Digital Rights Management for E-Commerce Systems

Dimitrios Tsolis
University of Patras, Greece

Lambros Drossos
TEI of Messolonghi, Greece

Spyros Sioutas
Ionian University, Greece

Theodore Papatheodorou
University of Patras, Greece

Information Science REFERENCE

INFORMATION SCIENCE REFERENCE

Hershey · New York

Director of Editorial Content: Kristin Klinger
Director of Production: Jennifer Neidig
Managing Editor: Jamie Snavely
Assistant Managing Editor: Carole Coulson
Typesetter: Carole Coulson
Cover Design: Lisa Tosheff
Printed at: Yurchak Printing Inc.

Published in the United States of America by
Information Science Reference (an imprint of IGI Global)
701 E. Chocolate Avenue, Suite 200
Hershey PA 17033
Tel: 717-533-8845
Fax: 717-533-8661
E-mail: cust@igi-global.com
Web site: http://www.igi-global.com

and in the United Kingdom by
Information Science Reference (an imprint of IGI Global)
3 Henrietta Street
Covent Garden
London WC2E 8LU
Tel: 44 20 7240 0856
Fax: 44 20 7379 0609
Web site: http://www.eurospanbookstore.com

Library of Congress Cataloging-in-Publication Data

Digital rights management for e-commerce systems / Lambros Drossos ... [et al.].

p. cm.

Includes bibliographical references and index.

Summary: "This book highlights innovative technologies used for the design and implementation of advanced e-commerce systems facilitating digital rights management and protection"--Provided by publisher.

ISBN 978-1-60566-118-6 (hardcover) -- ISBN 978-1-60566-119-3 (ebook)

1. Electronic commerce--Technological innovations. 2. Copyright and electronic data processing. 3. Data protection. 4. Computer security. I. Drossos, Lambros, 1961- II. Title: Digital rights management for ecommerce.

HF5548.32.D54 2009

005.8--dc22

2008022547

British Cataloguing in Publication Data
A Cataloguing in Publication record for this book is available from the British Library.

Chapter X
Digital Rights Management and E-Commerce Transactions:
Online Rights Clearance

Dimitrios P. Meidanis
SilkTech S.A., Greece

Spiros N. Nikolopoulos
SilkTech S.A., Greece

Emmanouil G. Karatzas
SilkTech S.A., Greece

Athanasia V. Kazantzi
SilkTech S.A., Greece

ABSTRACT

This chapter investigates intellectual property rights clearance of as part of e-commerce. Rights clearance is viewed as another online transaction that introduces certain technological and organizational challenges. An overview of the current intellectual property rights legislation is used to describe the setting in which business models and digital rights management systems are called to perform safe and fair electronic trade of goods. The chapter focuses on the technological aspects of the arising issues and investigates the potentials of using advanced information technology solutions for facilitating online rights clearance. A case study that presents a working online rights clearance and protection system is used to validate the applicability of the proposed approaches.

INTRODUCTION

Rights clearance has always been an important issue in every transaction that involves copyrighted objects but even in other transactions such as land property acquisition. Typically the owner (seller) has to prove that he possesses the right to make the transaction and the buyer has to be sure of the

legitimacy of the transaction that he is going to be part of. The general perspective of this chapter is to address every aspect of rights clearance in e-commerce transactions mainly from the technical point of view. The major topics that will be addressed in the remaining of this chapter are the investigation of on-line rights clearance background in terms of broad definitions, discussions and contradicting views, the inquire of intellectual property rights as part of a Digital Rights Management system and with respect to a plausible business model, the analysis of the technical components involved in on-line rights clearance, along with the arising flow control and engineering issues as well as the presentation of an operative DRM system integrating on-line rights clearance practices.

BACKGROUND

"Rights clearance" is a term often used indiscriminately to describe a set of processes that are followed both in the physical and digital world. As a consequence, the "bad" use of this term and in general the terminology related to rights clearance is usually a source of many ambiguities and misconceptions that prevent readers from acquiring a common understanding on the issue. The goal of this section is to outline the related topics, address controversial issues and eventually formulate a clear basis that will help the reader gain an insightful view of the subject.

Intellectual Property Rights (IPR) and Current Legislation

Current legislation concerning intellectual property primarily aims at protecting artworks that exhibit a considerable level of creativeness and novelty, such as works originating from literature, theatre, music, art etc. Among the large corpora of law proceedings that concern intellectual properties, there is a considerable portion that attempt to address intellectual properties as formulated by digitizing and distributing content through computer networks. There is a very strong tradition that seeks to harmonize the activities of all European countries under a common, international action line, with the aim to tackle the problems generating from the misuse of intellectual properties. The need for common treatment of such issues is considered essential in the context of a European market, mainly due to differences in conception of intellectual property and the obstacles arising by the enforcement of domestic copyright restrictions. If we consider the pace by which digital information is being generated and the practices that are often used for its distribution and sharing, it is evident that individual national legislations are inadequate to guarantee the interests of intellectual property owners, in the light of an emerging and without boundaries digital trade.

The purpose of national legislation is to determine the amount of actions that are considered legitimate within the nation boundaries. However, the study of a national legislation should not be carried out independently from the international status quo. The international state of affairs is constituted by international conventions and directives that act normatively in the establishment of national laws. The most important international conventions are:

- Berne convention (supervised by World Intellectual Property Organization) [WIPO]
- The international convention regarding copyright (UCC)
- TRIP's agreement (Trade Related Intellectual Property Rights) under the auspices of World Trade Organization

The purpose of the aforementioned conventions is to introduce a set of minimum requirements to be adopted by all member states. In this context, the European Commission (EC) envisages the establishment of a European legislation that will be founded on the international conventions and will be adopted by all European countries, in order to facilitate a global, liberal European market where the trade of goods will be conducted in a smooth and unrestricted manner.

Originality is the essential characteristic that an artwork should exhibit in order to allow for its rights to be granted under intellectual property laws. Berne convention does not provide an explicit definition describing which artworks should be considered copyright protected and which not. However, an artwork should be more than a simple digital representation of a physical object in order to be considered original. Berne convention does not treat the digitized version of an original artwork as a "new original artwork" with completely independent intellectual properties, despite the fact that under certain circumstance such rights can be granted. The copyright holder of an artwork is by default the person who has created it. In the case where the artwork has been generated by more than one creator, intellectual properties are assigned to all participants. Concluding, we can claim that the intellectual properties legislation framework in each European country derives from the combination of Berne convention, European directives and national laws.

Rights Clearance

The term "Rights Clearance" refers to the overall process of determining the terms and conditions that constrain the use of an artwork, identifying the person or organization that holds the right to grant its usage permissions and eventually trasnfering these permissions on the ground of a license agreement.

Although different types of intellectual properties exist such as a) copyright b) database right c) moral rights d) rights bound to patents e) execution right etc, the process of rights clearance can be considered roughly uniform.

The outcome of rights clearance is a set of rules that constrain the use of an artwork, always with respect to a certain agreement. This outcome is described by a license that serves as a contract between the rights owner and the final user. The license is a document that details the terms and conditions under which the content is allowed to be exploited by the end user without committing copyright violation. Hence, as long as the license counterparts obey to the conditions of the agreement, rights violation is not an issue. Nevertheless, this process can either be performed in the digital or the physical world raising important differentiations to its interpretation.

Rights Clearance in the Physical world is a process quite straightforward since it has been exercised for many decades and its long established practice has set a frame of rules that must be followed. It is usually transacted by attorneys or other professions or organizations with adequate knowledge and access to records describing the rights applied on an object.

Rights clearance in the Digital world has become an absolute necessity, since e-commerce plays a vital role in modern transactions. After the transition to the Digital world, rights clearance became a more complex procedure and a number of arising issues has to be studied. A key element of this study must be the dissimilarities between the original digital resources and the digitized ones which are bound by different kinds of intellectual property rights. Another important issue introduced by the digital world

is the rights on purely digital objects. Such a study will set the foundations on which some standards for on-line rights clearance will be defined**.**

Digital Rights Management (DRM)

Rights management involves the registration, maintenance, monitoring and administration of the protected content property rights in an efficient and profitable way. Services like tracking the usage of content engaged to a certain license, as well as identifying new rights that bring added value to the content at hand, are considered essential functionalities of a rights management framework. Since rights, as indicated previously, can either refer to physical (i.e., statues, paintings etc) or digital objects (i.e., computer graphics, multimedia content etc), rights management should facilitate both cases. As the number of artworks, digitized or digitally generated, that are being distributed over computer networks rapidly increases, the need for developing advanced digital rights management systems becomes apparent.

Enabling rights management on highly heterogeneous and complex environments as in the case of WWW, requires the extraction and representation of a sufficiently large amount of information in a manner that can be shared among computer systems of the same purpose. Metadata is data about data that aim at describing an object or a resource independently of its nature, physical or digital. Particularly, metadata try to describe sources in a systematic and structured way in order to facilitate their easy sharing and re-use. In this context, intellectual property rights are also information that has to be retained and organized in an interoperable way.

Numerous initiatives, each one with its own advantages and disadvantages, have attempted to establish a set of metadata able to sufficiently capture the information required for managing property rights. Among them, Dublin Core Metadata Initiative [DCMI] has emerged as an international standard that receives considerable support from both industry and academia.

