The Interactive-Music Network

DE4.5.2
Protection of coded music

Version: 1.2
Date: 01/06/05
Responsible: Fraunhofer-IGD, (FHGIGD)

Project Number: IST-2001-37168
Project Title: The Interactive-Music Network
Deliverable Type: PUB
Visible to the Working Groups: YES
Visible to the Public: YES

Deliverable Number: DE 4.5.2
Contractual Date of Delivery: 31/05/2005
Actual Date of Delivery: 01-06-2005
Title of Deliverable: Protection of coded music
Work-Package contributing to the Deliverable: WP4
Nature of the Deliverable: Public
Working Group: WG-PROT
Author(s): Martin Schmucker (Fraunhofer-IGD)

Abstract:
This document explains the basic knowledge needed to understand the fundamental functionality of DRM systems. It includes intellectual property rights, general requirements on DRM solutions, basic concepts of DRM solutions, business models, individual technologies (e.g. content identification and description, rights management, encryption, watermarking and fingerprinting). This document aims to support people and organisations in selecting or developing suitable technology for their specific requirements on the protection of musical content.

Keyword List:
music, multimedia, infotainment, edutainment, music notation, standards, music libraries, music distribution, music protection, protection, watermarking, fingerprinting, accessibility, education, music archives, music publishing.

Table of Contents

1. Introduction

More than five centuries ago copying content was difficult as each manuscript had to be copied by hand. Yet, this was the only possibility to save manuscripts although human errors were introduced in each copy causing a content decay. Technological progress, especially the movable-type press and digital technology, changed this situation completely: Nowadays, creating and also copying content is easy and protection has become an important issue for digital data as digital data can be copied without any loss of information and it can be distributed immediately all over the world via the Internet. While physical materials benefit from physical barriers, unauthorized exploitation of digital content has never been easier before. As a result, huge efforts have been spend on the developments of mechanisms addressing infringement before digital rights management (DRM) came into existence.

The term DRM comprises technologies that allow the usage control of digital content. This goes beyond the possibilities copyright holders had before, thus DRM threatens user privileges. For example, fair use[1] or archiving of content is also restricted as DRM systems restrict access to content. Unfortunately, there is no unique definition for DRM. Thus, when somebody faces the term DRM the connotation associated with it must not be neglected. In [ALA2005] an outlook on different connotations is given:

- "Digital rights management technologies are aimed at increasing the kinds and/or scope of control that rights-holders can assert over their intellectual property assets." - *Electronic Frontier Foundation*
- "DRM must be about the "digital management of rights" not the "management of digital rights." - *W3C Workshop Report on DRM for the Web*
- "The purpose of DRM technology is to control access to, track and limit uses of digital works." - *The American Library Association*
- "DRM are the technologies, tools and processes that protect intellectual property during digital content commerce..." - *Publishers' Requirements for DRM, W3C Workshop Report on DRM for the Web*
- "DRM systems restrict the use of digital files in order to protect the interests of copyright holders." - *Electronic Privacy Information Center*

Camp [Camp2003] outlined the copyright system's legal, technological, and economic foundations with the aim to support the design of DRM systems. She identified several key functions[2], which should be considered in the requirements of a DRM system. Among these key functions identified by Camp are:

- protection of the author's reputation
- protection of the work's monetary value
- archiving of content
- ensuring of content integrity
- providing surety through persistence[3]
- facilitating personalization through filtering and annotation[4]

Although copyright defines under which circumstances copying is legal and when copying is illegal, copyright infringements are ubiquitous. Some IPR infringements are obvious. Yet, a huge mass of people infringing IPRs – e.g. by exchanging music files in P2P-networks – is aware of their malpractice. One important issue that certainly hinders users in realizing copyrights infringements is the fact that the digital original is still available and even untouched, which is in contrast to stealing of physical goods. Therefore several campaigns were launched addressing the topic “copying is stealing”. For example in 2003 MPAA

[1] Fair use is a statutory exemption to the copyright law.

