



<http://virtualgoods.tu-ilmenau.de/2004/>

Reviewed Papers

Virtual
Page
Numbers

Session 1: Watermarking for Virtual Goods

1. **StirMark and profiles: from high end up to preview scenarios** 1-12
Andreas Lang, Jana Dittmann,
http://virtualgoods.tu-ilmenau.de/2004/virtual_goods_2004_LANG_DITTMANN.pdf
2. **Synchronization of Video Watermarks for Oblivious Detection after Geometrical Distortions** 13-23
Uwe Wessely
<http://virtualgoods.tu-ilmenau.de/2004/wmsync-VG04.pdf>
3. **Complexity Optimization of Digital Watermarking for Music-On-Demand Services** 24-35
Martin Steinebach, Sascha Zmudzinski
http://virtualgoods.tu-ilmenau.de/2004/watermarking_music_on_demand_steinebach_vg2004.pdf

Session 2: Culture and Business for Virtual Goods

4. **On-line music distribution: a case study** 36-46
Francis Rousseaux, Alain Bonardi, Romain Poncelet
http://virtualgoods.tu-ilmenau.de/2004/On-linemusicdistribution_a_case_study.pdf
5. **Secure Music Content Standard - Content Protection with CodeMeter** 47-58
Marcellus Buchheit, Rüdiger Kügler
http://virtualgoods.tu-ilmenau.de/2004/SecureMusicContentProtection_VG2004.pdf
6. **Towards a Secondary Market for Virtual Media - A Theoretical Approach** 59-71
Lutz Niehüser, Johannes Bräutigam
<http://virtualgoods.tu-ilmenau.de/2004/SecondaryMarket.pdf>

Session 3: The Value of Virtual Goods

7. **Modelling the eVerlage Payment Protocols** 72-83
Uwe Petermann
<http://virtualgoods.tu-ilmenau.de/2004/EVerlagePaymentProtocols.pdf>
8. **How to Pay in LicenseScript** 84-90
Cheun Ngen Chong, Sandro Etalle, Pieter Hartel
<http://virtualgoods.tu-ilmenau.de/2004/ceh04vgoods.pdf>
9. **Personalized Previews: An Alternative Concept of Virtual Goods Marketing** 91-100
Patrick Aichroth, Stefan Puchta, Jens Hasselbach
http://virtualgoods.tu-ilmenau.de/2004/personalized_previews.pdf

Session 4: Digital Protection and Digital Rights for Virtual Goods

10. **Enabling Digital Content Protection on Super-Distribution Models** 101-112
Carlos Serrão, Joaquim Marques
<http://VirtualGoods.tu-ilmenau.de/2004/VG2004-EDCP-SD-OSDRM.pdf>
11. **Licensing Structured Data with Ease** 113-124
Yee Wei Law, Cheun Ngen Chong, Sandro Etalle, Pieter Hartel, Ricardo Corin
<http://VirtualGoods.tu-ilmenau.de/2004/law04licensing.pdf>
12. **Interoperability Challenges for DRM Systems** 125-136
Andreas U. Schmidt, Omid Tafreschi, Ruben Wolf
http://VirtualGoods.tu-ilmenau.de/2004/Interoperability_Challenges_for_DRM_Systems.pdf

Enabling Digital Content Protection on Super-Distribution Models

Carlos Serrão

ISCTE – Instituto Superior de Ciências do Trabalho e da Empresa
Ed. ISCTE – Av. Das Forças Armadas – 1600-082 Lisboa – Portugal

Email: carlos.serrao@iscte.pt

Joaquim Marques

IPCB – Instituto Politécnico de Castelo Branco
Av. Pedro Alvares Cabral N°12 – 6000 Castelo Branco - Portugal

Email: joaquim.marques@ipcb.pt

Abstract: Consumers, content creators and owners have to deal with some complexities while using digital content e-Commerce - protection of digital rights is one of the most important ones. Digital content distribution can enable new consumer experiences and new architectures/frameworks oriented to protect and distribute content can help these new types of electronic distribution. The paper describes some of the most important functionalities of one of these platforms – OpenSDRM - and how it can be used to securely distribute content on a super-distribution mode protecting the copyright as an alternative to the traditional approaches

1 INTRODUCTION

The Internet's global reach enables the free distribution of content on an unprecedented scale. In current days, a large number of users exchange without any restrictions to digital content, creating great expectations on new ways to distribute and commercialize these new types of virtual assets. However, enabling an acceptable framework where both consumers and creators/content owners are attracted is not an easy task. These new types of distribution models must coexist in a flexible system where system operators can control the content exchanges but also creators/content owners must trust on the content protection technology.