Protecting Digital Rights

Despite the fact that rights clearance, and digital rights management in general, is still in its infancy, numerous technological solutions deriving either from industry or academia have been recorded. The engineering of a holistic rights management system that could meet the requirements of all existing business models seems particurarly difficult. However, certain aspects of the problem have been tackled successfully by custom solutions. The aim of this paragraph is to provide an overview of the current state in the field of digital rights protection and identify the areas open to further improvements.

As mentioned previously registration, maintenance, monitoring and administration of intellectual properties are among the most important requirements that a digital rights management system should fulfill. The design and development of technological means that will facilitate the aforementioned operations are considered essential, especially for tracking distributed content. The mechanisms that incorporate technological protection means, work complementary to the digital rights management systems in order to defend the financial interests of content creators.

There are several ways by which technology can be employed to serve the purposes of digital rights protection. The dominant trends can be categorized as follows:

- **Distribute digital content of low quality:** Constitutes a simple, economical and widely adopted technique for preventing unauthorized actions of content misuse (e.g., printing, replicating etc).

For instance, an image resolution of 72 dpi (dots per inch) is high enough to retain the image visual quality for preview purposes but very low to allow exploitation actions such as publishing printed copies.

- **Distribute encrypted content:** A popular method for protecting digital content, adopted by famous DRM systems is the distribution of multimedia content in an encrypted format. In this case only the user having payed a certain fee, obtains a use license which serves as the decryption key.
- **Steganography:** Protecting digital content using steganographic techniques involves the use of specialized mechanisms that hide encoded messages within the actual content. In this way tracking of content through computer networks is possible, via the transmission of data concerning the content users.
- **Digital watermarking:** Digital watermarking constitutes one of the most modern technological solutions for protecting digital content and has been adopted by a number of content providers. Digital watermarking introduces an additional level of protection and has been particularly popular in the field of digital images. Digital watermarks can be either visible or invisible and their purpose is to provide evidence for supporting the copyright holder ownership over the watermarked content.

RIGHTS CLEARANCE AND DRM

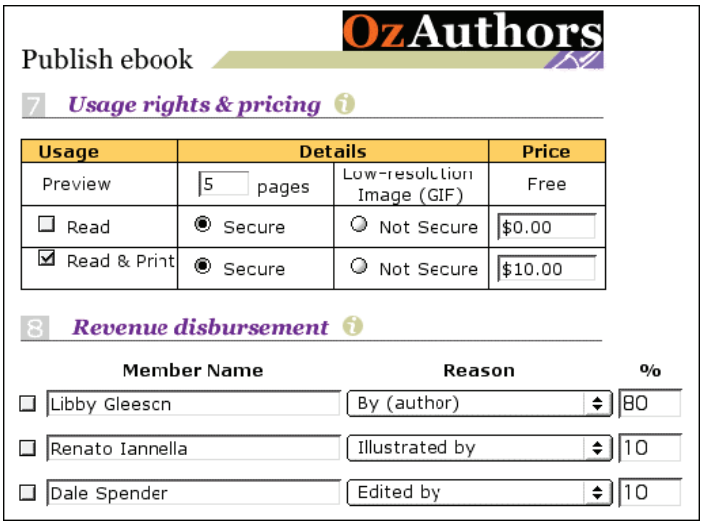
The process of rights clearance involves many different players interacting in various modes. The purpose of this section is to describe a case of electronic trade with special focus on rights clearance. The key-entities will be identified and their interrelations will be outlined. This process is motivated by the necessity to trace the slots in the electronic transaction sequence where advanced technologies can be attached and bridge the gap between physical and electronic commerce. Rights clearance can be regarded as part of the general digital rights management objective that has emerged as one of the greatest challenges for content distribution. First-generation DRM systems, used to rely on encryption techniques, limiting content distribution to a very restricted amount of legitimate users. Second-generation DRM systems facilitate the description, identification, trading, protection, monitoring and tracking of all forms of rights usage over both tangible and intangible assets.

Motivating Example

A typical example of a Digital Rights Management system that incorporates rights clearance functionality can be taken from the E-book sector. OzAuthors (OZAUTHORS) is a service provided by the Australian society of authors in a joint venture with IPR Systems, (Renato 2001). Their goal is to provide an easy way for society members (including Authors and Publishers) to deliver their content to the market place at low cost and with fair royalties for content owners.

Figure 1 shows the OzAuthors' interface for collecting rights related information. In this example, the "Usage Rights and Pricing" frame, allows the content provider to specify "Read" and/or "Print" permissions, pricing, and security options for the ebook. Additionally, a number of pages can be specified for free preview. The second frame of the interface allows the content provider to specify all involved rights holders, their roles, and their percentage on the royalty split. Each time the ebook is sold, the rights holders will automatically receive the indicated amount. By inspecting the front end of a DRM

Figure 1. DRM: Front end example application



system it is evident that there are two critical architectures to consider. The first is the Functional Architecture, which covers the high-level architectural components of a DRM system. The second critical architecture is the Information Architecture, which covers the modelling of the key-players within a DRM system as well as their relationships. In the following, indicative diagrams will be used to illustrate an electronic transaction, in terms of the aforementioned architectures, with special focus on the process of removing the constraints on the use of a digital asset by clearing the rights and obtaining on-line licenses for its use.

Functional Architecture

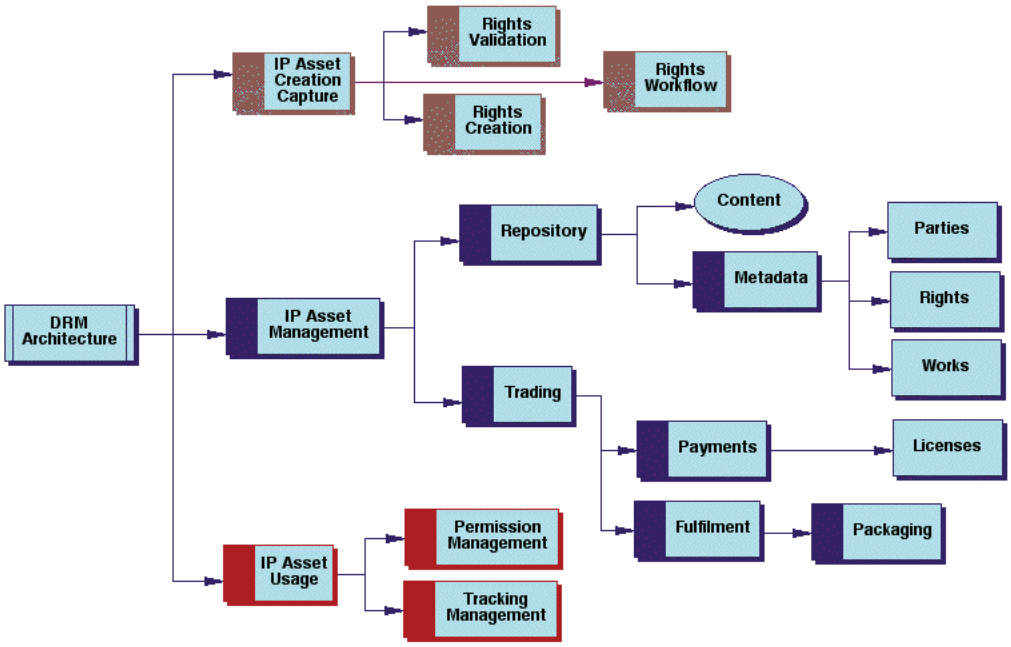
The core functionality of a DRM framework can be separated in the following three main areas:

- **Intellectual property (IP) asset creation and capture:** Refers to the circumstances under which content is created in order to favor its trade. Asserting rights when content is initially created is one such example, since it reduces the complexity of subsequent rights clearance.
- **IP asset management:** Asset management and trade, follows its creation and is carried out by a system that addresses trading requirements, such as descriptive and rights metadata management.
- **IP asset usage:** Monitoring of content usage once it has been traded is the primary goal of this component, which involves applying usage rules over traded content.

While the above core components comprise the broad trucks for DRM, these models need to be further extended in order to fully describe the functionality required by a DRM system (see Figure 2).

The Functional Architecture stipulates the roles and behavior of a number of cooperating and interoperating modules under the three areas of Intellectual Property (IP): Asset Creation, Management, and Usage. Each of these modes is attached with a model hierarchy that provides more detailed description

Figure 2. DRM functional architecture



of DRM functionalities. A thorough analysis of the functional architecture can be found in (Renato 2001). However, Functional Architecture is only part of the answer to the challenges of DRM, since rights management can become complex remarkably quickly. As a result, DRM systems must follow the, more flexible, information model that addresses these complex and layered relationships.

