead of an API definition, between IPMP Tools and the Terminal. This represented an evolution compared to the OPIMA specification which was API based, since messages can be secured with just a digital signature while interfaces require much more effort;
- An Abstract IPMP Control Graph that determines the structure of protection;
- An Authentication Framework that enables IPMP tools to perform mutual authentication with the terminal, in opposition to the OPIMA approach which was based on a closed tamper resistance environment;
- The development of an integrated server-based DRM platform, composed of several distributed components capable of fulfilling a specific role in the media chain, based on open standards and open-source technology.

The main MOSES results could be synthesised on the following:

- Close collaboration with ISO in the development and implementation of the MPEG-2/4 IPMP-X standard, namely, help achieving "consensus" and contribution in specifying, implementing (Reference Software) and validating (Conformance Testing) the MPEG-2/4 IPMP-X. It was the first ever implementation of IPMP-X;
- Development of a set of content players and integration of the MPEG-2/4 IPMP-X to several platforms (PC, PocketPC hand-held device and Symbian based mobile

devices). This represented the first implementation of media players, for several platforms IPMP-X capable;

- Development of an open-source DRM architecture to manage the content rights, referred to as OpenSDRM, **Open S**ecure **D**igital **R**ights **M**anagement;
- Development of an e-commerce web-site for digital music acquisition and consumption, referred to as Music-4You [33], which has demonstrated successfully the MOSES developed DRM technology.

6.2. The MOSES MPEG IPMP-X implementation

Regarding the MOSES MPEG IPMP-X implementation, the work consisted in the integration of the MPEG-4 IPMP-X in the IM-1 MPEG-4 standard reference player and in the deployment of a number of example IPMP Tools. The software was developed for the PC and an optimised version was deployed for the PocketPC and Symbian mobile phone environments.

While binary normative messaging interfaces have been used in MOSES for integration with any MPEG-4 player (Figure 6), the equivalent interfaces have also been implemented in Syntactic Description Language (SDL) for conformance reasons with IM-1 MPEG-4 reference player rather than updating the latter [34][35]. Translation modules among SDL based messages and binary ones have been also developed .