In this paper, the issue of content protection is exploited not only on traditional PC systems but also on embedded systems where a specific DRM system is applied (OpenSDRM). This system enables a new way of doing business, where protected content can be shared and distributed among several users. With the correct business model and the legal system in use, it is possible to control the content exchange on the OpenSDRM system, providing a new user experience and preserving the digital rights of all actors on content distribution chain.

2 DRM AND SUPERDISTRIBUTION

Several organizations may have different reasons for protecting and managing their digital content. Content owners and service providers may want to control access to their content in order to generate revenue from its sale, while a company may want to share content but not sell it. In a company, content access is generally controlled through authentication mechanisms. This, however, does not control what users can do with the content once they have access to it. DRM is the technology that defines and enforces the rules by which the content may be used.

DRM provides three main benefits: 1) persistent protection of content through encryption, 2) expression and association of usage rules with the content, and 3) enforcement of the usage rules [1]. Flexible rights expression languages allow the specification of different rights which can be associated with content usage; number of utilizations, transfer and copy rights, expiration date, preview and many others. DRM systems must have access to these rules before content accessed is cleared, in a safe and protected way. Encryption is a master piece on a DRM system not only to protect the content access but also the rules associated to that content usage. In formal terms DRM is the way of addressing the description, identification, trading, protection, monitoring, and tracking of all forms of rights over tangible and intangible assets, including the management of rights holders 'relationships' [2].

Competing with today's freely available content and user habits, DRM must not offer less than current systems to have success: portability and compatibility between different devices, interoperability between DRM systems, offline usage, privacy protection, enforcement of author rights and its exchange with other trusted devices, upgradeability and personalization and ease of use. To be effective, some constraints need to be observed: content requires identifier systems; persons and devices may need other types of authentication beyond their own native one (e.g. the serial number of the device); rules need to be expressed in a way intelligible to humans and devices. The rights data dictionary and rights expression language requirements are the engine of any effective, DRM-enabled, online content system. Interoperability is a fundamental issue: different platforms and DRM systems must be able to apply rights permissions associated to a specific content. Digital item identification is also critical to the success of DRM and the selected business model. The relationship between identity, content and rules (Figure 1), and the way they are managed are the core of any DRM system. The better DRM can manage this relationship the better are the chances to succeed.

$$DRM(Action) \leftarrow f(identity, content, \sum rules)$$

Figure 1 – The DRM function

Independently from these relationships, some basic constraints need to be established in order DRM can succeed. The first one is the ability to deliver content and usage rules independently of the content itself. The second is the protection of the persistent association between content and license for a particular user and content. In this way, content downloaded with the purpose to be used on a device cannot be transferred to a second device unless the permission obtained by the user explicitly permits it.

The digital value chain, beginning with the content provider and ending at the final consumer depends on the content format and the rendering device used – a digital music player, a television, a printer, etc. The responsibilities of the various participants in the value chain are high, establishing a network of dependencies. Most of the actual systems implement simpler business models – subscription-based are the most common. However, certain DRM systems can and will be used for the implementation of much more complex business models, particularly in the B2B environments, but also on B2C and C2C. One of the models which are well known and successful from today's users is super-distribution (Figure 2). However, to be exploited commercially, this model needs to incorporate DRM functionalities into the basic P2P mechanisms which allow the content sharing. This

continuous sharing process can continue, since content is protected. At the end, users will have to have the appropriate rights to use the content – either acquired from content owners or distributors, obtained from other users or from any other source [3].