Information Architecture

Entities and relations are two widely established notions that are used to model certain aspects of the real world. In this context, information architecture is primarily concerned with the entities and relations governing DRM functionality. Modeling all different aspects of DRM functionality requires the following actions:

- Model the entities
- Identify and describe the entities, and
- Express the rights statements

Modeling the Entities

A clear and complete model that incorporates all existing entities and relations is useful for identifying the underlying technologies of a DRM framework. The <indecs> project (INDECS) introduces a model where the three core entities: Users, Content, and Rights, are clearly separated as shown in Figure 3. The Users entity encompasses any type of user, from a rights holder to an end-consumer. Content can

Figure 3. DRM information architecture: Core entities Model

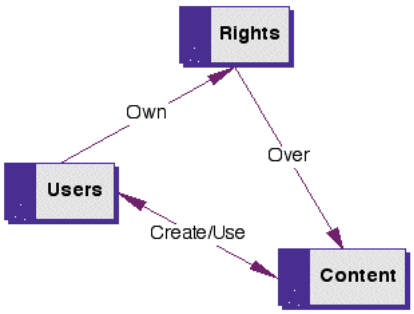
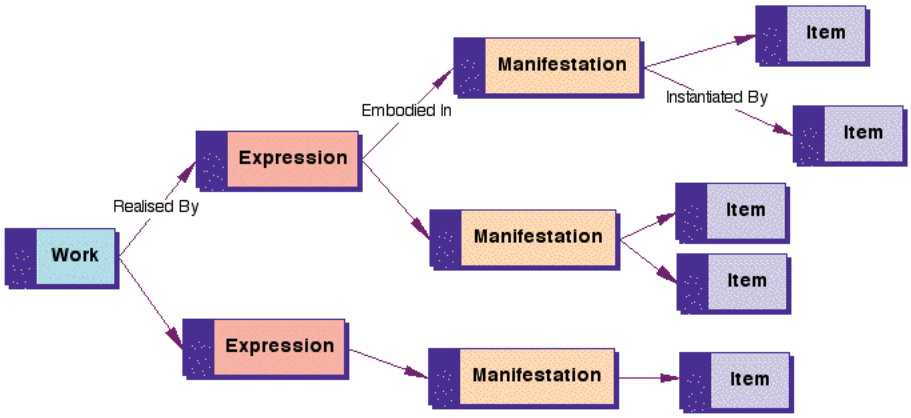


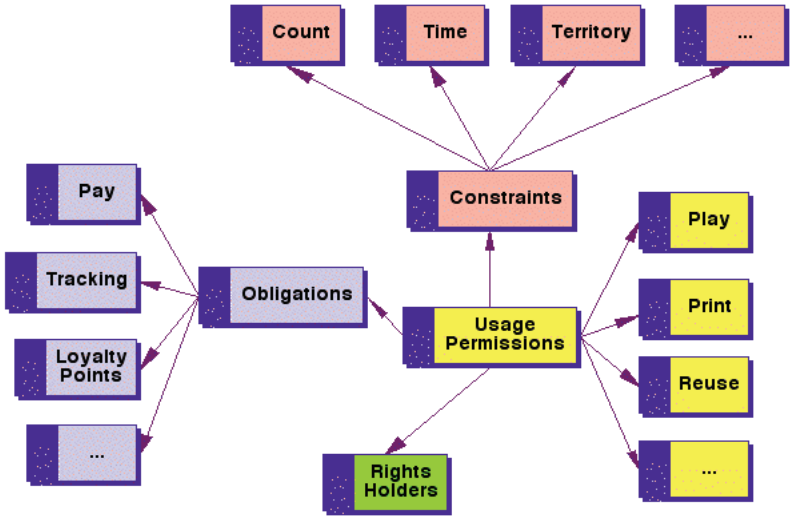
Figure 4. DRM information architecture: Content Model



be any type of content that is subject to electronic trade and the Rights entity is an expression of the permissions, constraints, and obligations between the Users and the Content. The main advantage of this model is that it provides the greatest flexibility when assigning rights to any combination or layering of Users and Content. The core entities model is highly adjustable and can be used to model the needs of new and evolving business models.

The core entities diagram depicted above, constitutes a rather abstract modeling of DRM functionality and indicates that all three entities need to incorporate a mechanism for communicating metadata between them. Attempting a more thorough analysis of the model would require the Content and Rights entities to be further extended by more fine grained entities and relations. International Federation of Library Associations (IFLA) has proposed an extended model for Content entity that is based on many "layers" from various intellectual stages or evolution of its development. The goal behind this extended model is to enable clearer (i.e., more explicit and/or appropriate) attribution of rights information. According to this model, Content can be identified at the Work, Expression, Manifestation, and Item layers, as shown in Figure 4. At each of these layers, different rights and rights holders may need to be supported. Further explanations of the extended model for Content entity can be found in (Renato 2001).

Figure 5. DRM information architecture: Rights Expression Model



Expressing Rights Statements

The Rights entity is dealing with the allowable permissions, constraints, obligations, and any other rights-related information involving Users and Content and determines the required expressivity power of the language used to represent rights metadata information. Rights expressions can become complex quite quickly, especially in cases where the number of required statements grows large. As shown in Figure 5, rights expressions should consist of: Permissions (i.e., usages) - what you are allowed to do, Constraints - restrictions on the permissions, Obligations - what you have to do/provide/accept and Rights Holders - who is entitled to what.

For example, as demonstrated by the motivating example, a rights expression may state that a particular ebook can be read and printed (i.e., a usage permission), for a $10 fee (i.e., an obligation to pay) and a maximum of 5 pages can be used for preview purposes (i.e., a count constraint). Additionally, each time the ebook is used, Libby, Renato, and Dale (the rights holders) receive a percentage of the fee.

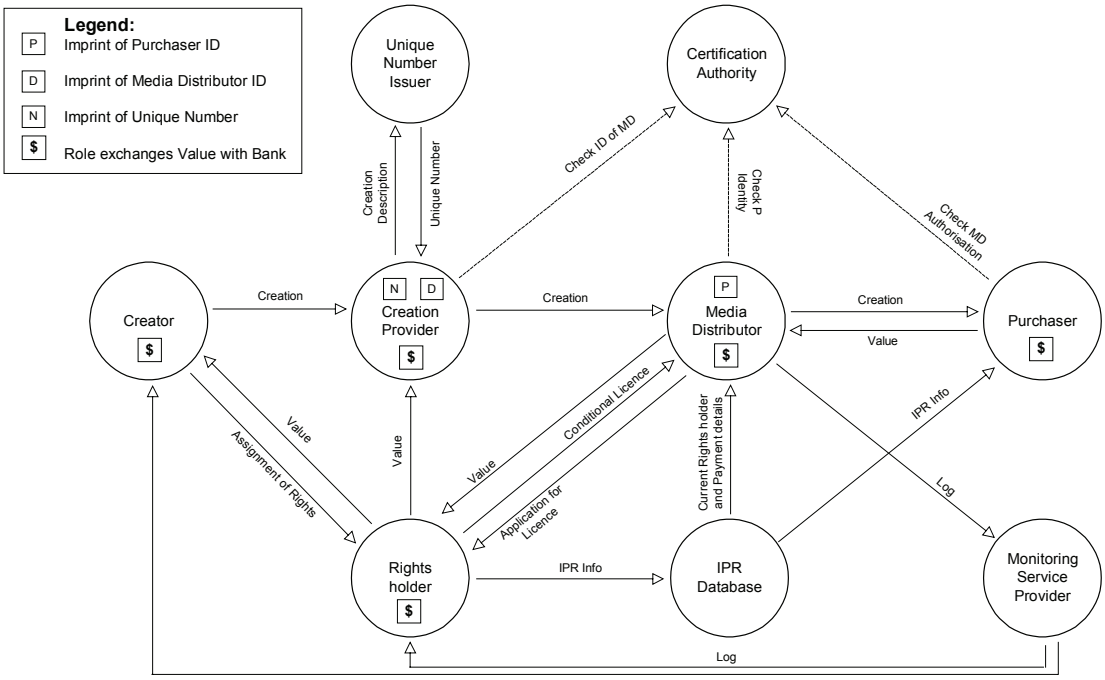
RIGHTS CLEARANCE & BUSINESS MODEL

After identifying and describing the key-entities and relations of DRM functionality, it is interesting to consider the aforementioned observations in the context of a more general business model. The aim is to investigate inherent weaknesses of on-line rights clearance activities and trace pitfalls that are likely to arise. Eventually, technology potentials will be investigated for tackling these weaknesses.

General Architectural Model

For the purposes of our investigation we will use the business model developed as part of the IMPRIMATUR Project (ESPRIT 20676) (IMPRIMATUR). The validity of this model was further certified

Exhibit 1.



via its subsequent adoption by the TRADEX (TRial Action for Digital object EXchange) Project (IST 21031) (TRADEX). For an extensive description of this model in the context of a cultural information system, the interested reader is referred to (Tsolis 2005).

The actors (stakeholders) identified in this model are:

- The **Creator** is the author of the copyrighted work.
- The **rights-holder** (or copyright owner), acts of behalf of the **Creator** and is responsible for licensing the use of the creation. Specifically, he defines the conditions of use, records the IPR information at a registry and collects the royalties deriving from trading of the works which he is in charge to administer.
- The **content provider** (or service producer), is in charge to prepare content for being traded electronically, and thus, for example, to embed into creations those mechanisms that will allow the tracking of copyright (watermarks). This player has to employ the necessary technological means so as to ensure that copyright can always be protected.
- The **media distributor** (or service provider), who has the responsibility to distribute to purchasers the creations, and thus to satisfy the request of his clients. This involves re-assuring that the IPR on the distributed material is protected and the related fees paid. This actor requires accessing the databases where IPR information is stored and using all the technological means needed to protect the copyright of the creations he trades (watermarking, cryptography, secure protocols). Moreover, he will have to offer the purchasers electronic licenses that determine the permissions, constraints and obligations of content use, as well as provide the authors, right-holders and other authorized actors a set of services to monitor and control the trading of their works.