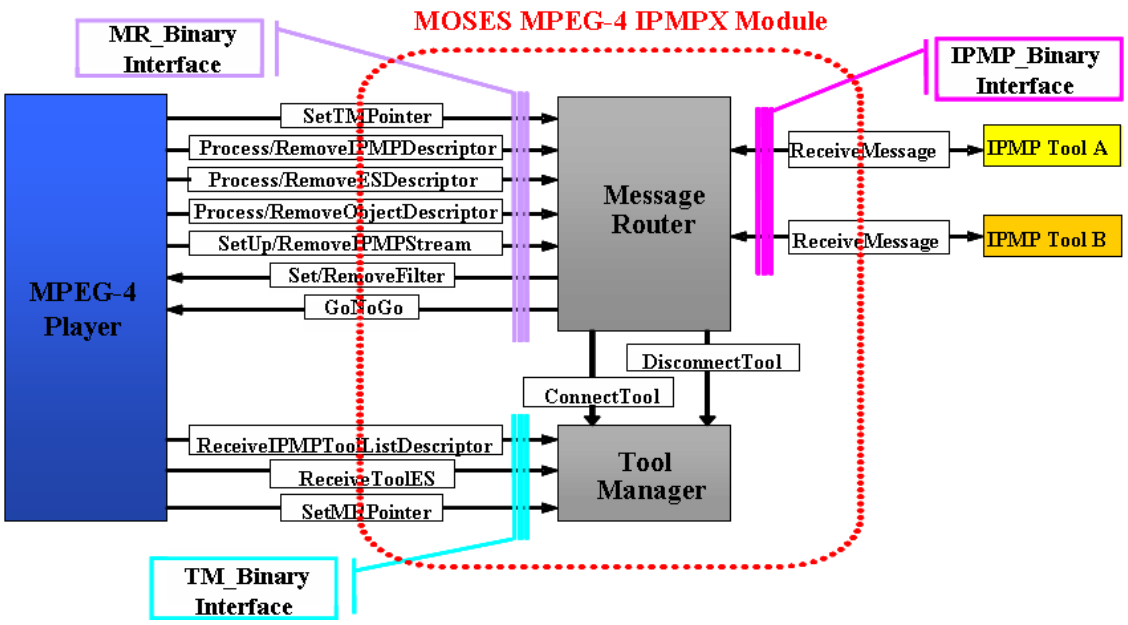

Figure 6 – MOSES MPEG-4 IPMP-X implementation architecture

One major deviation from the former OPIMA IPMP philosophy was the usage of a Message Router (MR) instead of OPIMA standardized APIs. This MR was capable of routing messages from the IPMP tool to the player and Tool Manager and vice-versa. The Tool Manager (TM) was responsible for the instantiation of the appropriate IPMP tools on the system which are needed to render the content . For more details on MPEG-4 IPMP-X and its MOSES implementation the interested reader should also refer to [36] and [35], respectively.

6.3. OpenSDRM, Open Secure Digital Rights Management

The MOSES MPEG IPMP-X module, was integrated in a broader technological platform, addressing all the issues of Digital Rights Management. This led to the development of an open-source DRM architecture to manage the content rights, referred to as OpenSDRM, Open Secure Digital Rights Management.

The OpenSDRM architecture was developed taken in mind that it could be adapted for use with several business models and different types of content, aiming at enabling business involving multimedia content to function, by enforcing licensing agreements

for content use and offering business opportunities to the content rights owner and content provider. At the time of development, various players and approaches in the DRM arena were already in place. One of such approaches addressed the DRM interoperability problem between different actors of the value chain by defining one unique media format and one type of technical solution used by every device. The format may be proprietary or open. The Open Mobile Alliance (OMA) [37] has targeted the DRM support for mobile phones and appliances, using an open specification. For the broadcast area and the home network Digital Video Broadcast DVB-CP/CPT [38] is an on-going step towards the standardisation of a Content Protection and Copy Management System, within the home network. Other vendors [39, 40, 41], are developing their own vertical strategies, that is, they are seeking and competing to establish a "de facto" standard in the DRM arena. Contrary to these efforts, the OpenSDRM DRM implementation, as followed a horizontal approach (in opposition to the vertical one described before). In this approach, the implementation has followed the guidelines and specifications of open standards, which address the DRM interoperability by defining common interfaces, tools and mechanisms that different DRM solutions should comply. To this aim OpenSDRM has provided support to the following standards:

- Open Digital Rights Language (ODRL/OMA profile), a language for rights expression [42] derived from an international effort aimed at developing and promoting an open standard for the Digital Rights Management expression language which has been adopted by OMA;
- MPEG-21 Rights Expression Language (REL), developed by MPEG-21 [43];
- MPEG-2/4 IPMP Extensions (section 4.2).

OpenSDRM is also based on the emerging Service oriented Architecture (SoA) of the W3C consortium (this SoA is composed by three major components: SOAP - Simple Object Access Protocol [44], WSDL - Web Services Description Language [45] and UDDI - Universal Description, Discovery, and Integration [46]).

This DRM solution is composed of several optional elements, as depicted in Figure 7, covering the content distribution value chain, from content production to content usage. It addresses several major aspects of the content distribution and trading: content production, preparation and registration, interactive content distribution, content negotiation and acquisition, strong actors and user's authentication and conditional visualisation/playback of content. OpenSDRM defines a distributed architecture in which every component can be separated. This allows the possibility to the architecture to be flexible to the addition of new components or the substitution of same components with new ones supporting different functionalities, or the integration of the DRM platform with third party networked systems and services. These components can all work side by side as long, as the defined integration point is respected (defined by WSDL). The communication between the single components will usually take place within insecure networks. Furthermore the components communicate with a text-based protocol (eXtensible Markup Language, XML). This introduces special needs regarding the security of this type of communication.

