# Frontiers of DRM Knowledge and Technology

**Habtamu Abie**

Norwegian Computing Center, P.O.Box 114 Blindern, N-0314 Oslo, Norway

## Abstract

In today's digital world digital information can be copied and distributed with ease and little expense. While this makes life easier for law-abiding citizens, it also facilitates misuse, mass piracy and the violation of Intellectual Property Rights (IPR) causing revenue loss to many rights holders. Consumers are also concerned about their privacy, and therefore experience a need to be able to have control over their own personal information, including the manner of its acquisition and the use to which it is put. In the future world of ambient intelligence, digital content will be ubiquitous and people will interact with it in all areas of their lives, a situation that presents new challenges in the area of Digital Rights Management (DRM). There are many techniques that can be used by a DRM system to curtail infringements of IPR. Each one has its strengths and weaknesses, which must be weighed against each other along with the cost of acquiring, integrating and maintaining them. This paper likewise gives an overview of the frontiers of DRM knowledge and technology in the form of a brief survey. On the basis of this review of the present state of the art and activities in the field of DRM, the paper also charts trends and predicts developments.

**Key words:**
DRM Survey, IPR, Trusted Systems, Standards, Business and Distribution Models, Technologies, Societal Issues.

## 1. Introduction

In the traditional physical world, copying on a small scale was not economically viable, and copying on a large scale was controllable to a certain extent by legal measures. However, these traditional methods of piracy control were more physically-based and have proved difficult to transfer to the context of the digital world [62]. In the present digital world things are different. Digital information can be copied and distributed with ease and little expense. While this makes life easier for law-abiding citizens, it also facilitates misuse, mass piracy[1] and the violation of IPR causing revenue loss to many rights holders. It is therefore necessary to prevent such illegal activity, or at the very least to deter it and protect IPR. It is impossible to do this solely on the basis of technology [54]. It will be necessary to combine technology with good business models, the education of consumers, adaptive public policy and legislation, and efficient law enforcement.

All these should be developed together in conjunction rather than separately and in isolation. There is therefore a need to adapt a multidisciplinary approach and to explore all factors in all areas.

The purpose of copyright law is to protect the interests of creators of IP so that they derive revenue from their efforts, and thus be motivated to continue to produce IP to the benefit of society. Copyrights to IP are held by creators and balanced by "carefully considered exceptions" [62]. Therefore any successful solution must uphold and enforce the fundamental principles of copyright laws [1] which protect the rights and interests of creators, consumers and society at large. This means that it must safeguard the interests of IP owners, ensure that IP is efficiently distributed and easily accessible, and further the interests of society at large. As also pointed out in [57], this will require not just technology, no matter how sophisticated, but also that the distribution system is both credible and trustworthy. To be so, it must ensure that the services, software applications, and devices which protect and manage rights in connection with all kinds of IP in digital form, are neutral, secure, commercially reliable, trustedly interoperable.

The increased availability of sensitive digital information that has to be stored, and shared and distributed within and between organizations, makes it essential to secure this digital information. While valuable digital information products need protection from theft and prying eyes, access to information and the ability to contribute to digital information products and to share information within communities are also essential to all citizens of the information society [79]. Many legal systems regard the right to privacy as a fundamental right, and this principle may affect how IP is distributed. Consumers are concerned about their privacy, and therefore experience a need to be able to have control over their own personal information, including the manner of its acquisition and the use to which it is put. Unfortunately present day system design tends to address privacy as an afterthought rather than as a prime concern and central factor, which makes the implementation of the protection of privacy rather difficult. In order to work efficiently, mechanisms for the protection of privacy must be included in the system from the word go, and must be

[1] The issues of piracy have been analysed by the Committee for Economic Development [1] through the lens of economic growth and productivity, i.e. by seeking answers to the question, "what is the effect of digital piracy on growth, productivity, and the future standard of living, and what would be the effects of alternative policies to curb it?"

taken into account at all stages, system requirement analysis, design, development, and deployment.

Consequently, there is a need for a flexible and effective system that prevents unauthorized access to and use of digital assets and manages, monitors, controls, secures and tracks them without violation of privacy and private/fair use. DRM solutions appear to be among the best technologies one can use to meet these challenges. The general technical challenges will necessary involve the development of (a) techniques, processes, procedures and algorithms for the management of rights in digital environments which will allow the flexible specification of rights, rights policies, conditions and terms of usage, and online negotiation and contracting of rights and rights policies, and (b) dependable security infrastructure for secure preparation, distribution, prevention of misuse and consumption of protected digital works, and privacy protection, usage tracking, account and key management. Moreover, DRM is a multifaceted concept and a complex topic. The topic of DRM exists at the meeting point of technology, business models, policies and law, and societal issues. It follows from this that any true understanding of DRM must be holistic and broad, not only to derive the full benefit of the current uptake of DRM, but also to gain insight into the future of DRM-enabled networked digital media.

This paper gives a structured overview of the frontiers of DRM knowledge and technology in the form of a brief survey. On the basis of this review of the present state of the art and activities in the field of DRM, we chart trends and predict developments, and thus analyze the criteria for success.

## 2. Arguments in the DRM Debate

This section gives an overview of the concepts and motivating arguments of both the boosters and the sceptics of DRM.

**The motivating concepts of DRM boosters**

The pro-DRM lobby is motivated by the following arguments: The protection of intellectual property in the form of digital assets is important in order to provide protection, or at least a deterrent, against mass piracy. The Internet now constitutes a rapidly expanding arena for commercial activity, especially for transactions involving intellectual property. The presence of this trading arena, in combination with improved compression technologies, provides a unique opportunity for the marketing and distribution of entertainment content. In the presence of these two factors, DRM will act as an enabler for mutually beneficial business transactions. Due to the ubiquity of digital content and the fact that DRM makes all stakeholders in a transaction winners, DRM concerns everyone. DRM is necessary because of the lightning speed and virtually zero cost of digital content reproduction and the relative inadequacy of prosecutorial channels for addressing infringement, motivating the need for technical protection measures. Finally, DRM is important in establishing and increasing security, trust and privacy in transactions involving digital assets, and in ensuring the persistent protection of content throughout the whole value chain, from preparation through delivery to usage.

**The Motivating concepts of DRM Sceptics**

The anti-DRM lobby is motivated by the following arguments: Free Software Foundation says defending freedom means thwarting DRM [77]. DRM may have the effect of preventing users from accessing encrypted material in the public domain. DRM may prohibit the fair/private use of protected materials, with the result that news agencies may no longer be able to acquire portions of copyrighted works for lawful purposes, and backups may not be allowed. DRM systems may require customers to disclose personal information in the form of, for example, a credit card number, and each access can be logged by the rights holder, both of which affect users' privacy. DRM can cause inconvenience to users when its technology behaves in counter-intuitive ways, like for example, when DRM-enabled software configured for laptops refuses to work on a desktop machine in the same home. Lastly, there are those who contend that copy protection and DRM are futile exercises on the basis that all digital copy protection schemes can be broken, and once they are, the breaks will subsequently be distributed. More information on consumer advocates' concerns about DRM could be found in [36], [81], [82], [61].

The above can be alternatively stated and conceptualized as follows [76].

**Intellectual Property (IP)**: One of the main topics of discussion in the field of IP is the raison d'être of IP rights, the question of why they should exist at all. This can be broken down into a number of subtopics, the establishment of their scope, the justification for using them, on what basis title to information gives the owner of said information reasonable grounds or the right to curtail the freedom of others when it comes to the use of this information. These topics are of a philosophical and general nature. Others revolve around more practical and specific matters, for example the manner of the adequate expression of IP rights in legislation and rules, and within the context of the institutions of our society.

**Privacy and data protection**: Then, there is the matter of ensuring that privacy and personal data are protected. The debate in this area revolves around what justification there is for restricting access to personal information. It can be reasonably stated on the basis of the norms of our culture and society that there are number of moral and ethical reasons for protecting the privacy of the individual, and thus for limiting access to personal

information and the ways it should be acquired, processed and disseminated. We can then say that one's right to privacy and to have one's personal information protected is an expression of moral constraints on what others may or should do with one's personal information.

**Equal access:** Another important topic is that of equal access to information. The point here is that there is or can be a class division, known as the digital divide, between the information haves, and the information have-nots. The crux of the matter is that information exists that is so crucial to individuals that there exists an obligation for someone – individuals or agencies – to ensure that individuals have equality of opportunity in the area of access to information too, or to the fair distribution of access to crucial information.