- The **IPR Database** or register, is the repository of all information related to the intellectual properties of copyright protected works, and has to be accessible at different levels of detail and confidentiality. For instance, the information useful for identifying the creations and detailing the licensing rules is of particular importance and will have to be persistently maintained.
- The **Unique Number Issuer**, a naming registration authority who will be responsible for assigning a unique identifier to each creation, for facilitating its tracking.
- The **Monitoring Service Provider** or controller, who will be a Trusted Third Party (TTP) responsible for monitoring that all transactions have been carried out legally.
- The **Certification Authority**, which is also a TTP, with the task to authenticate all actors, by means of electronic certification.

It is evident by the aforementioned analysis that besides the need of establishing trusted organizations, there are cases where technological solutions are necessary to facilitate secure and effective electronic trade, without violating intellectual property rights.

Technology Insertion Points

Following the description of the key actors, it is important to outline the technologies necessary to facilitate electronic trade and clearly situate their functionality within the rights clearance framework.

- **Relational databases,** can serve as the repository infrastructure that will store all information required by the framework.
- **Communication protocol,** will allow different components to seamlessly communicate. As suggested by the diagram depicting the IMPRIMATUR business model, engineering an information system for performing electronic trade, would require the existence of many distributed functional components. Employing a standardized communication protocol would make binding between components more loosely-coupled and greatly benefit the reusability of components and extensibility of the framework.
- **IPR Metadata standards,** are essential for representing intellectual property information in an interoperable manner. These standards are particularly important for the **IPR Database** and **Rights holder** actors and its proper use and adjustment will favor the openness of the developed framework.
- **Rights Expression Language**, will try to cope with the increased level of complexity stemming from the number of conditions, restrictions and obligations included in the license documents. The **Rights holder** along with the **Media Distributor** will be the main consumers of this technology and is particular important for implementing a valid rights clearance service.
- **Technological Protection Means** such as watermarking, encryption etc, are the key functional component used for the protection and management of intellectual property rights. The DRM framework requires for a means to prevent unauthorized users from violating the intellectual property rights of traded content. In the case of watermarking (Tsolis 2001), copyright information is invisibly embedded inside the image digital content and technological evidence of the image ownership can be obtained by extracting this information. The embedded information typically corresponds to the **Rights holder** copyright notice and according to the aforementioned business model, the player that benefits more from utilizing this technology is the **Content Provider**.

- **Uniform resource identifiers**, are the cornerstone of services involving transaction tracking, since all entities need to be both identified and described uniformly. Identification should be accomplished via open and standard mechanisms that will facilitate the association of metadata records with creations. Open standards such as Uniform Resource Identifiers (URI) and Digital Object Identifiers (DOI), as well as the emerging ISO International Standard Textual Work Code (ISTC) are typical schemes for producing uniform resource identifiers.

RIGHTS CLEARANCE TECHNOLOGIES

The purpose of this section is to elaborate on the technologies that are more tightly related to on-line rights clearance and not DRM in general.

Communication Standards

Traditionally, information systems are architected using a component-based approach. Typically, the distinct components of the information system are closely interrelated, in such a way that modifications in any one of them subsequently causes extensive changes to other parts. This fact restricts their maintainability and limits their future expansion. Web Services are a set of open standards and protocols that were introduced to increase the reusability and interoperability of the components, by making the binding between them more loosely-coupled. Further elaboration on the topic of web services is out of the scope of this chapter, but the interested reader can refer to (Tsolis 2005).

IPR Metadata Standards

Independently of the adopted rights protection and management strategy, information is considered of vital importance. It is the information that allows the rights administrator to check the validity of content use, to trace potential usage violations, to grant the copyright of an artwork, etc. Information is also the mean that allows the end user to communicate with the copyright holder in order to file a request for using the copyright protected content or acquire the pricing policy of an artwork available on-line. The data comprising this type of information concerns various aspects of object property status such as, a) the intellectual property rights owner b) the intellectual property rights holder in case he is different from the owner c) communication details of the rights holder d) technological means used to protect and manage property rights, etc.

This type of information should accompany the digital artwork and be easily and directly accessible. The amounts of information that is related with a digital object and describe their technical and semantic characteristics are addressed by the term metadata. The set of metadata is intended to capture the information that the content creator chooses to preserve. With regards to the protection and management of intellectual property rights, it is very important that the set of metadata chosen to document the digital artwork, also incorporates data related to intellectual property. These data will formulate the means on which digital rights management systems will base their functionalities. The need for including rights related metadata has been recognized by dominant standardization bodies and is reflected to some of the most widely accepted metadata standards.

Open standards were established to facilitate the description of digital resources. The introduction of XML (Extensible Markup Language) (XML) by W3C has launched numerous resultant languages, protocols and technologies, which are commonly used today by both research projects and commercial applications. XSD (XML Schema Definition) [XSD] and RDF (Resource Description Framework) (RDF) have standardized the processes of defining metadata sets and characterizing resources. In order to accommodate the requirements of vertical applications, specialized metadata sets were also introduced, such as Dublin Core (DC) (DCMI), DIG35 (DIG35), MPEG-7 (MPEG7) to name only a few.

Amongst the various metadata standardization initiatives, Dublin Core (DC) (DCMI) has gained significant visibility and appeal. Dublin Core is a metadata standard that supports the diversity, convergence and interoperability of digital cultural objects and aims at supporting a wide range of business models. The basic schema proposed by Dublin Core is a simple content description model, defined by its 15 elements, out of which four are related with intellectual property rights namely, creator, publisher, contributor, rights.

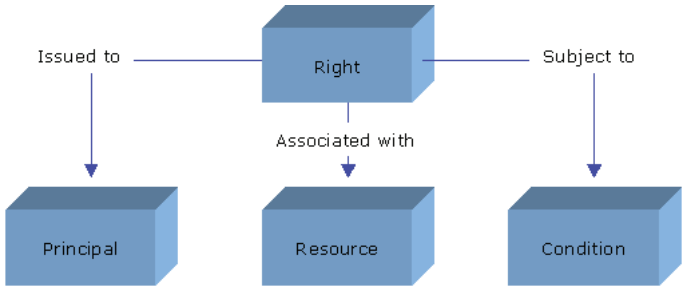
The Digital Image Group (DIG) [DIG35] is a non-profit cooperation between the industrial players of digital image such as software companies, consumers of digital images, etc. The primary goal of DIG35 is to establish an open framework for the exchange of ideas concerning the investigation, implementation and exploitation of methods and technologies that will boost the market related to digital imaging. This metadata standard is already being widely used in simple end-user devices and even to worldwide networks. DIG35 constitutes a rather extensive metadata set and includes information for a large set of digital image technical and semantic characteristics. Despite the fact that DIG35 is mainly oriented to digital images, the intellectual property related metadata are valid for all different types of multimedia content. The total amount of DIG35 metadata that are directly or indirectly related to intellectual property rights can be divided in 7 categories namely, names, description, dates, exploitation, digital rights management system, identification info and communication info.

Rights Expression Languages

MPEG-REL

MPEG - Rights Expression Language is a machine translatable description language, suitable for defining intellectual property rights, grants and licenses. Its role, in the context of rights clearance, is to provide a flexible and interoperable scheme for large scale consumption of digital objects and facilitate the distribution of digital content while protecting its intellectual properties. The Rights Expression Language defines the linguistics for expressing rules through rights statements. License rules can be rather simple such as, “this content is allowed to be replicated or reproduced” or more complicated such as, “this content is allowed to be reproduced on Tuesday on 7 of March and at 6:00 am, under the condition that the reproducing device satisfies a number of criteria”. Such expressions are likely to be created for every person that has the authority to transfer the copyright of protected content. Rights Expression Language is considered a fundamental part of MPEG-21 (MPEG21) mainly due to the intention of MPEG group in establishing a protocol that will allow heterogeneous systems to seamlessly communicate. Thus, the existence of a standardized language for incorporating digital content rights into machine understandable licenses is considered very important. The aim of this section is to investigate the REL data model, analyze its structure identify the key-components and summarize the relevant technological platforms.

Figure 6. REL Data Model



The REL data model (REL), as realized by MPEG-21, incorporates a simple and extensible data model for representing the basic concepts and components. Specifically, it is consisted of four basic entities and the relations among them. The following diagram depicts the fundamental entities and their interrelations.

- **Principle:** The principle entity models the potential users involved in the process of distribution, usage, and content consumption.
- **Right:** Right is the "action" the practice of which is being transferred to the Principle.
- **Resource:** Resource is considered the "object" the rights of which are being transferred to the principle.
- **Condition:** The condition entity determines the terms, restrictions and obligations under which the right is allowed to be exercised.

The four aforementioned entities, comprise a grant. By itself, a grant is not a complete rights expression that can be transferred unambiguously from one party to another. A full rights expression is called a license. A typical license consists of one or more grants and an issuer, which identifies the party who issued the license. In case the licence publisher wants to grant distribution rights to an e-shop or DRM, he signs a distribution license. The grant of a distribution license, instead of the right to be tranfered, contains a new grant as seen in Figure 7 .

The procedure of implementing the MPEG-21 REL initiated with the establishment of a set consisting of 48 requirements. Experts from heterogeneous sectors agreed that the fulfilment of the aforementioned requirements would suffice to guarantee the success of the initiative. The set of requirements extends to various fields ranging from the language expressivity to security. Eventually, the XrML (eXtensible Rights Markup Language) (XrML) technological platform was selected to serve as the groundwork of MPEG-21 REL. To promote interoperability, MPEG has developed the Rights Data Dictionary (RDD) to ensure that the semantic interpretation of new verbs is unambiguously understood. The RDD comprises a set of clear, consistent, structured, integrated and uniquely identified Terms to support the MPEG-21 REL. As well as providing definitions of Terms for use in the REL, the RDD specification is designed to support the mapping and transformation of metadata from the terminology of one namespace (or Authority) into that of another namespace (or Authority) in an automated or partially-automated way, with the minimum ambiguity or loss of semantic integrity.