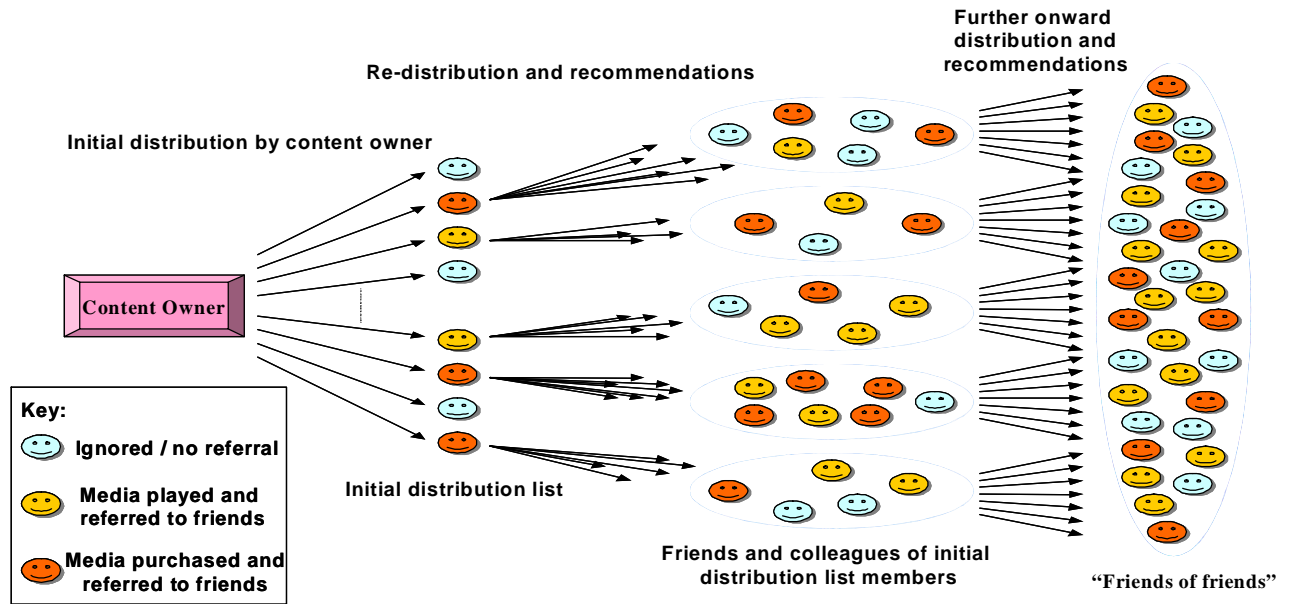


Figure 2 – Super-Distribution model

3 THE OPEN DRM APPROACH

DRM technology was developed and has been evolving, having in mind the protection of commerce, the intellectual property ownership and privacy rights of digital content creators and owners as it travels through the distribution chain, from producer to distributor to consumer and within consumers themselves. It persistently protects and governs content based on usage rules specified by the content owner and rights held by the consumer. DRM can be used to control and track authorized access and use for marketing, sales, and royalties, penetration, and accountability reasons. For these reasons, DRM can be an important component of an organization’s business strategy, but also a precious tool to assist creators and traders with the management of their digital content assets enabling a set of business models according usage rules.

The DRM platform that is presented in this paper - OpenSDRM [5] - is a global framework can be configured to with several business models and different types of content which means that it is flexible and adaptive [4]. It can be applied for publishing and trading of any type of content adopting traditional DRM solutions for content rights protection. Additionally, the security architecture proposed is inline with recent international specifications OPIMA [6], MPEG-4 and MPEG-21 [7]. It is important to clarify the word “open”. This word doesn’t mean that it is insecure. It simply means that the DRM proposal is open in several senses: it is based on open standards, it was developed using open-source technology, and it is open in the sense that it is extensible by allowing the integration of additional components. Part of the OpenSDRM system is based on Intellectual Property Rights Management and Protection (IPMP) model [8] and its extensions [9] proposed by MPEG. It is oriented on the regulation of restrictions upon the users but giving some flexibility on content exchange among them. DRM systems based on

IPMP are a broad and flexible model having support to lightweight and heavyweight model. A significant portion of this model is based on the existence of IPMP-standardized devices and tools. It can be implemented as a centralized or decentralized protection system and can be so versatile that can adapt to almost any situation. This open DRM platform was developed primarily in the scope of the IST MOSES project. MOSES implemented MPEG-4 IPMP Extensions and at the same time developed business models and applications for secure content exchange between devices (PCs and embedded) [10]. This DRM solution is composed of several optional elements covering the content distribution value chain, from content production to content usage. OpenSDRM covers several major aspects of content distribution and trading: content production, preparation and registration, interactive content distribution, content negotiation and acquisition, strong components and user's authentication and conditional content rendering.

3.1 DRM Architecture

OpenSDRM covers several major aspects of the content distribution and trading: content production and preparation (Content Preparation Server, Registration Server), content protection (Registration Server, License Server, Intellectual Property Management and Protection - IPMP tools server and Authentication Server), content interactive distribution (Media Delivery Server), content negotiation and acquisition (Commerce Server, Payment Gateway), strong components and users authentication (Authentication Server) and conditional visualization/rendering (Media Player, IPMP tools Server, License Server) [5].

This architecture provides an integrated DRM solution, interfacing with several external actors which have their own specific role and requirements: User wants to use content, Content Provider(wants content trading, but assured that this content is protected and that it receives a financial return), IPMP tools Provider (wishes to commercialize their own content security tools), Payment Infrastructure (represents the financial environment) and the Certification Authority (the entity responsible for injecting trust on the system).