**Responsibility and information:** Those who wield power must feel or be constrained to exercise that power in accordance with some set of moral and ethical principles. Current technology enables us to acquire knowledge, and to process and disseminate information and data. The ability and power to act, and to control things and achieve the previously impossible, is accompanied by a responsibility, a responsibility refrain from using this power irresponsibly.

## 3. DRM Security and Trust

In this chapter we examine the security and trust in DRM after which we describe briefly the risk management and tamper resistant approaches.

**Trust Model:** Trust is one of the most important elements in human relationships, and is a critical basis for consumer-to-provider relationships. To wit providers need to establish trust and confidence in their products and services, and consumers need to protect their privacy and information, and assess the trustworthiness of their providers. Thus, a DRM-enabled application depends in part on the ability of DRM systems to engender trust among consumers. A DRM trust infrastructure is thus the technology and processes which make DRM system components trustworthy. The trust model in DRM differs from the simple cryptographic model in which two trusted parties own a shared secret key and exchange encrypted information while an attacker located between them attempts to intercept and recover this information. In a DRM trust model one communication party (the end user) cannot be trusted with a shared secret key or even unencrypted data, i.e. distinguishing between honest and dishonest users is no easy task [8].

**Security:** A DRM system thus requires persistent content protection so that content cannot be used and redistributed illegally. The content must be protected during delivery and restrictions of the content usage rights have to be maintained after the content is delivered to the end user. As a result the required security level in DRM systems goes beyond simply granting digital licenses to authorized users. This means that the protection has to stay with the content and that end-to-end security has to be maintained, i.e. every link in the delivery chain has to be secured and content must only be accessible to authorized/ authenticated person or compliant devices, i.e. rights are correctly executed and enforced. Current approaches to the problem of protecting digital content fall into four broad categories, the encryption/scrambling of content, watermark, risk management, and other methods [36].

**Encryption/scrambling**: In DRM systems the general rule is that a symmetric key algorithm is used to encrypt digital content, and an asymmetric key algorithm is used to encrypt the content encryption key. The non-repudiation issuing of rights is generally achieved by using digital signatures, the issuer signing licenses digitally and the user application verifying the correctness of the rights and keeping the signature as a proof of purchase. The integrity of content is generally checked by using one-way hash functions contained in digital signatures. The content and the identities of the involved parties are generally authenticated and verified by using digital certificates.

**Watermarking/fingerprinting**: In DRM systems, watermarks can be used a) for binding information to digital content, such as content owners, the buyer of the content and usage rights associated with the content (such as payment information), b) forensically to trace digital pirates, and c) for data annotation and access control. The watermarks that are used for data annotation are named annotation watermarks by the authors in [37]. For example, the usage rule defining the allowable number of secondary copies and playbacks can be embedded as annotation watermarks in every copy of the content. When the digital content is accessed, the user's player application counts annotation watermarks, checks the usage restrictions and updates watermarks as required. The major advantage of using annotation watermarks is that it binds usage rights with digital content no matter where the content travels [37]. However, the robustness of many watermarking systems is not very satisfactory. The majority of copyrights marking schemes in the literature are vulnerable to attacks [38]. Therefore, merely applying watermarking technologies to the DRM solution may not be secure enough to meet the commercial requirements.

**Risk Management:** A number of researchers make an optimistic claim that DRM models can be advantageously deployed by using risk management and being able to adapt to security compromises. The underlying philosophy is to identify specific threats to a system, to determine the costs of possible attacks as well as the costs of protecting against them, to implement protection mechanisms only when the benefits of such

mechanisms outweigh the costs of their implementation, and to respond gracefully to break-ins rather than attempting to establish absolute yet brittle security [73]. Cryptography Research in [66] gives an account of how the credit card industry successfully curbed credit card fraud by adopting a risk management model, and points out how a number of the same ideas can be applied to the protection of copyrighted material [72]. Hence, risk management is a framework for identifying, assessing and controlling risks relevant to digital content.

**Tamper Resistance**: Tamper resistant systems protect trusted software running on a malicious host. To prevent malicious users from tampering with rights entitlement functions of the DRM-enabled applications, it is essential to employ tamper resistant technology to make hacking extremely difficult and ensure that the DRM client can be trusted to perform as designed. There are generally both software-based and hardware-based tamper resistant approaches. Software-based technologies rely only on software mechanisms to defend against tampering. Some common software based approaches include (i) code obfuscation [39], [68] in which the software is transformed into a functionally equivalent form which is difficult to understand and analyze, (ii) code encryption that prevents hackers from seeing and accessing the software, and (iii) self-modifying code that generates other code at run time. Hardware based technologies rely on secured hardware devices for protection. The hardware-based approach to DRM consists of the provision of a hardware-trusted space, an execution space which is protected from external software attacks, in which protected content is hosted, in which only approved applications can execute. This trusted space is the only place where DRM services, such as content decryption, authentication and rights rendering, take place.

## 4. A Structured State of the Art in DRM

DRM-enabled information distribution consists of a combination of applications, business models, distribution models, technology and systems, and legal infrastructures. The applications use business models, the business models use the distribution models, the distribution models use the technology and systems, and all four are underpinned by the legal infrastructures. The stakeholders in all these areas also have a relationship to each other. Figure 4-1 shows the relationship between the various components of DRM-enabled distribution.

There are many techniques that can be used by a DRM system to curtail infringements of IPR. Each one has its strengths and weaknesses, which must be weighed against each other along with the cost of acquiring, integrating and maintaining them. Generally the choice of which particular techniques to adopt in a given situation or context is governed by an assessment of the level of risk associated with the distribution and use of the content in question. For a more thorough and exhaustive account of the state of the art in DRM see [9], [10], [8], [5], [70], and of the background, concepts and definitions of DRM see [55], [80], [2], [3]. This chapter presents a structured and categorized (see Figure 4-1) overview, assessment and analysis of many of the major works in the area, a rundown of the various companies that are developing DRM systems, and a couple of examples of the activities of standard bodies in the field.

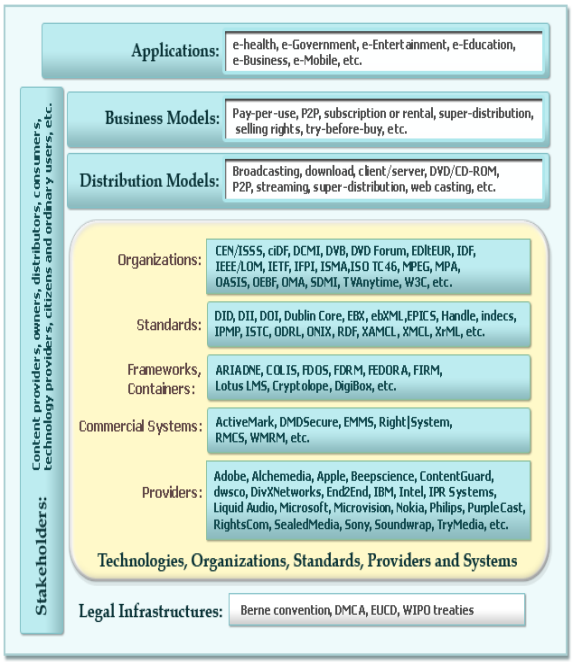


*Figure 4-1 The various components of DRM-enabled distribution*

### A Wider Range of DRM Applications

A flexible, balanced and effective DRM solution is one that is capable of creating, retrieving, trading and distributing content for a wider range of applications by ensuring that all stakeholders, including producers, owners, distributors/retailers, users, and technology providers who make possible the delivery, and hardware and software companies who make possible the consumption of IP content, are all winners. We describe briefly the wider range of DRM-enabled applications as follows [78]:

**eHealthcare:** The healthcare and welfare sector is one of the most crucial application domains. By virtue of the sensitivity of this domain, as exemplified by the Hippocratic oath, the professional discretion of the physician and specific professional legislation, health data is generally handled with special care. The misuse of a patient's medical data can be highly injurious, and may easily discredit a citizen in both social and professional life. The misinterpretation of these same data can lead to

incorrect medical treatment which may be detrimental to the health of the patient, or even lethal. Therefore it is more important than ever to protect all types of digital medical data - image, audio, video, biomedical signals of, e.g., body functions (ECG or EEG), and mixed. Thus, DRM can be a great boost to eHealth since it protects both the privacy and the integrity of medical data while at the same time making them easily and quickly accessible to health service personnel on a differential basis.

**eGovernment:** The eGovernment community would greatly benefit from DRM-enabled application, which will engender trust in e-communications, thereby building the trust of consumers and businesses in e-government services by preserving citizens' privacy. DRM can provide digital policy management and risk management that can facilitate the automation of eGovernment activities. It can enable government to make available electronically a large amount of information in a secure manner, which will open new business opportunities and improve services to citizens. It can also enhance the enforcement of IPR, which can serve to improve credibility and can, thus serve to encourage the production of digital products and services.