Figure 7. MPEG 21 - REL data model

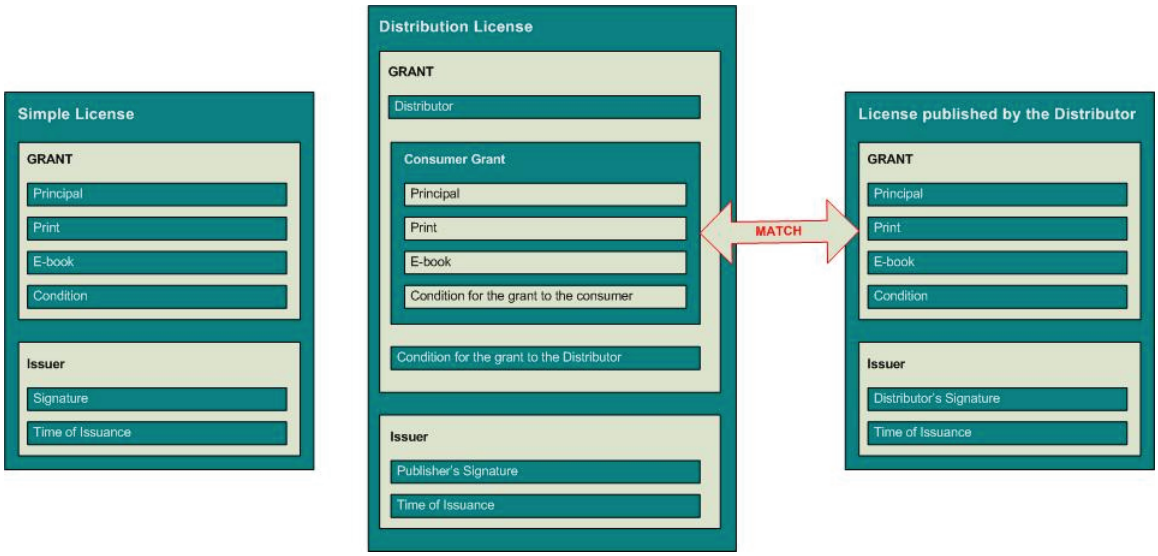
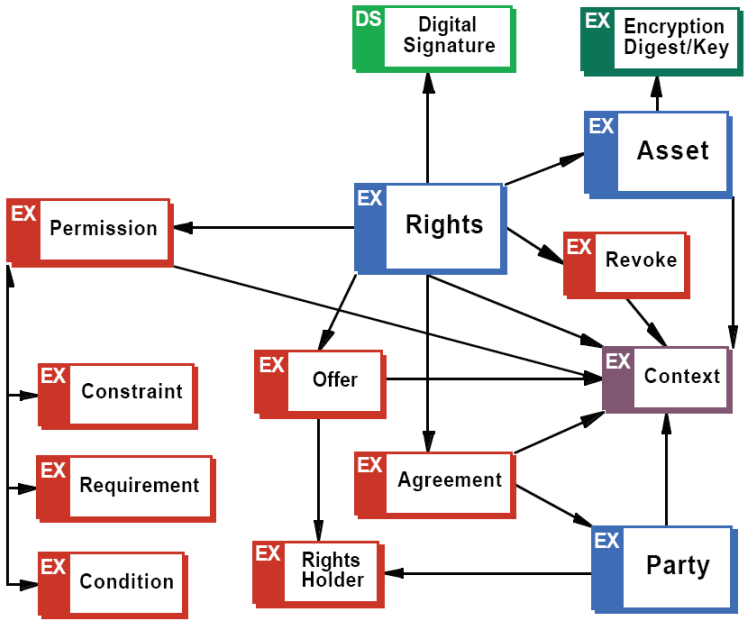


Figure 8. The ODRL foundation model



Open Digital Rights Language (ODRL)

ODRL complements existing analogue rights management standards by providing digital equivalents, and supports an expandible range of new services that can be afforded by the digital nature of the assets in the Web environment.

ODRL is a standard language and vocabulary for the expression of terms and conditions over assets. It covers a core set of semantics for these purposes including the rights holders and the expression of permissible usages for asset manifestations. Rights can be specified for a specific asset manifestation or could be applied to a range of manifestations of the asset. *ODRL* is focused on the semantics of expressing rights languages and definitions of elements in the data dictionary.

ODRL does not enforce or mandate any policies for DRM, but provides the mechanisms to express such policies. Communities or organisations, that establish such policies based on *ODRL*, do so based on their specific business or public access requirements. *ODRL* depends on the use of unique identification of assets and parties The *ODRL* model is based on an analysis and survey of sector specific requirements (including models and semantics), and as such, aims to be compatible with a broad community base.

ODRL is based on an extensible model for rights expressions which involves a number of core entities and their relationships. This *ODRL* Foundation Model is shown in Figure 8.

The model, as shown in Figure 8, consists of the following three core entities: Assets, Rights, Parties. The Assets include any physical or digital content. The Assets must be uniquely identified and may consist of many subparts and be in many different formats. The Rights include Permissions which can then contain Constraints, Requirements, and Conditions. Permissions are the actual usages or activities allowed over the Assets (e.g., Play a video Asset). Constraints are limits to these Permissions (e.g., Play the video for a maximum of 5 times). Requirements are the obligations needed to exercise the Permission (e.g., Pay $5 each time you Play the video). Conditions specify exceptions that, if become true, expire the Permissions and renegotiation may be required (e.g., If Credit Card expires then all Permissions are withdrawn to Play the video). The Parties include end users and Rights Holders. Parties can be humans, organisations, and defined roles. End users are usually the asset consumers. Rights Holders are usually parties that have played some role in the creation, production, distribution of the Asset and can assert some form of ownership over the Asset and/or its Permissions. Rights Holders may also receive royalties.

Most entities in the model can support a specific Context. A Context, which is relative to the entity, can describe further information about that entity or the relationship between entities. For example, the Context of an Agreement may specify the date of the transaction, the Context of a Party may specify their role.

The Asset entity (sometimes referred to as a Work, Content, Creation, or Intellectual Property), is viewed as a whole entity. If the Rights are assigned at the Asset's subpart level, then such parts would require to also be uniquely identifiable. However, *ODRL* can specify constraints on subparts of the asset. Additionally, Assets can be identified as to their layer of intellectual property as defined by the IFLA model. These include Work, Expression, Manifestation, and Item. These features also allow rights to be expressed over non-tangible assets and individual instances.

These core Entities together allow for a wide and flexible range of *ODRL* expressions to be declared. Additionally, the expressions can be digitally signed.

Watermarking

Watermarking can be considered as an integrated service, providing protection and assisting management of intellectual property rights. Watermark technology incorporates encryption methods to ensure unambiguous and categorical proof of ownership, as well as image processing techniques for conveying

useful information inside the digital content, (Cox 2002). The level of functionality that can be achieved by the proposed scheme depends upon the usage policy of the conveyed information. A typical scenario involves an organization that owns a great collection of digital images and is willing to sale high quality copies of collection objects for a standard price. Prior to delivery, the organization embeds a digital watermark inside the image content. The watermark serves three different purposes, a) give proof of ownership, b) identify the transaction that took place and c) correlate the transaction description with the specific image copy. All details necessary for describing a transaction are included within the image metadata information maintained within the content provider's database infrastructure.

In this case, the input arguments of watermark embedding mechanism consist of two integer numbers. The first number corresponds to the encryption key while the second to the transaction identification number. The encryption key is used for invoking the core cryptographic module that guarantees for watermark's security. It's a unique private number that constitutes the key of the system's cryptographic attributes and is used by the right's holder for proving his ownership.

Thus, there is a need for universal administration of such numbers in order to avoid conflicts and irresolvable disputes. This role is appointed to uniform resource identifier systems that will be described at a later section. If we consider that a uniform resource identifier is consisted of two distinct numbers, a prefix and a suffix, the watermarking scheme performs the following actions. By using the prefix number as seed for cryptographically encoding the watermark information within the image digital content, the proposed scheme exploit's the handle system administration facilities for resolving ownership disputes. The suffix is an independent number selected by the institution protocol service; it is administered locally and can be regarded as the transaction identification number. This number is encoded inside the digital image content and can be retrieved by the decryption mechanism.

Unique Resource Identifier

Open object identification systems are deemed very important for distributed environments like the ones encountered in electronic commerce. Global identifiers should allow for unique identification of digital objects in order to facilitate the operations of rights clearance.

Handle System

The Handle System, (Kahn 2006), is a distributed information system designed to provide an efficient, extensible and confederated name service that allows any existing local namespace to join the global handle namespace by obtaining a unique Handle System naming authority. Local names and their value-binding(s) remain intact after joining the Handle System. Any handle request to the local namespace may be processed by a service interface speaking the Handle System protocol. Combined with the unique naming authority, any local name is guaranteed unique under the global handle namespace.

It is probably best to view the Handle System as a name-attribute binding service with a specific protocol for securely creating, updating, maintaining, and accessing a distributed database. It is designed to be an enabling service for secured information and resource sharing over networks such as the public Internet. Applications of the Handle System could include metadata services for digital publications, identity management services for virtual identities, or any other applications that require resolution and/or administration of globally unique identifiers.