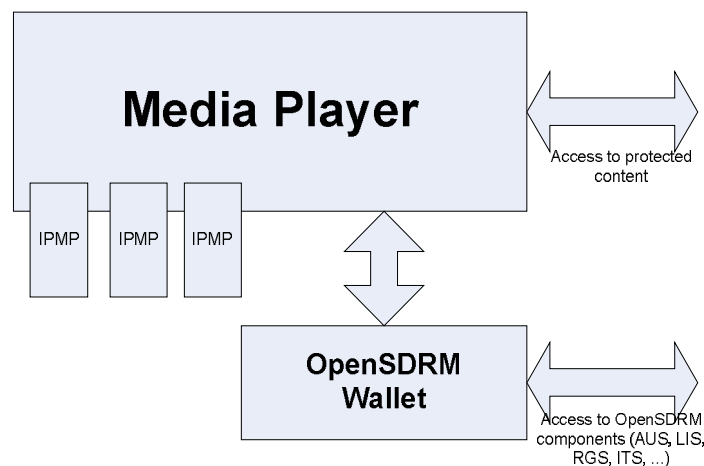


Figure 2 - OpenSDRM on the client-side

Although OpenSDRM represents DRM architecture at the conceptual level, an instance of this concept has already been implemented. The implementation followed an LAMP-based (Linux, Apache, MySQL and PHP) approach based on open-source software.

The DRM functionalities are shared between the server-side components and the client-side components. On the client-side, MPEG-4 IPMPx was used for the first time. IPMPx was implemented and integrated with the IM-1 MPEG-4 reference player. This model allowed the flexibility need to download and integrate the necessary IPMP tools (encoders, encryption, watermark, license parsing, ...) to uphold the necessary copyrights on the user-side.

Another important component that was developed that allowed the system to increase the security on the client side was the wallet. This wallet allowed the user to secure store information (such as personal information and content licenses) and also to contact the rest of the OpenSDRM platform.

The main innovations from this concept were the usage for the first time of the MPEG-4 IPMPx and the usage of an open DRM approach (opposing to closed DRM solutions that already existed).

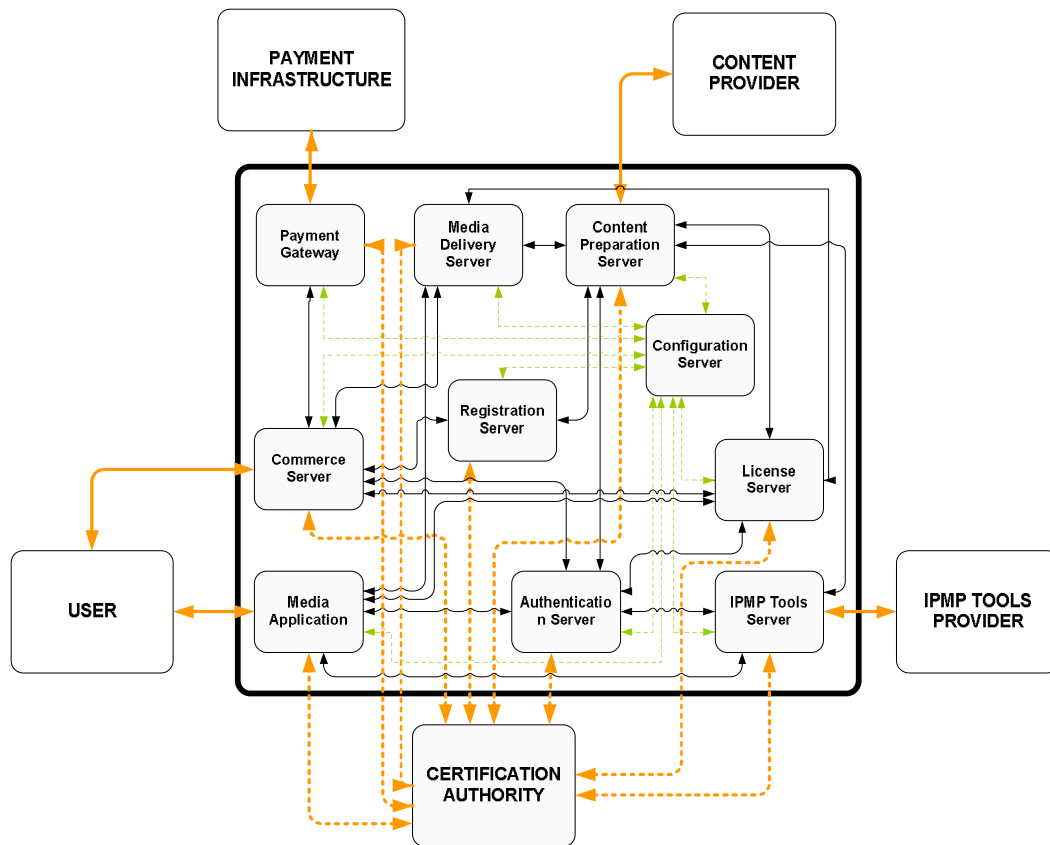


Figure 3 - The OpenSDRM architecture

3.2 OpenSDRM interactions

3.2.1 External actors Interactions

This part provides a general presentation of the components and actors that interact externally with the OpenSDRM architecture: User, IPMP Tools Provider, Content Provider, Payment Infrastructure and Certification Authority.