**eEducation:** DRM can boost eEducation by facilitating the easy and secure management of the creation, retrieval, trading and distribution of online learning objects and by supporting secure collaborative development. Promoting the exchange and reuse of quality learning objects, and respecting and rewarding the intellectual property of the various contributors, are the two key issues which have to be dealt with before online learning can become cost effective [3].

**eMobile:** OMA's (openmobilealliance.org) focus on the development of mobile DRM service enabler specifications, which support the creation of market-driven, interoperable, end-to-end mobile services, is evidence of the importance of mobile DRM applications. OMA's DRM enabler allows the expression of three types of usage rights: the ability to preview content, the ability to prevent content from being illegally forwarded to other consumers, and the ability to super-distribute content.

**eEntertainment:** Within the principle and technical DRM protection zone, digital information such as music can be offered to consumers via a virtually limitless range of business models such as sale of downloads, subscriptions, pay-per-listen, super-distribution, file-sharing, etc.

## Business and Distribution Models

In the most basic sense, a business model is the method of doing business by which a company can sustain itself, i.e. generate revenue and profits. The business model spells out how a company makes money by specifying where it is positioned in the value chain. Business models that are currently commercially relevant and that a DRM system should therefore support include the download and purchase of individual content, subscription models (e.g. to a whole music catalogue), pay-per-play, pay-per-listen, usage metering, peer-to-peer (p2p), super-distribution, selling rights, and a limited number of plays for preview purposes [19], [2]. Another example of a business model for the content value chain is the IMPRIMATUR business model described in [29].

The major content distribution channels or systems are Internet distribution (delivery system and edge servers, unicast streaming and download), distribution over physical media (such as DVD, CD, etc.), and broadcast (terrestrial, cable, satellite, etc.). Distribution model scenarios can further be categorized as file sharing, personalized distribution service, distribution using subscriptions and memberships, and super-distribution. In [30] distribution models are categorized according to several case studies involving new distribution mechanisms like file sharing, peer-to-peer, streaming and super-distribution in the electronic market for online music that leads to challenges on the supply and demand side. For 2006 year in review of DRM-enabled content services see [85].

## Technologies, Organisations, Standards, Providers and Systems

### Identification

The identification of rights is an essential part of DRM. In this context entities and the metadata records associated with them containing all rights pertaining to these identities, must be clearly identifiable. Digital Object Identifiers (DOI, doi.org), Handle System (handle.net), Uniform Resource Identification (URI), the emerging ISO International Standard Textual Work Code (ISTC) [11] and other open standards are among those now in general use for the identification of rights. A basic requirement of identifiers of content and rights is that they must be unique, persistent/stable, and linked to a minimum set of metadata. Some examples of frameworks for identification are:

**DOI** is a system for identification and exchange of intellectual property in a digital environment. It provides a framework for managing intellectual content, for linking customers with content suppliers, for facilitating electronic commerce, and allowing automated copyright management for all types of media. DOIs are names assigned to digital objects such as electronic journal articles, images, learning objects, e-books, and any kind of content. Information about a digital object may change over time, including where to find it, but its DOI will not change.

**Handle System** provides a general-purpose global name service allowing secure name resolution over the Internet and is designed to enable a broad set of

communities to use the technology to identify digital content independently of location. It is a comprehensive system for assigning, managing, and resolving persistent identifiers, known as "handles", for digital objects and other resources on the Internet. Handles can be used as URNs (Uniform Resource Names). The information associated with the Handle can be changed as needed to reflect the current state of the identified object without changing the Handle, allowing the name of the item to persist over changes of location and of other state information.

The DOI System utilises the Handle System as one component in building an added value application for the persistent, semantically interoperable identification of intellectual property entities. The Handle system is a necessary component of DOI, but not sufficient by itself for the DOI system to function as a complete framework for managing IP content and facilitating e-commerce. In addition to the Handle System, DOI needs a numbering syntax, a data model system, and policies and procedures for its function. DOIs consist of more things than just Handles. A thorough discussion of the relationship between DOI and Handle with reference to persistence, consistency, ease of use, expressing relationships, technical infrastructure, semantic interoperability, development activities, costs and not least, governance, see [12].

Other examples of frameworks for identification and description include MPEG-21 DID and DII [13], ISAN [14], UMID [15], ISWC [16], GRid [74], and GUID [75].

**Rights Expression Languages**

The introduction of rights expression languages (RELs), the two most important of which are XrML (xrml.org) and ODRL (odrl.net), marks the advent of the standardization of DRM solutions [17]. The purpose of RELs is to provide flexible, interoperable mechanisms [13] which a) support the transparent and augmented publication, distribution and consumption of digital content on such a way that the content is protected and the rights of all stakeholders are honoured, and b) support the specification of access and usage control and the exchange of sensitive or private digital information, and ensure that this personal data is processed in such a way that the rights of all individual parties are respected. Standard RELs must be able to support guaranteed end-to-end interoperability, consistency and reliability between different systems and services. Below we analyse two of the most frequently mentioned RELs.

**XrML** is one key to interoperability for DRM systems and services. It provides a universal method for securely specifying and managing rights and conditions associated with all kinds of digital content and services at varying levels of granularity. The components of XrML, Grant (a relationship), Rights (permissions), Principal (the entity itself), Resource (the entity's asset or content) and Conditions (Context) abstract elements as they relate to the rights entity in the specification's data dictionary in order to express agreements between data controllers and data processors for specific rights over data. XrML expressions are licenses that grant rights to a principal associated with a resource and subject to conditions. It is extensible and compliant with XML, and supports XML signature and XML encryption for the authentication and protection of the rights expressions.

**ODRL** provides the syntax for a DRM expression language and data dictionary pertaining to all forms of digital content. It supports a vocabulary for the expression of terms and conditions over digital content including permissions, constraints, obligations, requirements, and offers and agreements with rights holders. It is stated that it is supported by different industry sectors (including e-books, music, audio, software) as a core interoperability language intended to provide flexible mechanisms to support the transparent and innovative use of digital content across many sectors, and enforce the rights, conditions and fees specified for digital content.

While ODRL has been officially endorsed by the OMA as the standard rights expression language for all mobile content, XrML has been adopted by the MPEG-21 (as MPEG REL) standard for multimedia devices and networks. XrML's primitives map less directly on to the kind of license terms that are found in media in the real world than those of ODRL. For example, ODRL has explicit features for specifying things like resolutions, encoding rates, and file formats for content. ODRL seems better suited to actual transactions in the world of media and publishing while XrML aspires to being more broadly cross-vertically applicable. For a comparison between ODRL and XrML by DRMWatch see [18].

Other RELs are IPMP and MPEG-21 REL by MPEG [13], XMCL (xmcl.org) by RealNetworks, and XACML (xacml.org) by OASIS.

**Frameworks and Architectures: FDOS and FEDORA**

In the area of frameworks and architectures for digital objects, we present two selected examples: A Framework for Distributed Digital Object Services (FDOS) [20], and Flexible and Extensible Digital Object and Repository Architecture (FEDORA) [21].

**FDOS** is an open architecture infrastructure, which can handle a large, and extensible class of distributed digital information services like new applications for electronic commerce, and digital libraries [20]. FDOS defines those basic entities where digital objects containing information are stored, accessed, disseminated and managed, provides naming conventions by which digital objects can be identified and located, describes a service which locates and disseminates objects by using

object names, and provides elements of a repository access protocol (RAP) that provides services for depositing and accessing digital objects. A digital object is defined in [20] as a content-independent package that includes the content of a work, a unique identifier for the digital object (its handle), and other data about the object, which might include policy expressions dictating use of it.

**FEDORA** is an architecture consisting of digital objects and repositories which stores and disseminates digital library content. The important characteristics of this architecture are that it (1) supports heterogeneous data types; (2) handles new types as they emerge; (3) aggregates different data types, which may come from different sources, into single, complex objects; (4) can specify multiple dissemination of content; and (5) can associate schemes for rights management with these objects. It has been implemented in the context of a research project to develop the next-generation services for digital libraries. FEDORA is also an open architecture framework which modularizes the functionality of a digital library into a set of services with well-defined interfaces which allow these services to be combined with each other and with other value-added services to create usable instantiations of digital libraries.