[2] Interestingly the existing solutions analysed by Camp, which included copy protection as well as circumvention technologies, only partially fulfilled these requirements.

[3] The analogue mass-production ensured that a document survives unaltered and can be located.

[4] The publishers’ and broadcasting investment results in a careful selection of content.

launched an advertising campaign “copying is stealing” to sensitive public that IPR infringement by private people can be compared with stealing a CD from a record shop [MPAA2003].

Similar threats to music can be identified even before in the pre-digital age (before the 1980s), for example short after the completion of the first pianolas in 1895 [Pianola] a Pinola copyright ruling was cited in 1899 [Pianola1899]: “Boosey vs Whight (1899) involved copyright charges arising over the production of pianola rolls, in which the court found that the reproduction of the perforated pianola rolls did not infringe the English copyright act protecting sheets of music.” (see also [Pianola1908]).

When analogue audio tapes and also video tapes emerged potential threats caused by illegal copies were realized. As described in [MPAA2003] in the pre-digital age several legal disputes are known where copyright owners claimed copyright infringement offences:

- Ames Records allowed subscribers to hire records from it for a small rental charge.
- Amstrad supplied tape-to-tape recording equipment.
- Sony's video recorders were used for illegal copying.

Interestingly, neither Ames nor Amstrad nor Sony was liable for copyright infringement. Before the introduction of the compact disk (CD) in 1982 music was typically sold on long playing (LP) vinyl records. The sales LPs slowly declined with the introduction of the music cassette (MC), which allowed copying of music [Lewis2003]. However, content was stored in an analogue representation. Copying this analogue content was not possible without loss of quality. Therefore a “natural barrier” existed limiting the amount of recopies. In addition to these natural barriers copy prevention systems were developed. This natural barrier no longer exists in the digital world. As the storage and distribution of audio content other then in digital format can be neglected we will not consider the analogue world in this report.

Nowadays, copying digital data is much easier and commercial oriented pirates as well as some consumers exploiting these new opportunities: Digital data can be copied without any loss of information and distributed fast world-wide via the Internet. Especially P2P file-sharing networks - the most popular one was probably Napster - enable users to share content. Although the US courts shut down Napster[5] [Napster] rights holders still claim that Napster's descendants cost them billions of dollars in revenues. As direct consequence rights holders are now targeting consumers, ISPs, operators and even founders of file sharing systems.

Although this kind of illegal distribution is the major traffic in P2P-network, there are other kinds of illegal distribution: E.g. besides the digital distribution of highly compressed data via the Internet, pirates are selling counterfeited media carriers to customers, who want to buy original content.

While the rights holders were quite successful against Napster actions against other P2P-software suppliers like Grokster [Grokster] and StreamCast [StreamCast] failed because the technology can be used for legitimate purposes, the service suppliers cannot control the use of the technology by the end user and the users' communication is entirely outside the control of the service suppliers.[6] Although Verizon RIAA won a court order forcing an Internet Service Provider to disclose the identity of individual consumers who traded music files, technologies like Freenet[7] [Freenet2004] allow users to share any kind of content strongly reduced risk of being identified by rights holders. It seems that P2P-developments reacted on the content industries activities: While the first generation of P2P-file sharing networks has a centralised file list, the second generation is a purely distributed architecture. The third generation addresses the anonymity of its users [WIP2P].

The content industry – especially the music and movie industry – nowadays sues P2P users who exchange content illegally. At the beginning of these activities, the P2P users reduced their illegal file exchange [MC]. Nowadays, news spread continuously that P2P users are sued for their IPR infringements.

[5] An information collection is available at RIAA [NapsterCases].

[6] Napster had a centralised architecture while its descendants are decentralised.

[7] Freenet can be summarized as a decentralized network of file-sharing nodes tied together with strong encryption and further technology, which allows anonymous users.