User - The User represents a person who wishes to operate a way of enjoying some 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) [5].

IPMP Tools Provider - The IPMP Tools Provider is any organization that produces tools 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. The IPMP Tools Provider requests to the OpenSDRM platform the tools upload [5].

Content Provider - The Content Provider is any multimedia content supplier that feeds OpenSDRM with content and/or metadata [5].

Payment Infrastructure - The Payment Infrastructure facilitates OpenSDRM e-commerce features by providing services for handling electronic payments. The Payment Infrastructure will be any infrastructure capable of handling payments [5].

Certification Authority - 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 [5].

3.2.2 Internal Components & Interfaces

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

Content Preparation server - This 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. If further metadata needs to be added, it is stored on the Registration Server. This component implementation is particular according to the type of content in-use. Some of the particularities that can be found on this component refer to the encoding tools to be used and also to the protection tools which may change according to the type of content and level of protection.

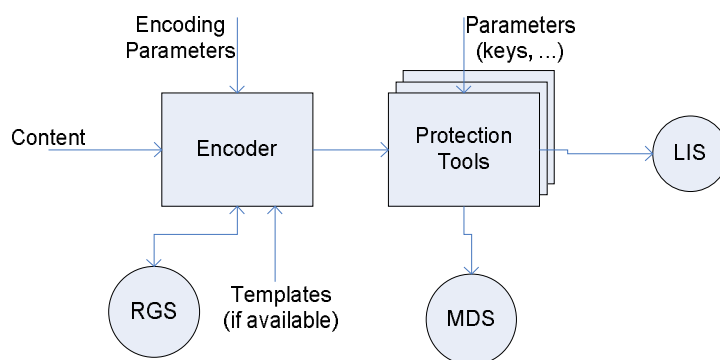


Figure 4 - Content production and protection

Currently, and under the MOSES project, content type is music, which is 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.

Commerce server - The Commerce server is a server component responsible for trading the content or licenses with the users. In fact, what the Commerce server trades are the specific access conditions to access the content.

This component may not necessarily represent an electronic commerce shop. It can be seen as a licensing broker between the user and the content provider or distributor. This broker negotiates the conditions under which the final user can access the content, and how the content keys can be cleared.

Content can be chosen via web browser (although it may be actually obtained from any other source, such as other users or P2P systems), some very generic metadata might be consulted, information about the price is also available, and especially the content usage conditions might be established. The user must be authenticated to this component through the Authentication server and the licenses for the content are also produced online based on this user authentication and the conditions he chose. This operation may also involve a financial transaction in which a particular user pays a specific price for the conditions selected to access the content.

Media Delivery server - The Media Delivery server is a server component responsible for exchanging pieces of content with the client.

This component is used to register the place where the content is located and when it should be delivered to the user. The component itself may not store the content or implement the delivery method to provide the content to final users – this may be a particular function of the delivery server itself (download, streaming, broadcast).

Registration server - The Registration server is a server component whose role is to assign unique identifiers to content and to register metadata information for that specific content. One of the goals of this architecture is to be as close as possible to standards and therefore for this unique ID, it follows the MPEG-21 directives about Digital Item Identification (DII), using a reduced version of the MPEG-21 DII Digital Object Identifiers (DOI) [11]. Other content identification schemes may also be used.

Authentication server - This server component is responsible for authenticating all the entities, internal and external to the DRM system. It validates the access rights of all the entities and components in the system. The Authentication Server works as a single-sign-on point in the entire system, 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. All messages between components are exchanged over a secure and authenticated channel, such as SSL/TLS. Additionally, the messages exchanged between components are signed and authenticated. Since OpenSDRM is a distributed architecture. The communication between the single components will usually take place within insecure networks. Furthermore the components communicate with a text-based protocol. This introduces special needs regarding the security of this communication. An underlying concept behind the OpenSDRM platform is the existence of two security layers. A first security layer is established at the communication level, which will provide the necessary secure and authenticated communication medium to components to communicate with each other. A second layer is established at the application level, ensuring the security, integrity, authentication and non-repudiation mechanisms needed by the different components.