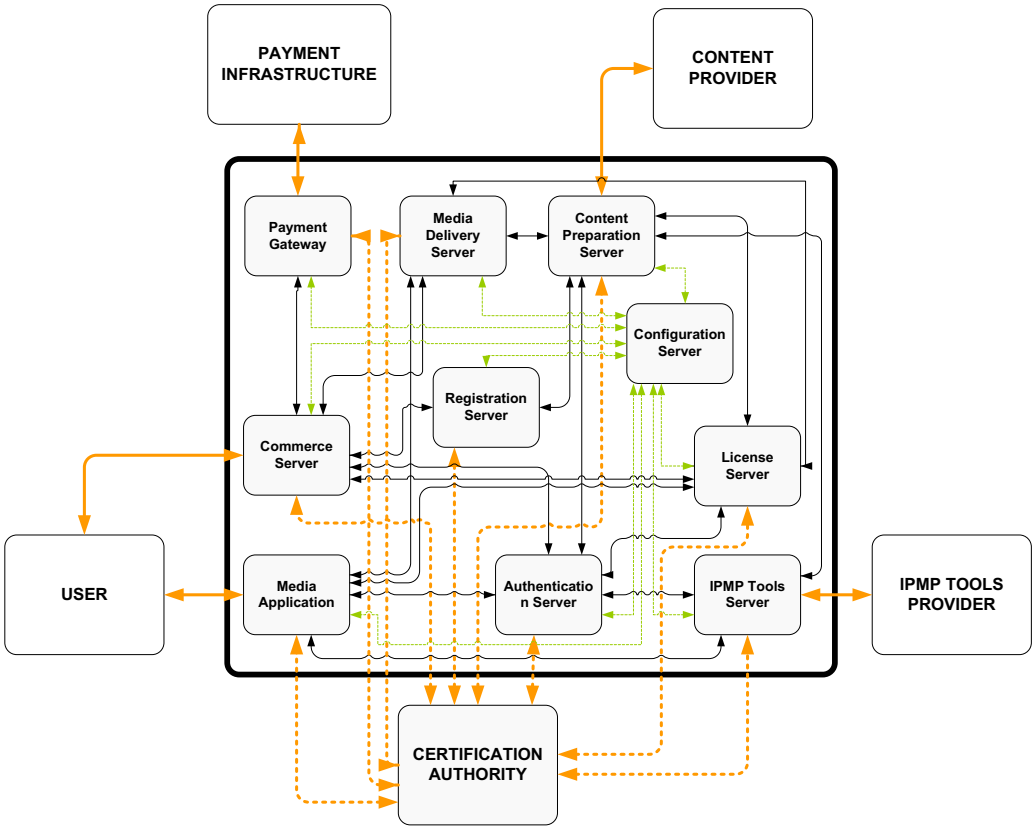

Figure 7 - OpenSDRM general architecture

Even though the MOSES project has addressed MPEG-4 content, the OpenSDRM infrastructure was designed with the concern to be adaptable and applicable to all types of content, business models and distribution channels (download, super-distribution, streaming or even broadcasting). The next sections detail the External Components & Interfaces and the Internal Components & Interfaces of OpenSDRM.

6.3.1. External Components & Interfaces of OpenSDRM

This sub-section will present in detail the components and actors that may interact externally with the OpenSDRM architecture, namely, the User, the IPMP Tools Provider, the Content Provider, the Payment Infrastructure and the Certification Authority.

- The User represents a person who wishes to consume a piece of content. This content may or may not be protected. However the way to access and display such

content may require the use of protected devices, software and licenses. The user will make requests to Open SDRM in order to: identify him, download licenses and play multimedia using a Media Player, embedded or not on a web browser. In a final analysis, the User interaction with OpenSDRM will always result in one of two things: either the user can play/render the content and enjoy it or he/she cannot; being then informed of the reason for this prevention.

- The IPMP Tools Provider is any organization that produces tools and technologies for encryption, scrambling, watermarking and others that can be applied to content protection. These tools will be made available to OpenSDRM for use in content rights protection. These tools will need to comply with some guidelines. These guidelines and a subscription, are translated into a business relation that must exist between a given Content Provider and the IPMP Tools Provider, since mostly, a given producer and/or distributor of content, may want to choose which type of protection the content will have and, respectively, which tools can be applied to the content and from which supplier.
- The Content Provider is any multimedia content supplier that feeds OpenSDRM with content and optional metadata. The content can be complex multimedia content that is ready for distribution, or simple content, for example JPEG images, that can be edited and combined with other content. As mentioned, the MOSES project has addressed MPEG-4 content.
- The Payment Infrastructure facilitates OpenSDRM e-commerce features by providing services for handling electronic payments. The interface between OpenSDRM and the Payment Infrastructure is generic and independent of the payment method, allowing therefore a multiplicity of payment systems.