Handle Namespace

Every handle consists of two parts: its naming authority, otherwise known as its prefix, and a unique local name under the naming authority, otherwise known as its suffix:

<Handle> ::= <Handle Naming Authority> "/" <Handle Local Name>

The naming authority and local name are separated by the ASCII character "/". The collection of local names under a naming authority defines the local handle namespace for that naming authority. Any local name must be unique under its local namespace. The uniqueness of a naming authority and a local name under that authority ensures that any handle is globally unique within the context of the Handle System.

For example, "1082.5000/image1" is a handle for a digital image published on a cultural website. Its naming authority is "1082.5000" and its local name is "image1". The handle namespace can be considered a superset of many local namespaces, with each local namespace having a unique naming authority under the Handle System. The naming authority identifies the administrative unit of creation, although not necessarily continuing administration, of the associated handles. Each naming authority is guaranteed to be globally unique within the Handle System. Any existing local namespace can join the global handle namespace by obtaining a unique naming authority so that any local name under the namespace can be globally referenced as a combination of the naming authority and the local name as shown above.

Naming authorities under the Handle System are defined in a hierarchical fashion resembling a tree structure. Each node and leaf of the tree is given a label that corresponds to a naming authority segment. The parent node notifies the parent naming authority of its child nodes. Unlike DNS, handle naming authorities are constructed left to right, concatenating the labels from the root of the tree to the node that represents the naming authority. Each label is separated by the octet used for ASCII character "." . Each naming authority may have many child naming authorities registered underneath. Any child naming authority can only be registered by its parent after its parent naming authority has been registered. However, there is no intrinsic administrative relationship between the namespaces represented by the parent and child naming authorities. The parent namespace and its child namespaces may be served by different handle services, and they may or may not share any administration privileges.

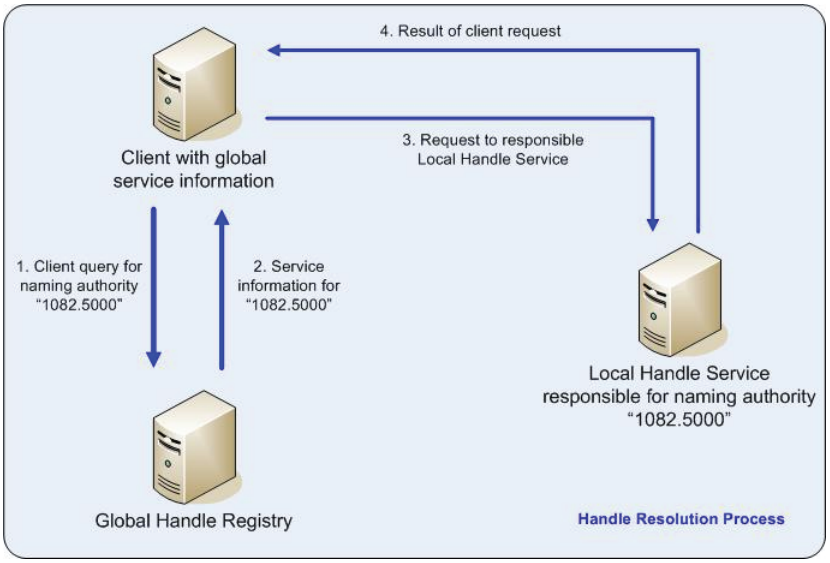
Handle System Architecture

The Handle System defines a hierarchical service model. The top level consists of a single handle service, known as the Global Handle Registry (GHR). The lower level consists of all other handle services, generically known as Local Handle Services (LHS).

The Global Handle Registry can be used to manage any handle namespace. It is unique among handle services only in that it provides the service used to manage naming authorities, all of which are managed as handles. The naming authority handle provides information that clients can use to access and utilize the local handle service for handles under the naming authority.

Local Handle Services are intended to be hosted by organizations with administrative responsibility for handles under certain naming authorities. A Local Handle Service may be responsible for any number of local handle namespaces, each identified by a unique naming authority. The Local Handle Service and its responsible set of local handle namespaces must be registered with the Global Handle Registry.

Figure 9. Example of handle resolution process



The Global Handle Registry maintains naming authority handles. Each naming authority handle maintains the service information that describes the "home" service of the naming authority. The service information lists the service sites of the given handle service, as well as the interface to each handle server within each site. To find the "home" service for any handle, a client can query the Global Handle Registry for the service information associated with the corresponding naming authority handle. The service information provides the necessary information for clients to communicate with the "home" service.

Figure 9 shows an example of a typical handle resolution process. In this case, the "home" service is a Local Handle Service. The client is trying to resolve the handle "1082.5000/1" and has to find its "home" service from the Global Handle Registry. The "home" service can be found by sending a query to the Global Handle Registry for the naming authority handle for "1082.5000". The Global Handle Registry returns the service information of the Local Handle Service that is responsible for handles under the naming authority "1082.5000". The service information allows the client to communicate with the Local Handle Service to resolve the handle "1082.5000/1".

To improve resolution performance, any client may choose to cache the service information returned from the Global Handle Registry and use it for subsequent queries. A separate handle caching server, either stand-alone or as a piece of a general caching mechanism, may also be used to provide shared caching within a local community. Given a cached resolution result, subsequent queries of the same handle may be answered locally without contacting any handle service. Given cached service information, clients can send their requests directly to the correct Local Handle Service without contacting the Global Handle Registry.

CASE STUDY: SilkDRM

SilkDRM is a new Digital Rights Management System that provides on-line Rights Clearance for digital images (or other digital assets). Individuals and/or institutions who own the Intellectual Property Rights of digital images can use SilkDRM in order to ensure the authenticity of their content. Additionally, the system can be authorized by the right holder to issue distribution licenses for the digital resources. This is done by signing a special license which describes the set of rights that can be assigned for a specific resource, as well as the equivalent necessary conditions under which the assignment can be made.

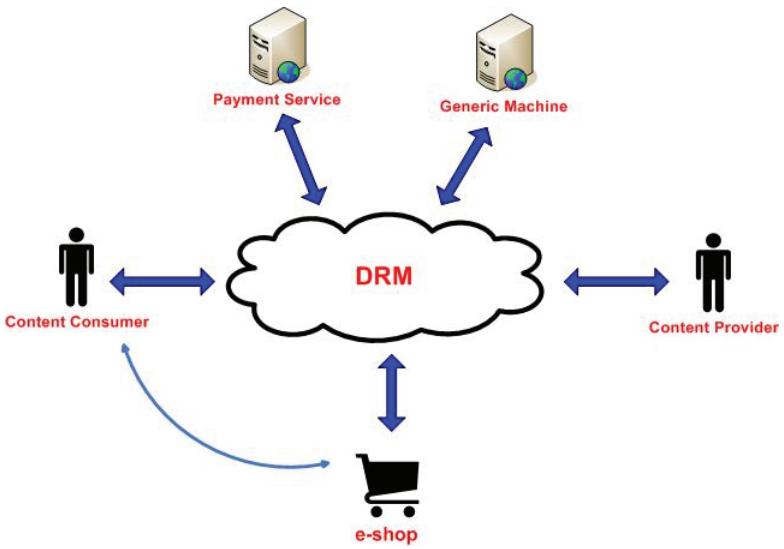
System Functionality

SilkDRM is accessible to internet users through its easy to use web interface. A number of Cultural Institutions who created websites for their digitized content, used the system in order to document their rights on the content and as a mechanism for the production of digital licenses on its use. In practice, the Cultural Institutions registered their content in the system and in parallel, in the webpages presenting the digital assets they provide a hyperlink to SilkDRM. By following that hyperlink, the visitor is directed to the corresponding page from where he can retrieve information about the intellectual propery rights binding the digital resource, as well as the conditions for obtaining a use license. If the rights holder decides to use digital watermarking for protecting his content, he is able to embody the unique code created by SilkDRM in the watermark. In this case, the detection of the watermark can lead one to the corresponding page of the DRM (through the code retrieved).

System Users

The two basic system user types involved in SilkDRM are Content Providers and Content Consumers. Content Providers include single users or members of a Cultural Organization aiming in registering

Figure 10. SilkDRM system functionality



their digital content in order to authenticate their ownership over the content and pursue its commercial exploitation. A Content Consumer is browsing the DRM webpages, receiving intellectual property information on specific digital resources and potentially apply for a use license. A Content Consumer can be not only an individual but also an e-shop. In this scenario, the rights holder has assigned the distribution of his content to an e-shop. The e-shop contacts the DRM in order to retrieve information concerning the terms and conditions set by the owner for the selling of the digital resource and present them to the potential buyers. In case the item is sold, the DRM is responsible for publishing the corresponding use license and forward it to the e-shop. SilkDRM is able to communicate with various payment services over the web, achiving this way transaction monitoring as well as the validation of published licenses. Beside the aforementioned users, any generic machine, implementing a specific communication protocol based on standard web technologies, is able to connect and transact with the system.