Additionally, the content industry started PR campaigns to raise the users' awareness for the illegality of the file sharing of copyright protected content. Despite these activities, illegal P2P-usage seems to have increased again and users identified other ways of exchanging content [PEW]: "Beyond MP3 players, email and instant messaging, these alternative sources include music and movie websites, blogs and online review sites." Also, with portable storage devices sharing content is very easy and convenient.

Although this document focuses on the protection of music we also like to stress that there is no unique view on the influence of P2P-exchange to the development of the market. On the one hand, each copied file can be considered as a loss. On the other hand people might download content as a foretaste. Different reports and studies exist where common people have been interrogated about the influence of P2P-networks. The results of the studies are contradicting comparable to the results of studies trying to identify the reasons for the decrease in CD sales.

The technical endeavours of controlling the usage of content are summarized in the term "digital rights management" (DRM) and were first focused on security and encryption addressing the problem of unauthorized copying. But DRM evolved and now it covers various issues including:

- the description of content
- the identification of content
- trading and exchanging content
- protection of content
- monitoring/tracking of content distribution and its usage

As emphasised by Iannella [Iannella2001], DRM is the "digital management of rights" and not the "management of digital rights". Thus, it has become a very complex area addressing issues far beyond security and encryption.

1.1. Structure of the document

This document explains the basic knowledge needed to understand the fundamental functionality of DRM systems. After some explanations of IPR within this introduction chapter the next chapters describe the general requirements on a DRM solution. Then we introduce the basic concepts of DRM solutions. As the concepts always support business models these business models are explained afterwards. Having in mind the general aspects of DRM we present some specific individual technologies including content identification and description, rights management, encryption, watermarking and fingerprinting. This document aims to support people and organisations in selecting or developing suitable technology for their specific requirements on the protection of musical content. Short analyses of current solutions as well as standardization efforts give further information and support.

After the introduction in this section basic legal issues are summarized in chapter 2. These are followed by the user requirements in chapter 3. Although several users are potentially involved, this report focuses on content creators, content providers and consumers. Chapter 4 finalises the social-economic aspects by describing fundamental business models. An overview on technological aspects is given in chapter 5. The general components of DRM systems and their interactivity are described. Details of the individual basic technologies can be found in chapter 6. Existing DRM systems are characterised in chapter 7. Recent developments are outlined in chapter 8. An outlook in chapter 9 finalises this report.

2. Intellectual Property Rights

In this section we shortly summarize the topic Intellectual Property Rights (IPR) given in [MUSICAL1.2]. Yet, due to the numerous facets of this aspect this summary is a motivation for DRM and not a detailed description. For a detailed description of legal issues we suggest to consider adequate material like [Bechtold2002b]. Also, in [Rosenblatt2002] there is a chapter addressing the interweavement between law and technology: Rosenblatt et al. describe the basic types of intellectual property including:

- patents,
- trademarks,
- trade secrets, and
- copyright.

First, we will introduce related rights management terminology as given by Rosenblatt et al. [Rosenblatt2002], before going into technical details of rights management technology[8]:

- *rights holder:* a legal entity owning rights in intellectual property
- *user:* a legal entity that intends to make use of intellectual property rights
- *content owner:* see rights holder[9]
- *rights transaction:* a business process involving legally acquiring intellectual property[10]
- *agent:* a legal entity authorized by a rights holder to enter into a rights transaction on behalf of the rights holder
- *royalties:* a monetary compensation to a rights holder or his agent for the use of intellectual property rights
- *rights management:* a business process, which tracks intellectual property rights and related issues
- *digital rights management:* digital management of rights[11]

Rosenblatt et al. calls rights management systems existing before DRM "old rights management" (ORM), which mainly consists of different organizations that came into existence as a reaction of technological menaces identified between the 40s and 60s.