- The Certification Authority is responsible for receiving requests for and issuing credentials to entities. These credentials will be used by entities to authenticate themselves to each other, allowing the establishment of secure and authenticated communication channels between them. All the components in the OpenSDRM architecture communicate using the channel security provided by the SSL/TLS protocol. This Certification Authority may be internal to OpenSDRM, and therefore entirely managed by some entity, or it may be an external commercial Entity.

6.3.2. Internal Components & Interfaces of OpenSDRM

In this part, the internal components of the OpenSDRM platform and the corresponding interfaces are presented. These components include: Media Application, Media Delivery Server, Commerce Server, Authentication Server, License Server, IPMP Tools Server, Registration Server, Content Preparation Server, Payment Gateway and the Configuration Server.

- Content Preparation server (CPS): this server component is responsible for the content preparation. It receives raw content from a specified source or sources and encodes it on a specified format, adds metadata and protects it. Under the MOSES project, content has been encoded in MPEG-4 format, according to some pre-established templates. These templates will allow the creation of MPEG-4 files containing music files in MP3 or AAC format together with some JPEG images about the album and artist.
- Configuration Server (CFS): this component is responsible for the storage and management of the locations of all the other components in the system. Any component that joins the system publishes its own location on the CFS so that other components can interact with it whenever they need to.

- Payment Gateway (PGW): is a server component responsible for verifying and validating the payment methods provided by the User for a Commerce Server;
- Commerce server (COS): is a server component responsible for trading the content with the users. Normally, content is chosen via web browser, some very generic metadata might be consulted, information about the price is also available, and especially the content usage conditions might be established.
- Media Delivery server (MDS): is a server component responsible for exchanging pieces of content with the client. This Media Delivery server will implement a specific protocol (download: FTP, HTTP or other; streaming: RTSP or other; broadcast) to exchange protected content with the client Media Application.
- Registration server (RGS): is a server component whose role is to assign unique identifiers to content and to register metadata information for that specific content. This architecture was designed to be as close as possible to ISO standards and therefore, for this unique ID, OpenSDRM follows the MPEG-21 directives about Digital Item Identification (DII) [47], using a reduced version of the MPEG-21 DII Digital Object Identifiers (DOI) [47].
- Authentication server (AUS): is responsible for authenticating all the internal and external entities to the DRM system. It validates the access rights of all the entities and components in the system working as a SSO point, registering and managing components and users on the system. It uses cryptographic XML credentials to authenticate both components and users in order to authenticate the transactions exchanged between them (XML Encryption and XML Signatures).
- License server (LIS): is a server component responsible for house-keeping the rules associating a user, the content and his/her corresponding access rights. This component will accept connections from authenticated Media Players clients for

downloading of licenses, which will be applied to the protected content through an appropriate IPMP tool. The licenses are XML formatted using Open Digital Rights Language (ODRL/OMA profile) [42] or the Rights Expression Language (REL), developed by MPEG-21 [43]. Although these two languages are used for the same functionality – rights' expression – they still don't interoperate. However, there is ongoing work to create bridges between ODRL and MPEG-21 REL [48] and achieve interoperability between them.

- IPMP tools server (ITS): is the server component responsible for registering new IPMP tools and for receiving authenticated client Media Application requests for the downloading of a specific IPMP tool. It is also responsible for making IPMP tools available to the Content Preparation Server to allow the protection of content.
- Media Application (MPL) This component represents the software that will be used to render the content. This is a generic component with the particularity of being able to display/playback the appropriate content for which the necessary audio/video codec should be available (if this codec is not available it must be downloaded from a remote secure server). This Media Application may work with one or several IPMP tools in order to control how the content is accessed by a particular user. This component works on the client side of the general architecture; however it plays an important role in the DRM functions. The Media Application design is fully compatible with the IPMP-X design and took in consideration that content can be exchanged on-line and off-line as well, since it supports the "Tools in Content" functionality where Content, Tools and Licenses can be packaged and distributed i.e. via Bluetooth together to a certain device.