**Self-Protecting Container Technologies**

Various container technology solutions have been proposed to counteract and curb the illegal copying and distribution of digital objects, but none of them have been taken into general use because of the heavy dependence of their security on the security of the client software [80]. One of the more elaborate of them, IBM's Cryptolope [26], includes the protected content and all necessary administrative information, and makes it possible for end users to produce software emulators by running its end opener component (a.k.a. Cryptolope Player) on the end user's PC. In addition to this it requires an infrastructure of trusted clearinghouses and online connections with these entities. A similar technology is InterTrust's DigiBox [27], which protects content even after the resale of it. Both technologies are platform dependent, lack an integrated payment scheme, and are designed for high-value digital goods and inadequate for low-value transactions and occasional business relations. Although the epithet "Self-protecting container" implies that all of the contained information is protected, these container technologies do not seem to address the matter of protecting the privacy of users in the case of fine-grained rights enforcement.

There are those who contend that self-protecting container technology can support almost any type of network topology with any number participants, and that it controls rights flexibly, which means that it is a true tool for super-distribution. For this technology to be deployed there is however a need for a secure environment in which containers can be processed. Therefore, pervasive deployment of tamper-resistant technologies is necessary [28].

There are also those who contend that self-protecting technologies are in fact so versatile that they can be made to combine, filter, index, rearrange, interpret and transform digital information [83], [84].

**Trusted Computing Platforms**

**Trustworthiness:** Trust is an essential factor in any business-transaction system, and this is true also of DRM systems. Lack of trust in the ability of DRM infrastructure to protect IPR constitutes a serious obstacle to growth in the IPR business. The trusted computing group (TCG) [40] is an industry standards body engaged in the development of specifications for a trusted computing platform which, according to them, is intended to improve trust in many platforms. Examples of hardware-based platforms include TCG's trusted platform module (TPM), a tamper-resistant chip which enhances the security of a platform, Microsoft's security support component (SSC) of the next generation secure computing base (NGSCB) architecture, which is a tamper-resistant cryptographic chip required for secure processing [41], and Intel's LaGrande, a composite of microprocessor, Chipset, I/O subsystems, and other platform components, which is a general-purpose environment for safer computing environment [42]. The three fundamental components of the trusted system proposed by the TCG are:

**Core Root of Trust for Measurement (CRTM)** [69] has the ability to measure at least one integrity metric for a portion of the software environment of the platform. The CRTM records this integrity metric in one of the sixteen-platform configuration registers (PCRs) held in the Trusted Platform Module (TPM). The CRTM also records details of the software being measured to a "trust platform measurement store" managed by the TCG software stack (TSS).

**TPM** is a tamper resistant chip responsible for accepting the integrity measurements from the CRTM and recording them. It calculates a cryptographic digest of all sequences of integrity metrics presented to it on request, and provides security functionality to the platform, such as platform authentication, protected storage, and sealing.

**TSS** consists of software elements deployed on the platform including trusted platform measurement store, TCG validation data, measurement agents, and a trusted platform agent.

Such trusted computing platforms (TCPs) have been developed as a basis for the implementation of DRM. The deployment of them has, however, become a controversial issue and the subject of much discussion [65], [62].

**Interoperoperables: FIRM and INDECS**

In the area of interoperable rights management there are two well-known interoperables: the Stanford FIRM (Framework for Interoperable Rights Management) [24], and INDECS (Interoperability of Data in e-Commerce Systems, indecs.org).

**FIRM** is one of the protocols of the Stanford "Infobus", which is a prototype infrastructure, developed as part of the Stanford Digital Libraries Project, designed to extend the Internet protocols to higher-level protocols for the management of information. It is a network-centric design which manages relationship-based rights, unifies the management of them from a user-centred perspective, and supports end-to-end integration of shared control state in network services and users' client applications. Architecturally it unifies services and protocols in a way that allows the networked management of rights. It does this by defining a network software service layer that is built on top of other network protocols to provide object definitions and services for the management of rights and obligations. It proposes that objects that implement control should be separated from objects that are controlled for the purpose of enhancing the system's flexibility.

**INDECS** is a project in which a framework has been defined for interoperable metadata in content-based e-commerce. Its approach is based on metadata whose function is 1) to identify uniquely every entity in an identified namespace; 2) to identify fine-grainedly an entity whenever it needs to be distinguished; 3) to identify securely the author of an item of metadata; and 4) to ensure that everyone has access to the metadata on which they depend, and to ensure the privacy and confidentiality of their own metadata so that it is protected from those who are not dependent on it. <indecs>2rdd [25] is a consortium based initiative, a continuation of the work of the original <indecs> project to develop a multimedia rights data dictionary (RDD), which supports the practical interoperability of different metadata models, descriptive, legal and financial semantics, and rights expression languages. This RDD is an essential infrastructural building block for DRM systems, which will enhance the value of proprietary technology and make the management and protection of rights interoperable.

**Educational Technology Models**

Some of the several models of educational application that manage and enforce digital rights [23] are:

- ARIADNE (Alliance of Remote Instructional Authoring and Distribution Networks for Europe) consists of a network of repositories with a set of related tools, and supports the sharing and reuse of learning objects, and a number of mechanisms for the preservation of digital rights.
- The COLIS (Collaborative Online Learning and Information Systems) project builds a broad, interoperable, standards-based DRM-enabled e-learning environment for the future.
- IBM Lotus LMS (IBM Lotus Learning Management System) manages both formal and informal learning, and it provides a standards-based authoring tool that can be used to create learning objects.

**e-Books: EBX and OeBF**

In the area of e-books the two most cited examples are EBX (Electronic Book eXchange, ebxwg.org), and OeBF (Open eBook Forum, openebook.org).

The task of the **EBX** Working Group is to develop open, freely available standards that are commercially viable for the secure distribution of e-books among rights holders, intermediaries, and users. EBX addresses how e-books should best be bought, sold, lent, given free, printed, subscribed to, and licensed. In their own words, EBX strives to achieve the highest possible levels of authentication, accountability, auditing, internationalisation, robust security and usability in order to satisfy all participants in the value chain quite irrespective of the actual content format. And their stated aim is to stimulate the growth of e-book markets by co-operating with other standardisation bodies.

**OeBF** is an international trade and standards organization for the electronic publishing industries, whose members are publishers, hardware and software companies, retailers, libraries, accessibility advocates, authors and related organisations. Their stated common goals are the establishment of specifications and standards and the advancement of the competitiveness and exposure of the electronic publishing industries. They also state that their work will foster the development of applications and products beneficial to creators of content, makers of reading systems and consumers.

**DRM Books**

At present there are two main books on DRM available, both of which receive a brief mention here.

- Digital Rights Management: Business and Technology, John Wiley & Sons, 2002, by Bill Rosenblatt et al. [2] gives a complete description of DRM from the points of view of business and technology. This book gives an outline of the state of DRM today for media executives and IT decision-makers, and covers business models (e.g. subscriptions), core technologies (e.g. watermarking, encryption, authentication, etc.), standards (e.g. XrML), vendors, etc.
- Digital Rights Management: Technological, Economic, Legal and Political Aspects, LNCS 2770, Springer, 2003, by E. Becker et al. [56]. This book, comprising 35 articles whose authors come from

academia, the IT industry, and from copyright industries, gives an overview of the overall DRM landscape, and specifically its technological, economic, legal, and political aspects. The focus of the book is on the "distribution of entertainment content (i.e. as music, pictures, movies, text, etc)".

**Existing Commercial Systems**

In order to gain a correct understanding of the existing DRM systems it is necessary to have a good overview of the current deployment of DRM systems. This section presents a brief review of DRM systems currently on the market along with their pros and cons. The ones which are selected and most frequently mentioned are the IBM Electronic Media Rights Management system (EMMS) [31] and Microsoft Windows Media Rights Manager (WMRM) [32].

**EMMS**

IBM's EMMS was developed by IBM for the preparation and secure distribution of all forms of digital content, and supports the goal of Secure Digital Music Initiative (SDMI). It comprises a suite of five software products: 1) Packager/Usage Tracking which is used by the content creator to specify usage and distribution rules for the content, and packages the content using a cryptographic coprocessor; 2) License Server/Key Distribution Server (Electronic Web Commerce Enabler – EWCE) which is responsible for the distribution of licenses and keys; 3) Content Distribution Systems which distributes the content purchased by consumers by hiding the details of the communication with a specific content hosting server from the customer; 4) Client SDK which enables users to develop industry-specific client applications that download, use, and manage media and business data in a tamper-resistant environment in accordance with usage conditions specified by content owners; and 5) EMMS Multi Device Server which facilitates the transfer of digital content securely to specific devices such as mobile handsets, CD production system, or kiosks. The business models supported by EMMS are pay-per-use, pay-per-time, subscription, controlled printing, and protected transfer to portable devices and media. EMMS is mainly used in Japan for the online distribution of music, where it has been used for the famous mobile distribution service, DoCoMo's music service [8].