- *The American Society of Authors, Composers, and Publishers* (ASCAP) provides music licenses to users and royalties to members through a collective licensing system.
- *Broadcast Music International* (BMI) is a performing rights organization comparable to ASCAP.
- *Copy Clearance Center* (CCC) developed a licensing system.
- *The International Confederation of Societies of Authors and Composers* is a non-profit organization representing authors and composers.
- *Harry Fox Agency* (HFA) is the subsidiary of NMPA.
- *Motion Picture Association of America* (MPAA) and *Motion Picture Association* (MPA) are organizations related to the movie industries. MPAA was founded as a national trade association. Several years later MPA was formed to represent the audiovisual industry worldwide.
- *National Music Publishers Association* (NMPA) represents "mechanical" rights related to music such as reproduction and "synchronization rights".
- *Recording Industry Association of America* (RIAA) "fosters a business and legal climate that supports and promotes members' creativity and financial vitality". Together with the major record labels it started the "Secure Digital Music Initiative".
- *SESAC* (a French organisation) started as a licensing agency for classical music.

[8] Further definitions can be found at [CEN/ISSS2003].

[9] A content owner may not own all rights to the content.

[10] It includes a simple process (buying an article) and complex processes (like buying a business or rights holder).

[11] According to Rosenblatt et al., rights management that uses digital technology and applies to IP in digital form.

Some of the previously listed organizations influence the digital world. Yet, not all have or had the same influence on the legislative, which tries to balance the impact of new possibilities of digital media. For example, certain possibilities related to digital media were and are still regulated by law in the so-called copyright.

2.1.1. Intellectual property and copyright

As Intellectual Property (IP) is the basic for the following chapters, first the term “IP” has to be defined. IP is described in [MUSICAL1.2] as “creative ideas and expressions of the human mind that have commercial value and receive legal protection in the form of property rights.”, which include patents, trademarks, designs and copyright.
Hence, IPR's main purpose is to prevent others copying a person's original work. IPR lasts for a specific duration[12]. After this well-defined period of time the work enters public domain. “Copyright” is generally equivalent to “author's rights”. Although certain organisations like World Intellectual Property Organisation (WIPO) prefer the term “author's rights”, “copyright” is used within the area of DRM.

Cohen [Cohen2002] describes how copyright changed due to the appearance of online work: Initially copyright didn't control or access to or private use of an already purchased copy. Also copyright didn't interfere with fair use derivatives. Today content owners claim the right to control the access to and the use of content.

2.1.2. Music copyright

Music copyright is a negative right, which means it gives the composer the right to restrict others from certain activities including copying music. Third parties not acknowledging these restrictions are liable for copyright infringements. Copyright automatically arises upon the creation of content without any formal registration process. Thus, copyright is distinct from other subsequent copyrights.

Music copyright includes different exclusive rights. For example the U.S. copyright law give copyright owner the right to (details can be found in [MCTable]):

- reproduce copyrighted work
- prepare derivative works
- distribute copies
- perform the work publicly
- perform sound recordings of the work publicly

Further information on (music) copyright can be found at [C4MusicLibrarians], [CInMusic], [CIssues], [CMyths], [CGuru], [CPrimer], [ArtistPro] and [CGov].

2.1.3. Publishing rights and licensing

Copyright owners have the exclusive right to reproduce or make copies of their work. Furthermore, the copyright owner also has the exclusive right to perform publicly a copyrighted work, directly or indirectly through means of communication or transmissions. While these two rights (recording and public performance rights) where clearly separated before the digital distribution of content via the Internet, today this is not so clear anymore. Hence service, providers are forced to obtain multiple licenses from different parties. This process can be very difficult as typically each right is connected with certain limitations. Rights can be negotiated either with the rights owner or with collection societies.

2.1.4. Legislation

International agreements that protect artistic and literary works aim to harmonize legal definitions and terms of protection. In the Berne convention, which was signed by more than 1979 member states in 1979, such an international framework was determined. Yet, this framework has a degree of freedom to deviate from: As described in [Cohen2002] the copyright industries had secured an international

[12] E.g., the copyright for a new composition lasts for the lifetime of the composer and additional 70 years after his death.

commitment to additional legal protection for technological protection regimes in the 1996 WIPO Copyright Treaty, which leaves member states substantial flexibility in implementation.