6.4. MOSES User Trial – Music-4You.com

The Music-4You web-site (www.music-4you.com), a digital music B2C e-commerce site, was developed to prove the technological concepts behind MOSES, that is, the MPEG-4 player IPMP-X implementation and the OpenSDRM platform integration. The content format adopted for this music web-site was Advanced Audio Coding (Low Complexity Profile) wrapped in MPEG-4 File Format. Thus a specific IPMP-X enabled MPEG-4 music player was developed and distributed to selected users, during the project lifetime.

Music-4You was developed with the purpose to be a music portal, directed for two types of final users: consumers that wanted to listen to music and to music bands (music providers). The portal aggregates the work of several bands, allowing them to disseminate their work on the Internet with little effort and investment, with the possibility to protect their content according to their wishes by filling on-line forms. On the other hand consumers, could access to a large set of free music and to non-free music previews and downloads.

Another important Music-4You characteristic is that its business model was built on the concept that protected content had no intrinsic value. This seems contradictory with MOSES objectives. However what it really means is that users may download the content they want from the web-site, share it with their friends on P2P networks and publish the content on web-sites and so on, because content is protected (ciphered). Therefore content by itself has no “real” value. What confers value to the content are the associated licenses (which contain associated rules of content usage and the corresponding decryption keys) personalized for a given user. This license is to be used by the MPEG-4 player and the appropriate IPMP tool, which enforces the rules on the content and uses the appropriate deciphering key to render it. The licenses used by

Music-4You are count-based and time expiry-based. However, many other usage conditions could be added to the licenses, which can be expressed in ODRL or in MPEG-21 REL [49].

MOSES targeted not only the PC as the final device, but also embedded devices, such as hand-held PDAs and Mobile Phones. The same architecture, with the proper adaptations, tackled all these devices to provide the same functionality – the possibility to listen to music and at the same time uphold the rights of the copyright owners. A specific Music-4You portal (Figure 8) was developed also for small screen rendering devices, such as PocketPCs.

Figure 8 – Music-4You main web-page

Music-4You has brought clear innovations, as a music portal, if we compare it with similar ones in operation on the WWW in the end of 2003 [40]. The main innovations are listed bellow:

- Deployment of the first MPEG-4 IPMP-X based application: it was the first time that an MPEG-4 IPMP-X based application was deployed and tested on a trial, open to the Internet community in general, where users could experience controlled access to music[6];
- Contrarily to other solutions, and due to obvious commercial limitations, Music-4You targeted a music market niche composed mainly of amateur music bands, that could upload their own music tracks and made them available on the Music4You portal. The musicians were also responsible for defining all the information they would like to publish on the portal, associated to their content, for which they owned the exclusive rights;
- The Music-4You portal allowed the possibility for users to define the music access contractual conditions, varying the final price according to the versioning choices made. This was identified as a more flexible business model than the one that has been presented by most music-stores available on the web, in which a price table is fixed [40] [41].
- The music obtained via download from Music-4You was completely ciphered. Any attempt to listen to it without the appropriate license resulted in frustration. Therefore the Music-4You portal could be seen not as a mere place for buying music, but rather a place where users could buy licenses that would grant the rights to access a certain version of the music. This set-up enabled users to share their own music tracks with others (even on P2P networks) without copyright infringement. Any user willing to listen to the a music track would necessarily had to acquire a license from the portal.

[6] Eighty users have participated in the controlled Project trails and more than 500 (general public) have accessed the site during the short period (end of 2003), when the Music-4You portal was up and running.

- Finally, the portal supported the possibility to enjoy the same content on multiple devices, such as PCs and Pocket PCs.