The advantages of EMMS are that it is distributed, has a flexible architecture, has a flexible SDK Player, has flexible rights specification using XML, has flexible methods of setting up business relationships using visual tools, integrates pricing information, and can be deployed in a wireless environment.

The disadvantages are that it supports only Windows platform with the exception of EWCE component that can run on multiple platforms, it requires a cryptographic coprocessor, and most components require one particular edition of the DB2 database.

**WMRM**

Microsoft's WMRM is an end-to-end DRM system for the secure distribution of multimedia files based on the Windows Media Player and Server, and supports the goal of SDMI. Its main components are 1) Windows Media Packager which is used by content owners to specify rights of usage and distribution, and which packages the content and transfers it to the License Server; 2) License Server/Key Distribution Server, which is responsible for the distribution of licenses and keys; 3) Content Distribution System, which is responsible for the distribution of content transparently with several different distribution scenarios (e.g. pre-delivery, post-delivery, silent delivery, and non-silent delivery); and 4) Client SDK, which is used to develop customized DRM solutions by associating rights with devices rather than users, and requires ActiveX. The business models supported by WMRM are subscription, on-demand streaming, download, counted operations, and secure transfer of protected digital media files to SDMI portable devices or media. WMRM is used by a large online music service company [33], PressPlay, to offer in digital form music from Sony, Universal, EMI Music and many independent labels. PressPlay differs from other music service providers in that it allows consumers to burn music on to CDs. BuyMusic, MusicMatch, MusicNow, Napster, and numerous others use WMRM's Windows Media Audio (WMA) format [22].

The main advantages of WMRM are that it uses Windows, whose media format is widely used on the Internet, and whose Media Player already supports DRM, it has a flexible SDK for the design and implementation of different applications, it has a flexible mechanism for the specification of rights in which the specification and encryption are independent, separate processes, and it allows the transfer of licenses to mobile devices.

Its main disadvantages are that it only supports Microsoft's proprietary WMA and Windows Media Video (WMV) formats without additional conversion, its Client SDK Player is integrated with Microsoft's Media Format Player for different devices, but has no plug-ins for other players, and licenses are associated with devices rather than users.

**Other DRM Systems**

In addition to the above systems, there are many others developed by, for example, Adobe (adobe.com), AegisDRM (aegisdrm.com), Alchemedia (alchemedia.com), Apple (apple.com), Beep Science (beepscience.com), ContentGuard (contentguard.com), DMDSecure (dmdsecure.com), Digital World Services (dwsco.com), DivXNetworks, End2End

(end2endmobile.com), Intel (intel.com), IPR Systems (iprsystems.com), InterTrust (intertrust.com), Microvision (microvision.com), Philips (philips.com), RealNetworks (realnetworks.com) RightsCom (rightscom.com), SealedMedia (sealmedia.com), Sony (sony.com), Soundwrap (soundwrap.com), TryMedia (Trymedia.com) and many more.

**Standardisation Initiatives**

The creation of interoperable DRM solutions which are accepted by intended users on the basis of their wide spread use is totally dependent on the standardization of DRM solutions. For example the use of a standard DRM architecture, a standard rights language, etc. will enable different DRM vendors to work together, and end-users to avoid being locked into a particular DRM system. In this section a brief overview is given of some of those initiatives that are proposing or actually developing standards for DRM.

**CEN/ISSS** (European Committee for Standardization Information Society, September 30, 2003) [9] have produced a report on DRM which examines thoroughly the state of the art in standardization in the field of DRM, identifies the current status of the different facets of DRM and its usage. It also examines possible ways of ensuring that DRM is effectively implemented in the marketplace.

**DMP** (Digital Media Project) [6] "is a not-for-profit organisation whose main aim is to ensure that digital media are successfully developed, deployed and used on an on-going basis, and that they respect the right of creators and rights holders to receive correct remuneration for their distributed works, satisfy the desire of end-users to get what they need out of using them, and protect the interests of various value chain players who wish to provide products and services according to the principles laid down in the Digital Media Manifesto.

**DVB** (Digital Video Broadcasting, dvb.org) project comprises broadcasters, manufacturers, network operators, regulatory bodies, and others, and exists for the purpose of developing global standards for delivering digital television and associated data services. The Content Protection and Copy Management (CPCM) sub-group of DVB works on end-to-end protection from the point of initial distribution to the end user.

**MPEG** (Moving Picture Experts Group) [13] is a working group of ISO/IEC for defining and developing open standards used for delivering and using multimedia. The goal of MPEG-21 is to define the technology needed to support the exchange, access, consumption, trade and manipulation of digital items in an efficient, transparent and interoperable way. It is standardizing RELs, digital item declaration (DID), digital item identification (DII), intellectual property management and protection (IPMP), digital item adaptation (DIA) and rights data dictionary, which are directly applicable to DRM solutions. The REL is based on XrML and the data dictionary is based on <indecs>.

**OASIS** (The Organization for the Advancement of Structured Information Standards, oasis-open.org) is a not-for-profit, international consortium contributing to the development, convergence, and adoption of e-business standards. It produces Web services, XML conformance standards along with standards for security, e-business, e-publishing, interoperability, and standardization efforts in the public sector and for application-specific markets. OASIS and the United Nations jointly sponsor a global framework for e-business data exchange, ebXML.

**OMA** (Open Mobile Alliance) is the leading industry forum for developing market driven, interoperable mobile service DRM enabler specifications. Its main goals are among others to deliver high quality open technical specifications based upon market requirements, and to be the catalyst for the consolidation of standards activities within the mobile industry. Its focus is on the development of mobile service enabler specifications, which support the creation of market driven, interoperable, end-to-end mobile services. Its DRM enabler allows the expression of three types of usage rights: the ability to preview content, the ability to prevent content from being illegally forwarded to other consumers, and to enable super-distribution of content.

**SDMI** (Secure Digital Music Initiative, sdmi.org) is a forum that has brought together more than 200 companies and organizations representing information technology, consumer electronics, security technology, the world-wide recording industry, and Internet service providers, and whose goal is to "protect the playing, storing, and distributing of digital music" using watermark-based standard/framework.

A list of several standards activities relating to DRM can be found in [34], [5], [7], and [35]. Also a 2006 year in review of DRM standards can be found in [87].

## Legal Infrastructures

As previously stated DRM-enabled distribution consists of a combination of business models, distribution models, technology and systems, and legal infrastructures. This section describes such legal infrastructures that aim to balance between the appropriate revenue of rights' owners and the interest of individual users.

**The Berne Convention** [43] is a convention for the protection of literary and artistic works, adopted in Berne in 1886, and first established the recognition of copyrights between sovereign nations. It provides each contracting state to recognize copyrighted works authored by nationals of other contracting states. Copyright under the Berne Convention is automatic, i.e. neither registration is required nor the inclusion of a copyright notice. The Berne Convention is provided for a minimum term of copyright protection of the life of the author plus fifty

years, but parties were free to provide longer terms of copyright protection. Prior to the adoption of the Berne Convention, nations would often refuse to recognize the works of foreign nationals as copyrighted works (http://encyclopedia.fablis.com/).

**WIPO Treaties** [44] are international treaties, signed in Geneva, Switzerland, in 1996, designed to bring uniformity to international copyright law. The purpose of WIPO is to promote the protection of intellectual property throughout the world through co-operation between states and, where appropriate, in collaboration with any other international organization, and to ensure administrative co-operation between the contracting parties. The WIPO Copyright Treaty provides additional protections for copyright deemed necessary in the modern information era. It ensures that computer programs are protected as literary works and that the arrangement and selection of material in databases is protected. It provides authors of works with control over their rental and distribution, which they may not have under the Berne Convention alone. It also prohibits circumvention of technological measures for the protection of works and unauthorised modification of rights management information contained in works.

**DMCA** [45] is an American law implementing the WIPO Copyright Treaty and Performances and Phonograms Treaty. DMCA backs DRM in that any attempt for the creation and distribution of DRM circumvention tools even for legal reasons may violate federal law under DMCA. Many people claim that DMCA stifles innovation and academic freedom and is a threat to open source software development [47].

**EUCD** [46] is a directive for implementing the WIPO Treaties in the EU member states into national law. If the directive goes through unmodified, it would be a criminal offence to break or attempt to break the copy protection or DRM systems on digital content such as music, software, or eBooks. The main concern raised by the EUCD is that it could prevent teachers copying materials for their students and prohibit academic research on security issues of an operating system or a protection mechanism. Critics argue that the EUCD is even more restrictive than US DMCA [48].