The Digital Millennium Copyright Act of 1998 (DMCA, U.S.) forbids circumvention of access control technologies and also the manufacture and distribution of circumvention devices. Hence usage controls are protected indirectly. One side effect of the DMCA is shown in the SDMI-hack [Craver2001] where the content industry tried to stop Felten distributing his research knowledge [Felten2002].

In Europe the digital copyright directive was approved, which defines a range of devices that are to be prohibited. Yet, it leaves member states free to define what constitutes “adequate legal protection” against the act of circumvention. Member states may require preservation of exceptions (e.g. private non-commercial copying)

Furthermore there are other legal frameworks, e.g. the Uniform Computer Information Transactions Act (UCITA), which would validate consume “assent” to these restrictions and legitimise the accompanying technological controls as part and parcel of the agreement.

Other potential areas of conflict are fair use and privacy. The possibilities of DRM are usage control. However a qualification of the usage is difficult. For example computers cannot distinguish (so far) between legal and illegal copying. Thus, a restrictive policy is enforced by DRM: No copying is allowed. This led to interesting court decisions like in France, where the French court ruled that copy protection schemes have to be removed from DVDs [REGDVD]. Similarly, the Deutsche Bibliothek[13] signed an agreement with the content industry that allows to crack and to duplicate DRM-protected digital media. Here, DRM opposes its legal mandate “to collect, process, and bibliographic index important German and German-language based works” [DDB]. Also, information is exchanged and stored. For example customer exchanges information with a third trusted party, which stores this information. This potentially infringes privacy of the customers.

2.1.5. Illegal file sharing

Obviously, content sharing is restricted by copyright as the copyright restricts copying and distributing content if not permitted by its author respectively composer. The problem for users is that they are not aware of the illegality of the sharing activity. In contrast to sharing (or more obviously theft) of physical goods digital content can be easily reproduced. Thus no other user experiences a lack of digital content in comparison to physical goods. Nevertheless, file sharing is against the copyright unless

1. the content is in public domain,
2. the owner/creator gave permission to share it, or
3. the content is available under pro-sharing license (e.g. Creative Commons [CC]).

Therefore the content industry successfully identified and still identifies users who illegally distribute digital content on the Internet via websites or via P2P-networks. Each user can be identified through the IP-address, which is required to access the Internet. For permanent IP addresses this is very easy (e.g. in the case of companies). In the case of dynamic IP-addresses (dial-in access) the Internet Service Providers (ISPs) store temporarily this information. The content industry was successful in identifying users by requesting user related data from the ISPs.[14] Nevertheless, this procedure is under strong discussion and different verdicts exist in the different countries.

Not only is this procedure but also the lawsuits under discussion. “Eight of nine lawsuits filed last summer against Emory students accusing them of illegally sharing copyrighted music files have been dismissed, according to Senior Vice President and General Counsel Kent Alexander. The Recording Industry Association of America (RIAA) spokesperson Jenni Engebretsen said that one of the Emory cases has been settled, but she could not confirm the dismissal of the others. ” [EW2005]

[13] The “Deutsche Bibliothek” is the German analogue to the US Library of Congress.

[14] Generally, user anonymity is not given. All users can be traced back by their IP and with the support of the ISP. It is very important for wireless-LAN (WLAN) operator to secure access to their WLAN against misuse as these operators are responsible for any kind of misuse.

2.2. Scenarios

DRM systems can be used in different scenarios. Although the main reasons for its application is the protection of IPR there might be some differences according to the individual scenario. These differences will reduce or increase the required DRM functionality.

- *Business-To-Business (B2B)* scenarios allow different assumptions, which are affected by the relationship between the business partners. Typically there is a certain level of trust between the partners otherwise they would not have a commercial relationship. Considering the computers hardware can be considered as administrated by a "well-selected" person and other persons are not able to modify the software installation on computers.