7. Conclusions

The present document provided an overview of the evolution of the standardization work related to copyright protection of digital content and Digital Rights Management, starting from OPIMA, through ISO MPEG IPMP “Hooks”, towards the development of the ISO MPEG IPMP-X standard. Two European IST FP5 R&D projects – OCCAMM and MOSES were introduced, which have been working inline with the standardization bodies, such as MPEG. The paper explained how strong and important is the symbiotic relation between standardization efforts and public European funding of clearly focused R&D programmes. We have shown that IST OCCAMM and MOSES have provided a significant contribution, both in terms of knowledge and technological products, which will eventually help to strengthen the European presence in the digital content market. The authors believe that market actors should harness the ability inherent in DRM of not just preventing unauthorized uses but also of enabling new business models in service and content provision. The content and distribution sectors have begun to experiment with new distribution, pricing and revenue models and will eventually settle on the ones best suited for mass-market consumption of protected content over connected devices and networks. Interoperability of media solutions (formats and DRM), from multiple vendors (such as the ones referenced in section 6.1.2.1), needs to be achieved so that users can rely on the assumption of being able to consume the services and content they may choose, from the consumer electronics equipment available to them. All the industry sectors agree that industry-led standards-based solutions offer what is seen as the best eventual outcome, but standards take time to

develop and implement. It is important that DRM ensures and enhances consumer choice and competition. Therefore, the European Commission should continue to foster deployment of open standards [50] by continuing to support the work of MPEG, OMA, DVB and perhaps most importantly, the work by DMP [51][52][53][54] being the last hope of digital media consumers [55] worldwide to break the currently offered "walled gardens", while blossoming horizontal and interoperable markets of digital media and other relevant standards bodies and appropriate fora through European Collaborative R&D programmes. Possible options for further consideration may include:

- RELs translation i.e. OMA REL vs MPEG-21 REL and/or the ability to download the client of the required REL interpreter;
- Conformance with open, transparent, and clear criteria of end user devices to specified trust levels, perhaps by defining and applying a profile of Common Criteria [56][57];
- Rules for governance of trust authorities and agencies and their role in society.

8. References

[1] IFPI, "The recording industry commercial piracy report 2004", IFPI, http://www.ifpi.org, 2004

[2] IFPI, "IFPI:05 Digital Music Report", IFPI, http://www.ifpi.org, 2005

[3] OCCAMM web-site, http://sharon.cselt.it/projects/occamm/

[4] MOSES web-site, http://www.ist-moses.org/

[5] ISO/IEC 14496-13:2003, Information technology -- Coding of Audio-Visual Objects -- Part 13: IPMP Extensions

[6] ISO/IEC 13818-11:2003, Information technology -- Generic coding of moving pictures and associated audio information -- Part 11: Intellectual Property Management and Protection (IPMP) on MPEG-2 systems

[7] “OPIMA Specification version 1.1”, 11th Meeting, Turin, 2000

[8] Bomsel O., Geffroy A., “Economic Analysis of DRMs”, Deliverable DB.5.14_Economic analysis of DRMs_V1_0, PF6 IST MEDIANET, December 2004.

[9] ISO/IEC 14496-2:2001, Information technology -- Coding of Audio-Visual Objects -- Part 2: Visual, 2nd Edition 2001

[10] ISO/IEC 14496-3:2001, Information technology -- Coding of Audio-Visual Objects -- Part 3: Audio, 2nd Edition 2001

[11] Pereira F., Ebrahimi T. (editors), “The MPEG-4 Book”, Prentice Hall, July 2002

[12] ISO/IEC 14496-1:1999 (MPEG-4 Systems 1st Ed.)

[13] ISO/IEC 14496-1:2003, Information technology -- Coding of Audio-Visual Objects -- Part 1: Systems, Amendment 3: IPMP Extensions

[14] ISO/IEC 14496-1:2001 (MPEG-4 Systems 2nd Ed.)

[15] ISO/IEC 14496-1:2004 (MPEG-4 Systems 3rd Ed.)