Other legal infrastructures include the US draft bill for law "Security Systems Standards and Certification Act (SSSCA)", and Australia's Copyright Amendment (Digital Agenda) Act (DACA). For 2006 year in review of DRM-related legal actions see [86].

## Protecting the Interest of all Stakeholders

It has been stated that ensuring that consumers are able to gain access to what they are after is good business practice rather than charity. All players, network owners, ISPs, hardware manufacturers, content creators and application developers, benefit from the empowerment of consumers to get and do what they want [49]. Any good and successful DRM system must adhere to the principle that all stakeholders should be winners, and must ensure that they are. Within the context of DRM this means:

- Content creators/owners such as artists and authors win by getting fairly paid for their efforts
- Content distributors such as publishers and retailers win by getting paid to distribute content.
- Technology Providers such as Telecos, ISPs, and DRM providers win by getting paid for enabling distribution of content
- Hardware manufactures win by getting paid for producing end-devices such as Computers, PDA, CD-Player, Mobile phones, etc.
- Users/Consumers such as businesses, schools, and libraries win by getting good and authentic service at a reasonable price.
- Education and learning sector is a double winner for being the major creator and consumer of IPR.

Godwin [36] has a similar attitude. In his essay he gives an outline of what a humane, balanced form of DRM might look like, and lays down the following set of criteria expressed here in his own words that such a form of DRM would have to meet:

- **For Copyright Owners:** It must limit (or, ideally, prevent) large-scale unauthorized redistribution of copyrighted works over the Internet or any similar medium, and must allow a range of business models for distributing content, within the constraints of copyright law.
- **For Technology Makers:** It must maintain technology companies' ability to create a wide range of innovative non-infringing products, and to design, build, and maintain those products efficiently. It must maintain the ability to choose between open-source and closed-source development models. It must enable technology makers to come up with robust, interoperable, relatively simple technologies that are fault-tolerant and easy to maintain.
- **For Citizens and Ordinary Users**: It must maintain access to a wide variety of creative works, both past and present, including both public-domain works and works still protected by copyright. It must maintain access to advancing consumer technology for uses not related to copyright. It must continue to allow for maintaining fair use (including time-shifting, space-shifting, archiving, format translation, excerpting, and so on) and also must be flexible enough to allow for new, innovative fair uses (e.g., uses of home net-working and other kinds of fair use we haven't yet imagined or discovered).

## 5. Discussions and Trend Analysis: Factors Affecting the Uptake of DRM

DRM is a multifaceted concept and a complex topic. The topic of DRM exists at the meeting point of technology, business models, policies and law, and societal issues [4], [80]. It follows from this that any true understanding of DRM must be holistic and broad, not only to derive the full benefit of the current uptake of DRM, but also to gain insight into the future of DRM-enabled networked digital media.

There has frequently been a lack of awareness of this multidisciplinary nature of DRM, and specialists have approached DRM from the perspective of their own speciality. For example, technologists have concentrated on purely technological issues, while businessmen have concentrated on business models, but few have considered how the technology and the business models might affect each other. In other words, people have habitually approached the different aspects of DRM in isolation rather than approaching DRM as a dynamic whole in which all the constituent parts interact and affect each other, a gestalt which is greater than the mere sum of its parts.

**Technical feasibility**: It is claimed by a number of technical researchers that both copy protection and DRM are futile exercises [59], [60], [61]. One expert in the field has actually stated that DRM approaches will always be futile as "all digital copy protection schemes can be broken and, once they are, the breaks will be distributed" [59]. It is certainly true that all digital copy protection schemes can be broken. This is, however, more of an argument for the futility of all security systems than for the futility of DRM specifically, and as we observe security has not been dropped in our world. A number of other researchers, on the other hand, make the more optimistic claim that DRM models can be advantageously deployed by using risk management and being able to adapt to security compromises [66], and we share their optimism. We also believe that a DRM system which operates on the principle of defence in depth, will provide an adequate level of security.

We have described the architectures, frameworks and schemes of DRM, and how DRM has attracted much attention from and become a major preoccupation and area of research for the research community, standards bodies, industry and legislators. On the basis of our review of the present state of the art and activities in the field of DRM we can chart trends and predict developments, and thus analyse the criteria for success. While well-designed system architectures, frameworks and security technologies for DRM would seem to be a Godsend for content providers who would like to develop their businesses and digital services without having to worry about losing control over their valuable digital assets, the actual successful deployment of such businesses and services depends on more than just the quality of the technology [8]. Another and essential factor is the customer's willingness to abide by the rules and to buy it. Among the main concerns expressed are, whether their privacy will be protected, whether their right to fair/private use will be respected, and whether they will be able to use purchased content without inconvenience and obstacles to usage.

**Privacy:** Many people hate DRM because they feel it invades the privacy of users. Others, supporters of DRM, regard the protection of users' privacy as irrelevant. We argue and believe, however, that DRM's use of mechanisms for the tracking of usage makes it mandatory for the DRM system itself to deploy mechanisms for the protection of users' privacy. The DRM system needs to authenticate the identity of users to grant access to protected content. This identity will be linked to the user's personal information [50], [63], [64], [19] like usage pattern for two legitimate reasons, the first being to improve the service rendered to this particular user, the second being able to render the user assistance in cases of emergency. This linking of user identity to usage pattern has two potentially negative aspects. Users can be tracked and monitored, and the system can pass collected specific information about users to marketing agencies, both of which constitute a violation of privacy, and providers can run the very real risk of incurring data privacy liability under the Data Protection Directive of the European Union or similar legislation [51], [1]. Privacy advocates have articulated a number of significant concerns surrounding DRM systems [63]. A good DRM solution must thus strike a balance in this area.

**Fair/Private Use:** One major criticism of DRM is that it cannot incorporate the principles of fair/private use. Fair/private use refers to the use of copyrighted content for research, teaching, criticism, review or news reporting, which is not an infringement of copyright [52]. Thus curtailment of fair-use by built-in technical restrictions gives many users a feeling of reduced ownership over purchased content. For example, customers can become frustrated and feel unfairly served on discovering that they are unable to read a purchased e-Book on a different computer, or on discovering that a purchased CD cannot be converted to MP3 format for use in their portable players. We feel that a future successful DRM system should respect and ensure the right of the consumer to do as he/she wishes with his/her purchased property as long as no piracy or other laws are infringed. To wit unless DRM technologies make room for future fair uses, fair use will have lost much of its ability to protect the public's side of the copyright bargain [67]. However, "offsetting this factor is the power of the market; consumers will vote with their wallets against technology that is too restrictive" [71].

**Ease of Use:** DRM solutions in use at the present time present obstacles to usability, especially platform restrictions on usage and plug-in requirements [53]. A number of them actually use their own proprietary players and readers to protect content. This means that when consumers wish to purchase content from different vendors, they are forced to acquire a fair quantity of different vendor-specific software in order to consume content, a situation which causes justifiable annoyance and irritation. We believe that future DRM systems, in order to gain consumers' acceptance, must be standardized and interoperable across proprietary boundaries.

**Balanced B2B Model:** Finally, there is one situation that has been overlooked and not provided for by existing DRM systems. We still need to develop a balanced business-to-business (B2B) model in which the responsibility for the protection of content is shared between the provider and a consumer community. Such a model is attractive to the consumer, which is a good selling point for the provider, and is advantageous to the provider in that it relieves him of the onus of protecting content directly at all times without depriving him of the ability to exercise direct control over distributed content.

**Other Desirable Properties of a Good DRM**: Desirable properties of a good and successful DRM are openness, flexibility, generality, scalability, interoperability, extensibility/renewability, and portability [66]. **Openness** and **flexibility** are often considered as fundamental values of any IT system including DRM system. However, one might argue that the extent to which a system should be flexible and open finds its natural limitations in the purpose it serves to its owner and communicating peers at any given point in time. In some situations maximum openness and flexibility are desirable. In others, the exact opposite might be true [40]. **Generality:** The use of metadata attributes gives flexibility to the system since they can express all the information necessary for the application of flexible policies of rights, security and privacy, and allows it to be used with different other models, hence **interoperability**. **Scalability** is the property of a system enabling the creation of profiles to support a wide variety of users and users' devices. If a large number of users request access to objects at the same time, queues and bottlenecks are avoided by the simple expedient of launching additional modules. **Extensibility** is the property of a system enabling the creation of specific, autonomous extensions for use in vertical markets, both open and closed.