Content Providers

When a content provider browses our web pages for the first time, he is prompted to fill in an application form for the creation of an account. This form includes personal and corporate information in case the user acts on behalf of an organization/institution. SilkDRM administrator processes the application and contacts the applicant in order to retrieve information about the resourses that he intends to register in the DRM. The next step includes the preparation of a legal contract, in which the applicant declares that he or the institution that he represents is the intellectual property rights holder of the content that will be registered in SilkDRM. When the contract is signed, a new account is created and the applicant becomes a registered user of the system. The first account created, is an account of the organization administrator having full rights to all system functionalities. The administrator can create new accounts and assign user rights to the people he chooses. The “register procedure” for a new digital resource in the DRM, is implemented by filling in some forms containing descriptive information about the resource and its intellectual propery. In parallel, a preview picture (eg. thumbnail) can be uploaded. In case the rights holder has decided to watermark the resource, he can ask the DRM to produce a unique identification number, in order to be embedded in the watermark. SilkDRM can also produce a handle for the resource, in order to facilitate a unique addressing method. The registration of digital assets to the DRM can also be acomplished through a batch process, during which SilkDRM processes a set of xml files (one for each resource), constructed according to a model given to the user. The user can navigate through his collection and edit the registerd information. For each digital resource in SilkDRM, the rights holder can authorize the system to publish use licenses, by signing a “distribution license”. This procedure is accomplished by selecting the “Create Distribution License” operation for one or more resources. The licese to be created will contain the conditions under which the DRM will be able to publish licenses, granting some of the rights “play”, “print”, “copy”, “adapt”, “embed”, “extract”. The set of conditions, could be one or more of the following:

- The consumer is obliged to pay a certain fee (There is a selection available between payment methods. A payment service can be chosen, or a bank account can be assigned for a deposit to be made)
- Time Limit Imposition (The right granted can be exercised not before a certain date and not after a certain date)

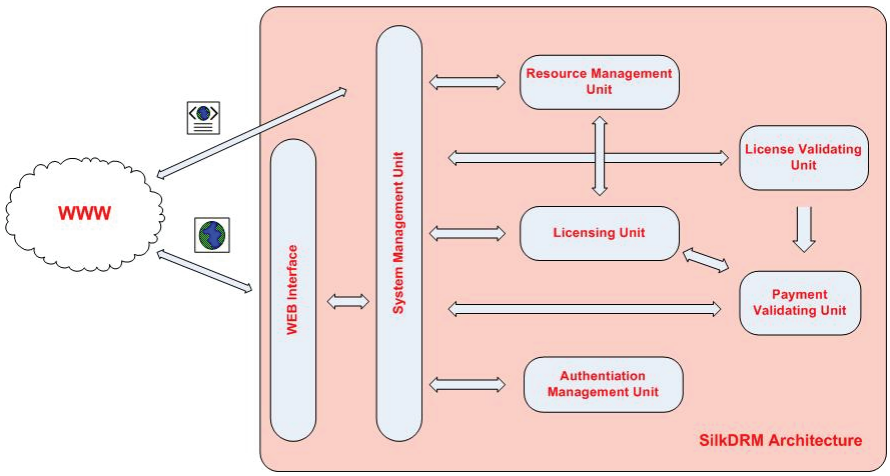
- Exercise Limit (There is a specific number of executions allowed for the right(s) granted)
- Geographical Restrictions (The right granted can be exercised only in a specified country)

When the conditions are selected, the license is published and the DRM acquires the authorization to create and publish use licenses for specific digital resources, due to the conditions of the distribution license signed. The last service offered to the content provider, is a license management service. The user can browse a list of all the licenses published by SilkDRM for his digital resources. For each license, the system provides information about the principal to whom the rights are granted as well as the potential use of the Validator. The Validator is a subsystem of the SilkDRM which is able to read a license and respond whether it is valid or not. This is accomplished by checking the fullfilment of the conditions set (e.g., fee payment, time limitations). The Validator is not a single "valid" or "not valid". It can indicate the specific terms that are not satisfied.

Content Consumers

The two main services offered to a content consumer, are browsing the collections of registered resources and managing obtained licenses. The resources collections are sorted by rights holder but there is also a search engine available. For each digital resource exists a page demonstrating all available information (e.g., for a digital image elements such as title, legent, description, rightsholder, creator, digitizer etc. are presented). In case the appropriate distribution license is issued, the choice of obtaining a use license is provided. If the user selects to obtain a license, he will be directed to the license creation page. In this page, the user can see all the rights the DRM is empowered to distribute and select those he wants to receive a license. For each right, the consumer must agree with the conditions set by the rights holder and finally affirm that he wants to obtain the license. Finally the license is published and sent to the user via e-mail. The e-mal, except from the license attached, contains a hyperlink to the Validator, where the obtained licese can be validated. The licence management service, provides a list of all the licenses granted to the user. The licenses are sorted by date and are accompanied by information about the resource and a link to the Validator.

Figure 11. SilkDRM system architecture



System Architecture

The system comprises of six distinct units, the functionality of which is described in the following paragraphs. These units are designed and constructed independenly, as the main goal was the production of a system with the highest possible maintenability and scalability.

System Management Unit
This is the unit that executes the system operation protocol. It receives requests from the web interface or another input (eg. Web service) and orchestrates system units by triggering the appropriate ones at a time, passing messages to them.

Resource Management Unit
This particular unit is responsible for the process of registering and documenting a digital resource. It also undertakes the task of retrieving the documentation and potentially editing and deleting it. Additionally, the Resource Management Unit embraces two distinct sub-units. The Unique Indentifier Generator and the Handle Creation Unit which create and register handles for the unequivocal addressing of the digital items.

Licensing Unit
This is the unit responsible for creating and processing licenses for digital resources. For each item, the unit can check whether a distribution licese has been published. If such a license is present, the unit is able to read it and dynamically create the terms and conditions a content consumer must agree with, in order to obtain a use license. When a license is published, the unit sends it via e-mail to the holder.

License Validating Unit
This unit receives a license as an input, and checks whether the conditions set in order the grant to be valid, are satisfied. For checking the validity of the payments, the unit is able to communicate with the Payment Validating Unit. Special response messages are produced, according to the results of the validity test. In case a license is not valid, the unit provides detailed information on which of the conditions are not met.

Payment Validating Unit
Payment Validating Unit's main task, is checking whether a fee is payed, according to the conditions set in a specific license. The unit offers the ability of validating a payment, due to the received input by the rights holder or a Payment Service.

Authentication Management Unit
This unit manages the process of creating, editing and deleting user accounts. According to the type of the user logged (content creator or content consumer), it defines the available operations to him on the system. The unit also manages different user rights, offering each user only the services defined by the rights assigned to him by the administrators.

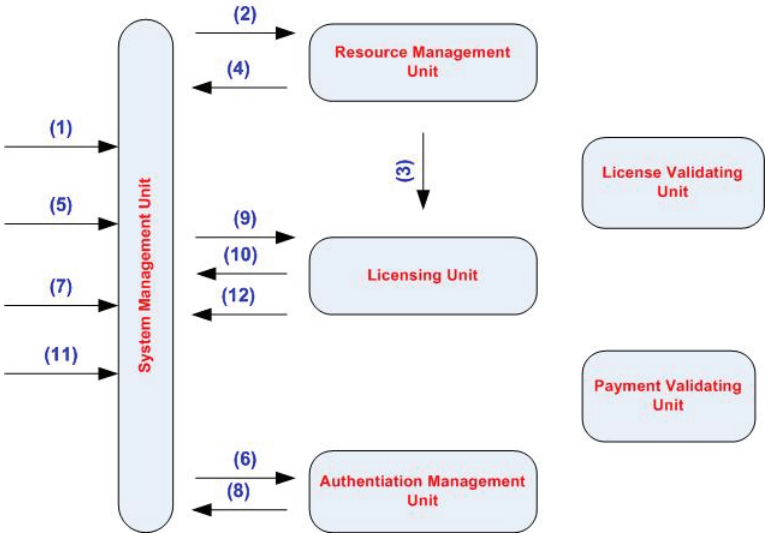
Implementation Details

Registering a Digital Object

The process followed for registering a digital object in SilkDRM, is described in this paragraph.

1. An application is received by System Management Unit, from a system user wanting to register a digital resource.
2. System Management Unit contacts Authentication Management Unit, to certify that the user is permitted to perform the action.
3. Authentication Management Unit responds whether the user has the right to register the content or not.
4. If the response received is positive, Resource Management Unit is initiated in order to start the registering process.
5. Resource Management Unit provides all necessary data, for the creation of the registering interface. In case of digital images, SilkDRM uses the DIG-35 Intellectual Property Rights Metadata set and when handling other digital resources the Dublin Core Metadata set is used for the registration process.
6. Content Provider fills in the forms with the appropriate data
7. Resource Management Unit receives and stores the data, using a selected format. Relational Database schemes are used for the data storage. The unit is able to export inserted data in xml files. According to the user's demands, the Unique Indentifier Generator and the Handle Creating Unit will be triggered. The Handle Creating Unit includes a Handle Server playing the role of the Local Handle Service responsible for the naming authority "1082.xxxx" Finally the output (the results of the registration process, the unique identification number, the handle etc.) is passed to the content provider (through the System Management Unit).
8. The user wants to create a distribution license for the resource.

Figure 12. SilkDRM flow-chart



9. Licensing Unit is called, for the creation of the license.
10. License Unit provides the necessary data for the production of the license creation interface. For the creation of a license, MPEG – Rights Expression Language is used.
11. The user fills in the form selecting rights and conditions and submits it, thus giving the order for the creation o a license.
12. Licensing Unit receives the data, creates the license, and e-mails it to the content provider. The licenses are created and stored in the xml format specified by the MPEG-REL specifications.

The Licensing Process

The next bullets describe the process followed for the creation of a digital license.