[16] Lacy J., Rump N., Shamoon T., Kudumakis P., 'MPEG-4 Intellectual Property Management & Protection (IPMP) Overview & Aplications', AES 17th International Conference on 'High Quality Audio Coding', Villa Castelletti, Signa, Italy, Sept. 2 - 5, 1999. J. Audio Eng. Soc., Vol. 47, No 5, p. 392, May 1999

[17] ISO/IEC 14496-5:2004, Information technology -- Coding of Audio-Visual Objects -- Part 5: Reference software, Amendment 4: IPMP Extensions reference software

[18] ISO/IEC 14496-4:2004, Information technology -- Coding of Audio-Visual Objects -- Part 4: Conformance testing, Amendment 4: IPMP Extensions conformance testing

[19] ISO/IEC 13818-1:2003, Information technology -- Generic coding of moving pictures and associated audio information -- Part 1: Systems, Amendment 2: Support of IPMP on MPEG-2 systems

[20] MPEG Requirements Group, "Call for Proposals for IPMP Solutions", ISO/IEC JTC1/SC29/WG11 N3543, Beijing, China, July 2000

[21] Ming J., Chiariglione F., Alberti C., Kudumakis P., Kaneko I., Schultz C., "MPEG IPMP Extensions FAQ WD 1.0", ISO/IEC JTC1/SC29/WG11 N5790, Trondheim, Norway, July, 2003

[22] ISO/IEC 13818-5:2004, Information technology -- Generic coding of moving pictures and associated audio information -- Part 5: Software simulation, Amendment 2: MPEG-2 IPMP reference software

[23] ISO/IEC 13818-4:2004, Information technology -- Generic coding of moving pictures and associated audio information -- Part 4: Conformance testing, Amendment 1: MPEG-2 IPMP conformance testing

[24] IBC'03 Press Release, "Industry join forces to support MPEG's Intellectual Property Management and Protection Extensions Framework", International Broadcasting Convention (IBC'03), Amsterdam, The Netherlands, Sept. 12-16, 2003, http://avalon.cselt.it/projects/moses/Public/docs/IPMPX%20PressRelease.pdf

[25] Internet Streaming Media Alliance (ISMA), "Encryption and Authentication Specification v1.0", Mountain View, CA, USA, Feb. 2004

[26] Koike M., Kogure T., Sonehara N. on behalf of the Japanese Digital Cinema Common Specification Development Committee (DCCSDC), "Digital Cinema

Distribution Using MPEG-2 IPMP - Implementation Report and Issues of Feasibility", ISO/IEC/JTC1/SC29/WG11/M11614, Hong Kong, CN, Jan. 2005

[27] Serrão C. (ADETTI), Kudumakis P. (CRL) and Alberti C. (EPFL) "Joint answer to the MPEG-21 IPMP CfP" on behalf of MOSES, ENTHRONE and MEDIANET EC IST projects, Ref. as ISO/IEC JTC1/SC29/WG11/M10854, Seattle, U.S.A., July 2004

[28] L. Chiariglione, "Interoperable DRM Platform (IDP), Interoperable End-user Devices (IED) and short-term IED (IED-s)", DMP, 4th April 2004, http://www.chiariglione.org/contrib/040404chiariglione01.htm

[29] Chiariglione F., Kudumakis P. on behalf of MOSES EC IST project, "Distribution of digital content", Digital Media Project, Contribution No 56, Los Angeles, U.S.A., April 2004

[30] Ming J., Schultz C., Kudumakis P., "Text of ISO/IEC 14496-5:2003/FDAM 4 (MPEG-4 IPMPX Reference Software)", Ref. as ISO/IEC JTC1/SC29/WG11/N6244, Waikaloa, USA, Dec. 2003

[31] Chiariglione F. (CRL), Kudumakis P. (CRL), Alberti C. (EPFL), Romeo A. (EPFL), Balestri M. (TILAB), Trindade J. (ADETTI), Ming J. (PANASONIC), 'MOSES implementation of MPEG-4 IPMP Messages - version 1.1', Ref. as ISO/IEC JTC1/SC29/WG11/M10042, Brisbane, Australia, Oct 2003. This contribution (software library and documentation) consists in the core conformance library and, as such, has been integrated in the following standards: MPEG-2 IPMP Reference Software (N6064) and MPEG-2 IPMP Conformance (N6062) MPEG-4 IPMPX Reference Software(N5818) and MPEG-4 IPMPX Conformance (N6065)

[32] "EU Funding Opens Up 'On Line' Music For The Masses", London, FP6UK, Oct. 28, 2004, http://fp6uk.ost.gov.uk/page.aspx?sp=2228