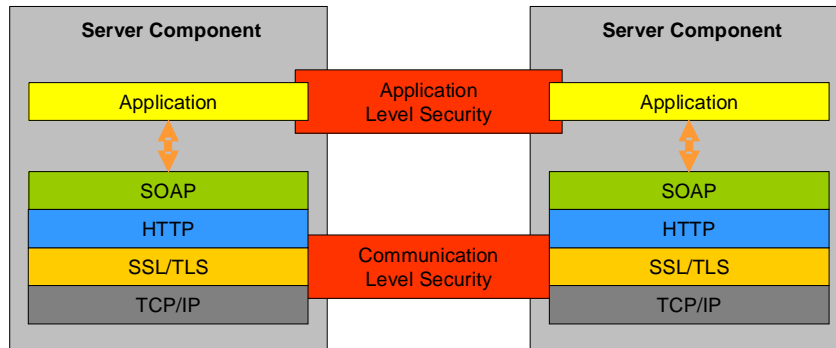
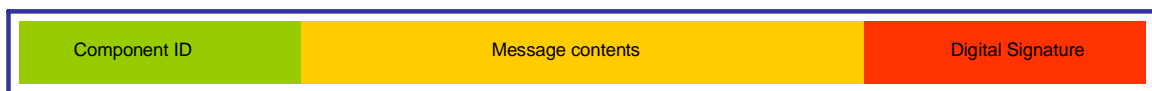


Figure 5 - Message security layers

Each of the messages exchanged between the different components share a common structure. The format as shown is composed of:

- Component ID: a 128 bits identifier (generated by an MD5 hashing algorithm) that identifies uniquely this component. This identifier was issued by the Authentication Server;
- Message Contents: this is a set of different fields of the message, and typically it is different from component to component;
- Digital Signature: the digital signature of the message, to avoid the message contents tampering.



SOAP message

Figure 6 - Message format

License server - The License server 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 client Media Players 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) [12], and, in the future, they will migrate to the Rights Expression Language (REL) [13], currently being developed by MPEG-21.

<pre><?xml version="1.0" encoding="UTF-8"?> <o-ex:rights xml ns:o-ex="http://odrl.net/1.1/ODRL-EX" xml ns:xsi="http://www.w3.org/2001/XMLSchema-instance" xml ns:o- dd="http://odrl.net/1.1/ODRL-DD" xsi:schemaLocation="http://odrl.net/1.1/ODRL-EX ../schemas/ODRL-EX- 11.xsd http://odrl.net/1.1/ODRL-DD ../schemas/ODRL-DD-11.xsd"> <o-ex:asset> <o-ex:context> <o- dd:uid>urn:mpeg:mpeg21:did:doi:pt/adetti/music/0001</o-dd:uid> <o-dd:name>MusicName</o-dd:name> </o-ex:context> </o-ex:asset> <o-ex:permission> <o-dd:play> <o-ex:constraint> <o-dd:count>2</o-dd:count> </o-ex:constraint> </o-dd:play> </o-ex:permission> </o-ex:rights></pre>	<pre><?xml version="1.0" encoding="UTF-8"?> <r:license xml ns:dsig="http://www.w3.org/2000/09/xml dsig#" xml ns:mx="urn:mpeg:mpeg21:2003:01-REL-MX-NS" xml ns:r="urn:mpeg:mpeg21:2003:01-REL-R-NS" xml ns:sx="urn:mpeg:mpeg21:2003:01-REL-SX-NS" xml ns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="urn:mpeg:mpeg21:2003:01-REL-R-NS ../schemas/rel- r.xsd urn:mpeg:mpeg21:2003:01-REL-SX-NS ../schemas/rel-sx.xsd urn:mpeg:mpeg21:2003:01-REL-MX-NS ../schemas/rel-mx.xsd"> <r:grant> <r:keyHolder> <r:info> <dsig:KeyName>UserID</dsig:KeyName> </r:info> </r:keyHolder> <mx:print/> <r:digitalResource> <r:nonSecureIndirect URI=" urn:mpeg:mpeg21:did:doi:pt/adetti/music/0001"/></pre>
--	---

<pre> <o-ex: party> <o-ex: context> <o-dd: name>UserID</o-dd: name> </o-ex: context> </o-ex: party> </o-ex: rights> </pre>	<pre> </r: digitalResource> <r: allConditions> <sx: exerciseLimit> <sx: count>2</sx: count> </sx: exerciseLimit> </r: allConditions> </r: grant> </r: license> </pre>
--	---

Figure 7 - ODRL and MPEG-21 REL license samples

IPMP tools server - The IPMP tools server is the server component responsible for registering new IPMP tools and for receiving authenticated client Media Player 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 Player - 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 is available (if this codec is not available it may be downloaded from a remote secure server). This player 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. For MOSES in particular we will have two types of Media Player (they will both be able to render MPEG-4 content) one for the PC environment and the other for the Pocket PC environment.

3.3 OpenSDRM and SuperDistribution

SuperDistribution encourages the free flow of digital content by charging of use, not possession. To be feasible a DRM system enabling SuperDistribution must control the content usage and this is given by a persistent cryptographic technology. That is in place by OpenSDRM giving access control relatively to digital property since the consumer agrees to the terms and conditions of use. Although the content control has its own security when content transfers from device terminals exists a licence management process centralized on clearinghouses that enables and ensure compatibility when a user need more rights than that's was transferred. This service would provide publishers with information about player devices and also support to alternative business models such as pay-per-view or subscription based pricing models based on secure licenses issued. Players with Internet connectivity could also support online security verification and downloadable security updates.