**Bottom Line:** Finally, the uptake of DRM systems and their acceptance by users will depend upon security, privacy, interoperability, openness, adaptability and user-friendliness as technological factors, upon innovative and attractive business models that are easy to use, fairly priced, and respectful of the rights of consumers, upon societal benefit being balanced so that all stakeholders are winners, and upon all these things being underpinned by an equitable legal framework. DRM can provide a common focus and basis for combined collaborative research by integrating common concepts, methodologies and tools adapted, developed and synthesised from components drawn from jurisprudence, the social sciences, business theory and economics, and science and technology. This is our considered prediction.

## 6. Conclusions

DRM is a complex and multifaceted concept. Many disciplines affect it, and it affects them. Therefore any true understanding of DRM must be holistic and broad. We have described the basic architectures, frameworks and schemes of DRM, and how DRM has attracted much attention from and become a major preoccupation and area of research for the research community, standards bodies, industry and legislators.

If properly designed and used a DRM system can enable corporate, government and other organization to protect digital assets and control their distribution and usage, thereby protecting IPR over digital information and increasing security, trust and privacy throughout the entire value chain. We have examined the security and trust in DRM and argued that a DRM-enabled application depends in part on the ability of DRM systems to engender trust among consumers.

On the basis of our structured review of the present state of the art and activities in the field of DRM we have attempted to chart trends and predict developments, and thus analyze the criteria for success. We have predicted that the uptake of DRM systems and their acceptance by users will depend upon technological factors, innovative and attractive business models and respectful of the rights of consumers, societal benefit being balanced, and all these things being underpinned by an equitable legal framework. We have also pointed out that for the sake of progress in the field of DRM much work must be done in these areas. More generally, it is apparent that there is a need for a prudent investigation and treatment of the complexity of DRM in order to stimulate, nurture and cultivate an in-breadth and in-depth understanding of DRM systems, and the relationship between them and people, organizations and society at large.

It is our considered opinion that DRM can become a key part of future secure platforms for a wider range of applications and services which will enable the IPR business to flourish. For this to be the case a DRM model must balance the interests of the various stakeholders, must ensure neutrality, security, privacy, commercial reliability and the trusted interoperability of services and applications. By contrast, an ill-balanced DRM model will be a showstopper.

## Acknowledgments

The author would like to thank Stamatis Karnouskos, Bill Rosenblatt, Wolfgang Leister and Arne-Kristian Groven for reading the draft of this paper and for their helpful comments that improved the paper greatly.

## References

[1] P. Horn, E. Maxwell, and S. Crawford, Promoting Innovation and Economic Growth: The Special Problem of Digital Intellectual Property, A Report by the Digital Connections Council of the Committee for Economic Development, 2004, www.ced.org
[2] B. Rosenblatt, B. Trippe, and S. Mooney, Digital Rights Management: Business and Technology, M&T Books, New York, 2002
[3] R. Iannella, Digital Rights Management (DRM) Architectures, D-Lib Magazine v.7, No. 6, June 2001
[4] Australian Government, A Guide to Digital Rights Management, www.dcita.gov.au/drm/
[5] G.A. Lyon, A Quick-Reference List of Organizations and Standards for Digital Rights Management, NIST Special Publication 500-241, October 2002
[6] The Digital Media Project: Purpose, Organisation and Work Plan, www.chiariglione.org/project/,
[7] DRM Watch, http://www.drmwatch.com/standards/
[8] Q. Liu, R. Safavi-Naini, and N.P. Sheppard, 'Digital rights management for content distribution', *Proc. Australasian Information Security Workshop*, Adelaide, Australia, 2003
[9] CEN/ISSS DRM Report, September 30, 2003, http://europa.eu.int/comm/enterprise/ict/policy/doc/drm.pdf
[10] EURESCOM: OPERA – Interoperability of Digital Rights Management (DRM) Technologies: Overview of state-of-the-art DRM systems and standardization activities, Project P1207
[11] ISO International Standard Textual Work Code, http://www.nlc-bnc.ca/iso/tc46sc9/istc.htm
[12] The International DOI Foundation, Fact sheets DOI and Handle Version 4.0, http://www.doi.org/factsheets/DOIHandle.html
[13] MPEG (Moving Picture Experts Group) http://www.chiariglione.org/mpeg/, http://www.mpeg.org/MPEG/index.html
[14] ISAN (International Standard Audiovisual Number), http://www.isan.org/
[15] UMID (SMPTE Universal Material Identifier), http://www.ebu.ch/CMSimages/en/tec_text_r108-2001_tcm6-4697.pdf
[16] ISWC (International Standard Works Code), http://www.iswc.org/iswc/en/html/Home.html
[17] K. Kerényi, Short Description of some Standards Currently Used in the Field of DRM Solutions, INDICARE Monitor, Vol. 1, No. 1, 25 June 2004
[18] Open Digital Rights Language (ODRL) 1.1. A comparison between ODRL and XrML. DRM Watch special analysis reports, August 9, 2002
[19] J. Feigenbaum, M. J. Freedman, T. Sander, and A. Shostack, Privacy Engineering for Digital Rights Management Systems, November, 2001
[20] R. Kahn and R. Wilensky, A Framework for Distributed Digital Object Services, Technical Report, Corporation for National Research Initiatives (CNRI), 1995, http://www.cnri.reston.va.us/k-w.html
[21] S. Payette and C. Lagoze, Flexible and Extensible Digital Object and Repository Architecture, *Second European Conference on Research and Advanced Technology for Digital Libraries*, Heraklion, Greece, September 21-23, 1998, Springer, 1998, LNCS; Vol. 1513
[22] R. H. Koenen, J. Lacy, M. MacKay, and S. Mitchell, The Long March to Interoperable Digital Rights Management, In the Proc. of the IEEE, Vol. 92, Issue 6, pp. 883-897, June 2004
[23] N. Friesen, M. Mourad, and R. Robson, Towards a Digital Rights Expression Language Standard for Learning Technology, A Report of the IEEE Learning technology Standards Committee Digital Rights Expression Language Study Group, http://xml.coverpages.org/DREL-DraftREL.pdf
[24] M. Röscheisen, FIRM (A Network-Centric Design for Relationship-Based Rights Management), Computer Science Department Stanford University, 1997
[25] <indecs>2rdd Consortium - Rights Data Dictionary, xml.coverpages.org/indecs2rdd.html
[26] M. A. Kaplan, IBM Cryptolopes, SuperDistribution and Digital Rights Management, V1.3.0, December 1996
[27] O. Sibert, D. Bernstein, and D. Van Wie, The DigiBox: A Self-Protecting Container for Information Commerce, In the Proc. 1st USENIX workshop on Electronic Commerce, 1995
[28] Z.Yan, Mobile Digital Rights Management, Nokia Research Center, In Telecommunications Software and Multimedia TML-C7 ISSN 1455-9749, 2001
[29] IMPRIMATUR Project, www.imprimatur.net/, www.imprimatur.net/IMP_FTP/cmi1.pdf
[30] W. Buhse, Categorizing Distribution Model Scenarios for Online Music. EC-Web 2001: 337-346, LNCS, Vol. 2115/2001
[31] IBM's EMMS (Electronic Media Management System), www-3.ibm.com/software/data/emms/
[32] Microsoft's WMRM (Windows Media Rights Manager), Windows Media Technologies, microsoft.com/windows/windowsmedia/drm.asp
[33] J. Borland, Pressplay to offer unlimited downloads, CNET News.com, July 31, 2002, http://news.com.com/2100-1023-947507.html
[34] Cover Pages, XML and Digital Rights Management (DRM), http://xml.coverpages.org/drm.html
[35] G. Larose, DRM standards and standards-related groups, http://www.info-mech.com/drm_standards.html
[36] M. Godwin, What Every Citizen Should Know About DRM, a.k.a. "Digital Rights Management", Public Knowledge, New America Foundation, Washington, DC,
[37] J. Dittmann, P. Wohlmacher, and R. Ackermann, Conditional and User Specific Access to Services and Resources using Annotation Watermarks, in Proc. of the Communications and Multimedia Security (CMS 2001), 2001
[38] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, Attacks on Copyright Marking Systems, 2nd workshop on