[33] Music-4You web-site, http://www.music-4you.com

[34] Chiariglione F., Kudumakis P., Balestri M., 'MPEG-4 IPMP-X MOSES Interfaces', Ref. as ISO/IEC JTC1/SC29/WG11/M9780, Trondheim, Norway, July 2003

[35] Chiariglione F., Kudumakis P., 'MPEG-4 IPMP Extensions for application developers' in 'A User's Guide to MPEG Standards', to be published by British Standard Institute, London, UK, 2005

[36] Senoh T., Ueno T., Kogure T. (Matsushita Electric Industrial Co., Ltd.); Shen S., Ji M., Liu J., Huang Z. (Panasonic Singapore Laboratories Pte Ltd.); and Schultz C. (Multimedia Architectures), “DRM Renewability and Interoperability”, IEEE Consumer Communications and Networking Conference (CCNC’04), Las Vegas Nevada, USA, 5-8 Jan. 2004

[37] OMA, Open Mobile Alliance, http://www.openmobilealliance.org/

[38] DVB TM CPT Copy Protection technical, http://www.dvb.org/index.php?id=62

[39] Microsoft, “Architecture of Windows Media Rights Manager”, Microsoft Corporation, http://www.microsoft.com/windows/windowsmedia/howto/articles/drmarchitecture.aspx, May 2004

[40] Lenzi R. et al, “Apple iTunes Music Store”, technical report, The Interactive-Music Network, June 2003

[41] RealNetwork Rhapsody, http://www.real.com/rhapsody/

[42] “Open Digital Rights Language (ODRL) Version 1.1”, W3C Note, September 2002, http://www.w3.org/TR/odrl/

[43] ISO/IEC 21000-5 Information technology -- Multimedia framework (MPEG-21) -- Part 5: Rights Expression Language

[44] SOAP, Simple Object Access Protocol, http://www.w3.org/TR/soap/

[45] WSDL, Web Services Description Language, http://www.w3.org/TR/wsdl

[46] UDDI, Universal Description, Discovery, and Integration, http://www.oasis-open.org/committees/uddi-spec/doc/tcspecs.htm#uddiv

[47] ISO/IEC 21000-3 Information technology -- Multimedia framework (MPEG-21) -- Part 3: Digital Item Identification

[48] Polo, J., Prados, J., Delgado J., ”Interoperability between ODRL and MPEG-21 REL”, First International ODRL Workshop. Vienna (Austria), April 2004

[49] “ContentGuard and Central Research Laboratories collaborate to provide support for MPEG-REL within MOSES”, Bethesda, MD, U.S.A., Sept. 16, 2003, http://www.contentguard.com/press_091603.asp

[50] High Level Group on Digital Rights Management, Final Report , March-July 2000, http://www.fep-fee.be/drm.htm

[51] Digital Media Project web-site, http://www.dmpf.org

[52] Chiariglione F., Kudumakis P. on behalf of MOSES EC IST project, “Distribution of digital content”, Digital Media Project GA2, Contribution No 56, Los Angeles, U.S.A., April 2004

[53] Serrão C. (ADETTI), Dias M. (ADETTI), Trindade J. (ADETTI), Fonseca P. (ADETTI), Kudumakis P. (CRL), Chiariglione F. (CEDEO) “Answer to the DMP CfP (DMP0145) for Portable Audio and Video Devices (OpenSDRM)”, Digital Media Project GA4, Contribution No 0216, Barcelona, Spain, Oct. 2004

[54] Kudumakis P. (inAccess Networks), “Answer to the DMP CfP (DMP0328) for Stationary Audio and Video Devices: A unified approach to interoperable DRM Systems by merging UPnP and the MPEG-2/4/21 IPMP family of standards for PAV & SAV DMP”, Digital Media Project GA6, Contribution No 0392, San Diego, U.S.A, April 2005

[55] Chiariglione L., “Collection of TRU Templates”, Digital Media Project, DMP0270rev1, 2004

[56] National Institute of Standards and Technology, Computer Security Resource Center, Common Criteria web-site, http://csrc.nist.gov/cc/

[57] Common Criteria Portal web-site, http://www.commoncriteriaportal.org/