To quickly understand how OpenSDRM handles the SuperDistribution model we must consider two simple usage scenarios after a user do a normal content acquisition (where users negotiate with Commerce Server and License Server to get the selected content and a license):

- 1) User sends content to other user without the respective license

In this case the final user (Ui) must contact the commerce server (COS). After negotiating the conditions with the user, this will contact the license server (LIS) to get a new license appropriated for that content. After get the license and store securely content the player renders it.

- 2) User sends content and license to other user

In this case the initial user (Ui) will signal the license server to produce a new license to the final user (Uf) with some transferred rights associated. After updating initial user license them is produced another license to the final user. After getting the new license from License server (LIS) the player can render it.

Both enables SuperDistribution but the big difference between them resides on contacting the commerce server to negotiate a new license. The second scenario is more decentralized than the first one being more versatile in the sense that will be easier to the final user because he wouldn't have to acquire a new specific license for that purpose.

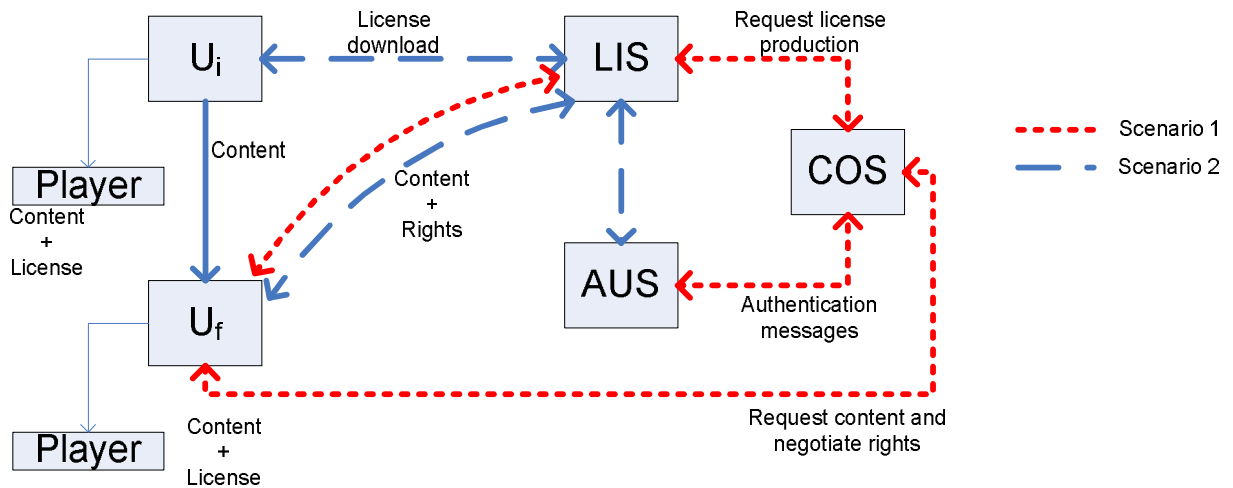


Figure 8 - Usage Scenarios

The OpenSDRM framework can be implemented as a centralized or semi-decentralized protection/management system can also be so versatile that can adapt to almost any trading situation. The content can be discovered and bought in different ways, after seeing an ad online or through a friend. Object metadata inserted includes the required information for purchasing rights. Also, if security is compromised, a new IPMP can be downloaded specifically to that content creating a chain of trust between all actors reducing the damage of piracy since each content/license must be hacked personally for each terminal.

The OpenSDRM can establish a flexible environment where relationship between rules, content and identity are managed enabling a global attractive framework to overall actors. Using international and widely accepted standards not only to identify but also to express and apply rights permissions turns it in a promissory DRM system giving to the final user the portability and compatibility between different devices he needs.

4 Conclusions

Content on OpenSDRM framework will spread without minimal intervention from distributors getting spread around communities of interests. Super-Distribution is surely a great way to find content. Super-Distribution will turn consumers in advertisers and promoters of content in a special interest group. Also the content owners, retailers and other actors get their fees with a minimal intervention.