- *Business-To-Consumer (B2C)* scenarios are different to the B2B-scenario as there needn't or can't be a certain level of trust between the partners[15]. But what is even more important is the fact that consumers have full control on their computers.

- *Consumer-To-Consumer (C2C)* scenarios are very interesting especially when considering social and legal aspects of DRM solutions. But these scenarios are not addressed in this document.

Of course, the previous examples are not comprehensive in depth as each scenario has specific requirements. Also there exist several hybrid forms not only due to the fact that content owners distribute content with the support of retailers. And this is indeed the main advantage of the Internet: its flexibility. Any business model can be selected for distributing content and adapted quickly. We will shortly address different business model in the next section and in chapter 4. But concerning the security of content one must keep in mind the different assumptions on the possibilities of the involved parties.

2.3. Business models

In this subsection we will give a short introduction into possible business models. More details can be found in chapter 4 and in [MN_DCM]. Business models can be distinguished by the type of organisations involved. Typically the distinction is between business-to-business (B2B) and business-to-customer (B2C). Although other types are possible like B2B2C (via intermediates) or C2C (like in eBay). Here protection aspects have to address distribution of content and the usage of content.

Especially usage is important as this is directly related to the rights the customer purchased and which are fixed in the license. Different cost models exist, which are more or less supported by existing DRM systems.

The most important ones are:

- Pay-per-download
- Pay-per-rendering
- Time-limited flat-rate
- Rendering-limited flat-rate
- Subscription based models

Microsoft's announced DRM-solution called "Janus" will provide new possibilities for subscription based models (see also subsection 9.4.3). The most important insight so far is the fact that users are willing to pay music. This was not only demonstrated by Apple's iTunes Music Store. In total, the numbers of songs purchased online is strongly increasing.

2.4. Technology overview

The term DRM comprises different technologies, which were initially designed to enforce restrictions on content or to protect the interests of the content owners. Thus restrictions have to be expressed within a

[15] Here trust is related to the actions of the consumer after purchasing a product or a digital item. There is no guarantee that a customer doesn't infringe any right at all.

DRM system. This is traditionally done by rules, for example number of rendering[16], renderable periods, etc. Hence, rules are central in the design of a DRM system.

As different business models can be supported by DRM solutions, we try to shortly describe typical business models below. An extensive description of some of the following business models can be found in [Rosenblatt2002]:

- promotional content by limiting to a specific number of renderings
- distributed retail by distributing content to retailers who sell it to customers (super distribution)
- super distribution P2P-environments
- license per content
- license per collection of content
- license per rendering
- subscription
- selling rights

More information about business models in the music distribution sector is available at [MusicNetwork]. Obviously, choosing the right business model does not only depend on monetary criteria. Other issues include market and user analyses or improved products and services. These are criteria are reflected in Iannella's functional analysis [Iannella2001].

Depending on the functional issues different technologies are deployed. However we will limit the discussion in this document to functional aspects and technologies related to digital rights management. Therefore technologies, which have to be considered in a complete system, e.g. billing components or components tracking users' behaviours, are not included in this document. Additionally we don't analyse the security of different technologies or implementations. The security analysis of different systems is very complex and typically a general analysis cannot be transferred to specific applications. The necessity of a specific security analysis is expressed e.g. in [Felten2003] who explains the first rule of security analysis ("understand your threat model") in the case of DRM and P2P-networks. Yet, one has to be aware that any DRM system is as strong as its weakest component. Hence, if a weak technology or a weak implementation is used the complete DRM solution suffers.

2.5. Summary

The legal situation is complex by its nature and far beyond the scope of this report. Especially in Europe the situation is even more difficult: Although the different European countries implement the same directive, national differences can be identified. Furthermore, contracts are valid for certain countries and national bodies – like the royalty collecting societies – cause further difficulties and problems. This national aspects are very crucial as the Internet spans over borders.