information hiding, Portland, Oregon, USA, LNCS 1525, pp. 218-238, 1998
[39] H. Chang, and M.G. Atallah, Protecting Software Code By Guards, ACM CCS-8 Workshop on Security and Privacy in Digital Rights Management, Pennsylvania, USA, pp. 160 – 175, 2001
[40] TCG Specification Architecture overview, Specification Rev. 1.2, 28 April 2004, https://www.trustedcomputinggroup.org/
[41] Microsoft's Hardware Platform for the Next-Generation Secure Computing Base (NGSCB), http://www.microsoft.com/resources/ngscb/documents/NGSCBhardware.doc
[42] Intel's LaGrande Technology Architectural Overview, 2003, http://www.intel.com/technology/security/downloads/LT_Arch_Overview.pdf
[43] WIPO, Berne Convention, for the Protection of Literary and Artistic Works, July 24, 1971, www.wipo.int/clea/docs/en/wo/wo001en.htm
[44] WIPO (World Intellectual Property Organization) Copyright Treaty, 1996
[45] DMCA (The Digital Millennium Copyright Act), United States Copyright Law, 1998, http://www.copyright.gov/legislation/dmca.pdf
[46] European Union Copyright Directive, 2001/29/EC, May 22, 2001
[47] ACM (The Association for Computing Machinery), Computer Professionals Concerned DMCA Stifles Academic Freedom and Speech, www.acm/usacm/copyright/DMCA-release.html
[48] J. Leyden, Alan Cox attacks the European DMCA, The Register, UK, April 30, 2002, www.theregister.co.uk/content/4/25088.html
[49] M. K. Powell, Preserving Internet Freedom: Guiding Principles for the Industry, February 8, 2004, Remarks
[50] EPIC (Electronic Privacy Information Center): Digital Rights Management and Privacy, 2002, www.epic.org/privacy/drm
[51] R. Owens and R. Akalu, Legal Policy and Digital Rights Management, in Proc. of the IEEE, Vol. 92, No. 6, June 2004
[52] Cornell Law School, Title 17, Chapter1, Sec 107. - Limitations on Exclusive Rights: Faire use, US Code Collection, Legal Information Institute, http://www4.law.cornell.edu/uscode/17/107.html
[53] M. Berry, That's What I Want – Developing user-friendly DRM, CMP Media's New Architect, 2002
[54] C. B. S. Traw, Technical Challenges of Protecting Digital Entertainment Content, IEEE Computer Society, July 2003
[55] Commission of European Communities, Commission Staff Working Paper: Digital Rights, Background Systems, assessment, SEC/2002 197, Brussels 14/02-2002
[56] E. Becker, W. Buhse, D. Gunnewig, and N. Rump, Digital Rights Management: Technological, Economic, Legal and Political Aspects, LNCS 2770, Springer, 2003, ISBN 3-540-40465-1
[57] N. Garnett, Digital Rights Management, Copyright, and Napster, ACM SIGecom Exchanges, Vol. 2, Issue 2, Spring, 2001
[58] H. Abie, P. Spilling and B. Foyn, "A Distributed Digital Rights Management Model for Secure Information-Distribution Systems", International Journal of Information Security (IJIS), Vol. 3, No 2, pp. 113-128, Springer-Verlag, Berlin, Heidelberg, November 2004
[59] B. Schnier, The futility of copy prevention, Cryptogram, may 15, 2001
[60] P. Biddle, P. England, M. Peinado, and B. Willman, The Darknet and the Future of Content Ditribution, in 2002 ACM Workshop on Digital Rights Management, Washington DC. 18 November 2002,
[61] E. W. Felten, A Skeptical View of DRM and fair Use, Communications of the ACM, Vol.46. No. 4, pp. 57-59, April 2003
[62] S. Leisten, DRM Implications and Alternatives for IP in the Digital Age, In Proceedings of the IASTED International Conference on Communication, Network, and Information Security, pp. 264-270, December 10-12, 2003
[63] J. E. Cohen, DRM and Privacy, Communications of the ACM, Vol. 46, No. 4, pp. 47-49, 2003
[64] J. E. Cohen, A Right to Read Anonymously: A Closer Look at Copyright Management in Cyberspace, 28 Connecticut Law Review, No. 981, 1996
[65] R. Anderson, Cryptography and Competition Policy – Issues with 'Trusted Computing', Principles Of Distributed Computing (PODC), Boston, MA, 2003
[66] P. Kocher, J. Jaffe, B. Jun, C. Laren, and N. Lawson, Self-Protecting Digital Content: A Technical Report from the CRI Content Security Research Initiative, Whitepaper, 2003
[67] F. von Lohmann, Reconciling DRM and Fair Use: Preserving Future Fair Uses?, in "Fair Use by Design?" Workshop, 12th Computers, Freedom & Privacy Conference, April 16, 2002
[68] P. C. van Oorschot, Revisiting Software Protection, Information Security, 6th International Conference, ISC 2003, Bristol, UK, October 2003, proceedings, pp 1-13, Springer-Verlag LNCS 2851, 2003
[69] C. P. Wanigasekera and J. Feigenbaum (2003), Trusted Systems: Protecting sensitive information through technological solutions, Sensitive Information in a Wired World (CS457), 12 December, 2003
[70] First INDICARE State of the Art Report: http://www.indicare.org/soareport
[71] M. A. Einhorn and B. Rosenblatt, Peer-to-Peer Networking and Digital Rights Management: How Market Tools Can Solve Copyright Problems, Policy Analysis, No. 534, February 17, 2005, http://www.cato.org/pubs/pas/pa534.pdf
[72] B. Rosenblatt, Analysis of Cryptographic Research, Inc.'s Self Protecting Digital Content, April 14, 2003
[73] B. Schneier, Secrets and Lies: Digital Security in a Networked World, John Wiley & Sons, 2000
[74] GRid (Global Release Identifier), http://www.ifpi.org/site-content/grid/
[75] GUID (Globally Unique Identifier), http://en.wikipedia.org/wiki/GUID
[76] M. J. van den Hoven & G.J.C. Lokhorst. Deontic logic and computer-supported computer ethics. Metaphilosophy, 33 (3): 376-386, 2002. ISSN 0026-1068.

[77] J. Williamson, Editor of Convergence World, If Content Is King, DRM May Be Queen, International Engineering Consortium, July 2006, Volume 2
[78] A. Mana, M. Yague, S. Karnoukos, and H. Abie, Information Use-Control in Digital Government Applications, book chapter in Encyclopaedia for Digital Government, , Edited By Ari-Veikko Anttiroiko and Matti Malkia, Idea Group Reference Publisher, ISBN 1-59140-789-3, July 2006
[79] H. Abie, B. Foyn, J. Bing, B. Blobel, P. Pharow, J. Delgado, S. Karnouskos, O. Pitkänen, and D. Tzovaras, The Need for a Digital Rights Management Framework for the Next Generation of E-Government Services, International Journal of Electronic Government, Vol. 1 No.1, pp 8-28, Inderscience Publishers, (ISSN: Print 1740-7494, Online 1740-7508), 2004
[80] H. Abie, A Distributed Digital Rights Management Model for Secure Information Distribution Systems, Series of dissertations submitted to the Faculty of Mathematics and Natural Sciences, University of Oslo, Book ISSN 1501-7710, UniPub AS, January 15, 2005
[81] Center for Democracy and Technology, http://www.cdt.org/
[82] Electronic Frontier Foundation, http://www.eff.org/IP/DRM/
[83] XIWT, Cross-Industry Working Group, Managing Access to Digital Information: An Approach Based on Digital Objects and Stated Operations http://www.xiwt.org/documents/ManagAccess.html, May 1997
[84] H. Abie, P. Spilling, and B. Foyn, Rights-Carrying and Self-Enforcing Information Objects for Information Distribution Systems, in the Proc. of ICICS'04 - October 27-29, 2004, Malaga, Spain, LNCS 3269, pp 546-561, ISBN: 3-540-23563-9, Springer Berlin / Heidelberg
[85] B. Rosenblatt, 2006 Year in Review: DRM-Enabled Content Services, December 27, 2006 http://www.drmwatch.com/ocr/article.php/3651116
[86] B. Rosenblatt, 2006 Year in Review: DRM-Related Legal Actions, December 29, 2006, http://www.drmwatch.com/legal/article.php/3651421
[87] B. Rosenblatt, 2006 Year in Review: DRM Standards, December 27, 2006, http://www.drmwatch.com/standards/article.php/3651126

**Dr. Habtamu Abie** is currently a senior research scientist at the Norwegian Computing Center. He received his B.Sc., M.Sc. and Ph.D. from the University of Oslo, and has many years of experience in computing, both as practitioner and researcher. He has a solid and extensive background in the design and development of real-time systems, and the design, modelling and development of security for distributed object computing systems. He has been a fellow at CERN. He participates as a reviewer and member of the technical program committee in international conferences and workshops and reviews scientific papers in books and international journals. His past and present research interests encompass DRM, security (protocols, requirements, policy, privacy, trust, risk management) in distributed and communications systems, architecture and methodology, formal methods and tools, hard real-time systems, and mobile, ubiquitous and ambient intelligent computing.