Some of the OpenSDRM characteristics can not by themselves contribute to the success of Super-Distribution but to the success of the business models that are possible to implement. These include:

- Is easy to use and convenient in the sense consumers can share (redistribute) its own content;
- Provide enough value to convince a significant number of users to choose it over free exchanges because a network of clearinghouses providing higher quality content and more efficient distribution can negotiate personalized licenses;

- Can give to the user a new consumer experience (pricing, sharing, others) contributing this way to enhancing its acceptance by encouraging users to exchange content;
- Can contribute to the acceptance of new standards (content file format, player, device type, others);
- It is secure and flexible enough to traders and consumers;

OpenSDRM offers a solution for securely distribute, trade and control the access and usage of valuable content giving partners on the value chain to build a global digital commerce system matching their interest and needs with adequate and flexible business models. Addressing the most fundamental issues associated with content distribution on digital area (content protection, usage control, usage tracking, flexible business models) it can give flexibility unattended on other solutions. Super-Distribution, can also be targeted given an usage experience very interesting to the final user. If allowed by initial rules further use of content by another consumer can occur only in compliance with the previous transmitted rules. If interested on more permission the user who receives content/license must contact the online OpenSDRM licence server to get more rights. Enabling the transmission of content independently of direct distributor intervention this can open a new usage experience that opens new opportunities to traders on content business but also to consumers.

OpenSDRM incorporates some degree of centralized control that provides the security and management features essential to drive an e-business solution to content market. Also when a consumer distributes content among others the final one can get a different usage experience from the initial if he gets more rights from the license server and enabling a new way of consuming content (promotion, fees collection, and others). This model has more advantages relatively to an exclusively centralized system because the generally observed bottlenecks issues are diluted. When an user sends content to another the major traffic are on Internet when final user tries to get a new license and this one are very bit smaller when compared with the bits amount on a content file. This point-to-point delivery of license files and a central point of distribution on OpenSDRM can give support to new opportunities on e-commerce giving wings to the concept of Super-Distribution.

Finally, the presented architecture has been implemented and applied to a specific service of digital music commerce and distribution. This service is called Music-4You and can be reached on the WWW through the following URL: <http://www.music-4you.com>. Music-4You represents an alternative to existing music trading websites, allowing music producers to automatically put their work online, protecting it, and allowing the final users to negotiate the conditions under which they would like to access the music, paying for it a fair price.

4 REFERENCES

- [1] "Digital Rights: Background, Systems, Assessment", Commission Staff Working Draft, Commission of the European Communities, 2002
- [2] Iannella R., 2002, D-Lib Magazine, June 2001, Volume 7 Number 6 ISSN 1082-9873 <http://www.dlib.org/dlib/june01/iannella/06iannella.html>
- [3] Ammar M., Judge P., 2003, "The Benefits and Challenges of Providing Content Protection in Peer-to-Peer Systems", *Paul Judge, Virtual Goods 2003*, Ilmenau <http://virtualgoods.tu-ilmenau.de/2003/BenefitsAndChallengesOfP2PContentProtection.pdf>
- [4] Gregor Siegert, Carlos Serrão, "An Open-Source Approach to Content Protection and Digital Rights Management in Media Distribution Systems", ICT Conference 2003, Copenhagen December 2003
- [5] Carlos Serrão, Daniel Neves, Panos Kudumakis, Trevor Barker, Massimo Balestri, "OPEN SDRM – AN OPEN AND SECURE DIGITAL RIGHTS MANAGEMENT SOLUTION", IADIS 2003, Lisboa, Portugal, May 2003
- [6] Serrão, C., Marques, J., Kudumakis, P., Balestri, M., Barker, T., "Protecting Digital Music Delivery and Consumption using the OCCAMM Project Framework", WEDELMUSIC2002, Darmstadt, Germany, 2002
- [7] INTERNATIONAL ORGANISATION FOR STANDARDISATION ORGANISATION INTERNATIONALE DE NORMALISATION ISO/IEC JTC1/SC29/WG11 CODING OF MOVING PICTURES AND AUDIO, ISO/IEC JTC1/SC29/WG11/N5231, Shanghai, October 2002, <http://www.chiariglione.org/mpeg/standards/mpeg-21/mpeg-21.htm>
- [8] Koenen, R., "Overview of the MPEG-4 Standard", ISO/IEC JTC1/SC29/WG11 N4668, MPEG, 2002
- [9] J. King and P. Kudumakis, "MPEG-4 IPMP Extensions", 8th ACM Conference on Computer and Communications Security (CCS-8), Philadelphia, Pennsylvania, USA, (2001).
- [10] MOSES – "MPEG Open Security for Embedded Systems", <http://www.crl.co.uk/projects/moses/>
- [11] INTERNATIONAL ORGANISATION FOR STANDARDISATION ORGANISATION INTERNATIONALE DE NORMALISATION ISO/IEC JTC1/SC29/WG11 CODING OF MOVING PICTURES AND AUDIO, ISO/IEC JTC1/SC29/WG11/N5231, Shanghai, October 2002,
- [12] Jan Bormans, Keith Hill, "MPEG-21 Overview v.4", ISO/IEC JTC1/SC29/WG11/N4801, 2002
- [13] Multimedia Description Schemes (MDS) Group, "MPEG-21 Rights Expression Language Working Draft", ISO/IEC JTC1/SC29/WG11/N4533, 2001