We provide a technological overview in chapter 5. Issues related to rights management are explained in section 6.2. Section 6.3, 6.4, and 6.5 explain individual technical aspects of encryption, watermarking, and fingerprinting. The functionality of an integrated DRM system is described in Chapter 7 explaining how the different components interact. A short history of the development of DRM can be found in [MUSICAL1.2]. Additional information on DRM is available in [CEN/ISSS2003].

[16] As general DRM is independent of the distributed content we use the term "rendering" as a summary of all possible actions with content.

3. Needs and Requirements

In principle, three different parties are involved in the distribution of content:

- content creators
- content providers
- consumers

Of course, this model is simplified. For example to sell a CD to a consumer, the music has to be played and recorded. The recorded music has to be mixed and a master record has to be created. CDs have to be created and delivered to stores. And the stores finally sell them to the customers. Similar additional steps are necessary for the production of sheet music.

These different parties have specific interest that might be mutually exclusive especially for business. For example, a content provider might want to maximize his income and therefore might increase the prices of his offers or restrict possible usages. On the contrary a consumer might want to minimize the costs or maximize the usage of the bought goods. Although consumers a typically not involved in the decision process determining the used DRM solutions the consideration of their needs determines the acceptance of a solution and therefore the market success. Similarly content providers are also affected by the variety of their offers.

For the distribution of digital, content creators potentially could remove the intermediaries involved in creation and distribution: A physical product, e.g. the audio-CD, is not necessary. A MP3-file should be sufficient. This can be distributed directly to the consumers with Internet access, who buy the MP3 file on the artists or creators website. Obviously, an ordinary artist is not able to perform all the work of the intermediaries. Additional tasks might be also necessary like the web shop. Thus, not all the intermediaries' tasks' can be solved by the musicians efficiently. Thus, the intermediaries will cover new tasks or perform carry them out in a new way: For example, labels might focus their task on the promotion of artists[17] and the organisation of live performance and artist tours. Similarly, supermarkets started online music shops.

3.1. General questions relevant for content creators

Content creators contribute their work to content providers. They are first interested in the benefit of the distribution and the protection level of their content in the distribution solution. Benefit is not limited to monetary aspects but also includes visibility, sales promotion, customer relationship, etc. If these aspects are interesting for content creators the next hurdle will be the integration of content in the distribution system. This is exemplified in the following questions on the protection and the distribution of content.

Potential questions of creators on the distribution aspects:

- Are multiple business models supported?
- Can the business model be chosen dynamically?
- Can content be integrated easily in the solution?
- Are modifications (e.g. format conversions) necessary?
- Which file formats are supported?

Potential questions of creators on the protection aspects:

- How good is the protection of content?
- Can the usage of content be monitored?
- Does protection influence the content itself?

[17] For example, when music videos became more and more important the labels supported artists in the production. Now labels can support artists in the creation and support of web pages.

Considering the questions relevant for content creators, one important fact must not be neglected: Only for a few artists their content is their primary source of income. This is indirectly discussed in [TP], which discusses the effects of IPR for originators.[18]

According to [TP], which reviews [OS], the benefit of illegal copies for artists and the general public is determined by network effects. Networks effects are explained with software technology: The more people use the same software the more the usage value of the software is increased. This is independent of the way the software is acquired. [OS] considers legal and illegal users and analysis three scenarios: illegal copying is possible, illegal copying is not possible without incorporating the illegal users, and illegal copying is not possible with incorporating the illegal users.

This scenario is similar to the situation of artists (see also [Gayer]). For artists the so-called “spill-over effect” is important: the more popular an artist is the bigger is the income from secondary sources like live performance, advertisements, or ring-tones. Summarized, a monetary benefit of stopping illegal copying and distribution can be achieved only if the income from media sells is very high. Otherwise the spill-over effect is more important. More details can be found in [Kretschmer].

3.2. General questions relevant for consumers

Obviously, the most important concern for users is the usability of the content. Consumers purchase content for listening or rendering it. If digital content is reduced in its usage its value for the consumer is also reduced independent of the reason for this limited usage. The dependency between the usability reduction and loss of value is not linear. This can be compared with physical products, which at least have to fulfil a minimum amount of requirements. Otherwise the physical products are valueless even if they fulfil other additional requirements.