1. A system user (content consumer) wants to browse the collections of registered digital items
2. Resource Management Unit is triggred for the presentation of the collection items.
3. Resource Management Unit contacts Licensing Unit to retrieve information about whether a distribution license is published, for each digital resource it will present.
4. Resource Management Unit presents the documentation for the registered items. In case a distribution license is published, the content consumer has the ability to request a lisence for the resource.
5. The user makes a license request for a specific digital resource.
6. System Management unit calls Authentication Management Unit to authenticate the user.
7. The user logs on the system if he has an account, or is taken through the steps to create one
8. Authentication Management Unit authenticates the user
9. The request is passed to the Licensing Unit
10. Licensing Unit retrieves and reads the distribution license, in order to produce the forms for the creation of the license.
11. The User accepts the licensing conditions and requests the finalization of the process.
12. Licensing Unit receives the final data, creates and stores the license and finally sends it to the user via e-mail.

Watermarking

Watermarking functional component incorporates multiple functionalities inside the content provider's operational chain. An Application Protocol Interface (API), was developed to support two basic interfaces for embedding and detecting digital watermarks.

The interface responsible for the embedding operation requires five different arguments from the service user:

- **Encryption key:** An integer value that, when used in conjunction with the hash function, produces a secret number appropriate for the invocation of the cryptographic module.
- **Transaction identification number:** An integer value that will be encoded as an imperceptible watermark inside the image digital content.
- **Input image file:** The binary data of the original unwatermarked digital image.
- **Output image file:** The binary data of the resulting watermarked digital image.

- **Strength modifier:** An integer between 1 and 4 indicating the embedding strength of the watermark procedure. A value of 4 produces more robust watermarks, but introduces more distortion to image quality.The interface response returns a zero value on success of the watermarking process and a negative value in case of failure.Respectively, the interface responsible for detecting digital watermarks requires the following input arguments.
- **Decryption key:** The integer used during the embedding procedure. With regards to the specific watermarking system, the encryption and decryption keys must be identical in order for the detection to be successful.
- **Input image file:** The binary data of the image under detection. The detector's response, as already mentioned, is consisted of two parts.
- **Detection intensity:** Indicating the existence possibility of the watermark inside the image content. If this value is well above a predefined threshold the watermark is considered detected.
- **Decrypted information:** An integer value representing the number encoded during the embedding procedure. Normally, this number corresponds to the transaction identification number.

CONCLUSION

Rights Clearance has always been an important issue in human transactions. The Internet revolution made the issue a lot more complicated since we passed from the material to the digital substance of an asset. Multiple copies of a digital resource exist over the internet, thus making the monitoring of its use and the identification of its origin an extremely difficult task. Throughout this chapter, we described the rights clearance process in the physical and digital world and the ways it can be accomplished on-line through a Digital Rights Management system. Important issues concering a DRM system are the definition of key-entities and relations of its functionality, the way a digital resource is represented, protected bound with metadata sets, uniquely identified and the way rights are digitally expressed and assigned. Finally we present an application of all discussed attributes of a DRM system, in an existing system (SilkDRM) that provides on-line Rights Clearance for digital images (or other digital assets).

FUTURE RESEARCH DIRECTIONS

Future research involves integrating Rights Clearance as a fully functional component of second-generation DRM systems. More specifically, as opposed to first-generation DRM systems where the enforccment of encryption techniques allowed very limited access to content, second generation DRMs introduce more flexible content delivery schemes at the expense of balancing between a set of diverse features such as:

- Uniformly describe and identify an asset (both tangible or intangible).
- Adhere to a globally estrablished protocol for registering rights-holders as well as the set of rights they are allowed to grant.
- Support rights expression languages that are able to describe different types of property rights and facilitate their transfer to a person or an organization.

- Seamlessly co-operate with technological protecting means both for the tasks of copyright protection and transanction tracking
- Finally, to make all the above work in a unified e-commerce business model.

Each bullet can be considered as a different research field. Although several DRM systems have been developed none of them manages to successfully address all aforementioned aspects. A unified DRM system that operates over the internet is envisaged as the only plausible solution for providing consistent and bulletproof protection of Intellectual Property Rights.

REFERENCES

ContentGuard, http://www.contentguard.com

Cox, I., Miller, M. L. & J. A. Bloom. (2002) *Digital watermarking.* San Francisco, CA, USA: Morgan Kaufmann Publishers Inc.

DCMI, Dublin Core Metadata Initiative, Last checked: October 11 2007, <http://www.dublincore.org/>

DIG35, Digital Image Group - DIG35 Specification – Metadata for Digital Images. Last checked: 11 October 2007, http://www.i3a.org/i_dig35.html

DOI, Digital Object Identifier. Last checked: 11 October 2007, http://www.doi.org

IFLA, Functional Requirements for Bibliographic Records, IFLA Study Group on the Functional Requirements for Bibliographic Records, (Approved September 1997) K . G. Saur München, 1998. Not available, http://www.ifla.org/VII/s13/frbr/frbr.htm

IMPRIMATUR, Intellectual Multimedia Property RIghts Model and Terminology for Universal Reference, Not available, http://www.imprimatur.alcs.co.uk/index.htm

INDECS, Interoperability of data in e-commerce systems, Last checked: October 11 2007, <http://www.indecs.org>

ISTC, ISO International Standard Textual Work Code. Last checked: 11 October 2007, http://www.nlc-bnc.ca/iso/tc46sc9/istc.htm

Kahn, R. & Wilensky, R. (2006). A Framework for Distributed Digital Object Services. *International Journal on Digital Libraries*, *6*(2). Springer.

MPEG21, MPEG-21 Overview v5, Last checked: 11 October 2007, http://www.chiariglione.org/mpeg/standards/mpeg-21/mpeg-21.htm

MPEG7, ISO/IEC Moving Picture Experts Group. Last checked: 11 October 2007, < http://www.chiariglione.org/mpeg/standards/mpeg-7/mpeg-7.htm >

Open Digital Rights Language (ODRL), version 1.1 (2002) from http://odrl.net

OZAUTHORS, OzAuthors Online Ebook Store, Last checked: October 11 2007, http://www.ozauthors.com

RDF, Resource Description Framework. Last checked: 11 October 2007, http://www.w3.org/RDF/

REL (2003). The MPEG-21 Rights Expression Language, A White Paper, Rightscom Ltd,

Renato, I. (2001). Digital rights manegement (DRM) architectures. *D-Lib Magezine Article*, *7*(6).

Sun, S., Lannom, L., & Boesch, B. Handle system overview. *Internet Engineering Task Force (IETF) Request for Comments (RFC), RFC 3650*, November 2003 from http://www.handle.net

TRADEX, TRial Action for Digital object EXchange, Not available, http://www.iccd.beniculturali.it/download/tradex.pdf

Tsolis, G. K., Nikolopoulos, S. N., Kazantzi, N.V., Tsolis, D. K. & Papatheodorou, T. S. (2005, August 15-17). Re-Engineering digital watermarking of copyright protected images by using xml web services. *In Proc. of the Ninth IASTED International Conference on INTERNET & MULTIMEDIA SYSTEMS & APPLICATIONS (IMSA 2005)*, 264-270. Honolulu, Hawaii, USA.

Tsolis, G. K., Tsolis, D. K. & Papatheodorou, T. S. (2001). A watermarking environment and a metadata digital image repository for the protection and management of digital images of the hellenic cultural heritage. *Proc. IEEE International Conference on Image Processing 2001*, 566-569. Thessaloniki, Greece

URI, Uniform Resource Identifiers (URI): Generic Syntax, IETF RFC2396. Last checked: 11 October 2007, http://www.ietf.org/rfc/rfc2396.txt

WIPO, World Intellectual Property Organization, Last checked: October 11 2007, <http://www.wipo.int>

XML, eXtensive Markup Language. Last checked: 11 October 2007, http://www.w3.org/XML/

XrML, eXtensive rights Markup Language. Last checked: 11 October 2007, http://www.xrml.org

XSD, eXtensible Markup Language Schema, Last checked: 11 October 2007, <http://www.w3.org/XML/Schema>

ADITTIONAL READING

DCMI, Dublin Core Metadata Initiative, Last checked: October 11 2007, <http://www.dublincore.org/>

DIG35, Digital Image Group - DIG35 Specification – Metadata for Digital Images. Last checked: 11 October 2007, http://www.i3a.org/i_dig35.html

DOI, Digital Object Identifier. Last checked: 11 October 2007, http://www.doi.org

MPEG21, MPEG-21 Overview v5, Last checked: 11 October 2007, http://www.chiariglione.org/mpeg/standards/mpeg-21/mpeg-21.htm

MPEG7, ISO/IEC Moving Picture Experts Group. Last checked: 11 October 2007, < http://www.chiariglione.org/mpeg/standards/mpeg-7/mpeg-7.htm >

URI, Uniform Resource Identifiers (URI): Generic Syntax, IETF RFC2396. Last checked: 11 October 2007, http://www.ietf.org/rfc/rfc2396.txt

WIPO, World Intellectual Property Organization, Last checked: October 11 2007, <http://www.wipo.int>

XML, eXtensive Markup Language. Last checked: 11 October 2007, http://www.w3.org/XML/

XrML, eXtensive rights Markup Language. Last checked: 11 October 2007, http://www.xrml.org

XSD, eXtensible Markup Language Schema, Last checked: 11 October 2007, <http://www.w3.org/XML/Schema>