Generally, consumers will accept a digital distribution solution if

- content fulfils their needs in terms of usability, quality, diversity and variety
- costs (e.g. ease of use and value) are reasonable in comparison to the benefit
- it ensures their privacy

Here costs are not only the price for the product. Other factors like complexity of acquisition process (e.g. registration, payment or software installation) or usage limitations (e.g. due to a strong protection model) raise the costs and should be considered. Users’ aspects include acquisition and usage of content.

Potential questions of users on the content acquisition:

- What are the software requirements for the download?
- How complex is the registration process?
- What else is necessary for the download?

Potential questions of users on the content usage:

- How strong will restrictions influence the usage? (DRM = Digital Restriction Management)
- What kind of rendering software (audio and video players, image viewer...) must be used?
- What about the exchange of data with other devices? (ideally no limitations)

Of course some users are also concerned about privacy.

3.3. General questions relevant for content providers

On the one hand content providers need content. On the other hand customers have to buy this content. Therefore they depend both on content providers and on customers and they have to balance the needs of content creators and customers in a reasonable way allowing a working business model. Content providers and customers, the content itself, and the chosen business model determine relevant needs. Yet,

[18] We will not discuss the benefit of copyright here. Instead we’d invite the reader to revise these arguments to embrace a huge variety of different needs.

a content provider has to be aware what kinds of products have to be protected or managed digitally and how (how long, how strong …) they have to be protected. And these aspects are indeed important as DRM is certainly a restriction of rights, which becomes easily contradictious to content providers' major aim in selling access. Also the content type lead to implications on and might even has some restrictions on usable technology.

Furthermore a distribution solution must address various further aspect not only related to the DRM functionality. As DRM functionality is combined with other functionality the resulting systems address new fields. New issues are emerging relevant for the design and the usage of DRM and solutions. We give some examples below:

3.3.1. Legal framework

The distribution and protection system must be within the legal framework. For certain countries this can be done easily due to the homogeneous law system, e.g. in the United States. Yet, in Europe this is more difficult as national laws and copyright related issues differ. Content providers facing these challenges have to solve a huge juristic and administrative overhead before they are able to provide content. Furthermore these differences influence the structure of the distribution and protection solution. E.g. fair use might be treated differently within European countries, which influences the restrictions in a protection solution. The resulting additional efforts are sometimes not manageable. Therefore unique IPRs at least within Europe would improve the situation of content providers.

3.3.2. Customer relationship

The tracking systems of protection solutions can be used to improve the information available about customers and their habits. This kind of information can be used to improve external services to customers or to improve internal decision processes like the stock composition.

Relevant information includes customer related information, like

- further information about customers behaviour
- information about/from other customers (reviews, similar interests)

as well as content related information, like

- protection of content
- monitoring of content distribution and its usage
- tracking of content distribution

It is important to use this information according to the privacy regulations of national laws, which might influence the amount and the kind of information that can be extracted.

3.3.3. Content related aspects

The tracking system also provides further functionality for identification and description of content, like

- content identification of previously unknown content
- creating a link of content to general additional information (e.g. general meta-data)
- creating a link of content to different kinds of content descriptions (e.g. content usage depending information, e.g. usage in a commercial vs. the "plain" content)

3.3.4. Copy accuracy

The key functions' design considerations of the copyright system as identified by Camp [Camp2003] must be expanded beyond those given by law. Camp states that economic and technological factors must be included instead of recreating existing law in a digital network. His postulation is based on the nature of technology: Technology alters society as it diffuses through it. The result of this recognition leads to a 'larger technological, economic, and legal system', which he called *copy accuracy*. His copy-accuracy functions include:

- author monetary incentive
- reputation right
- attribution and integrity
- persistence and archiving
- access
- personal annotation

In his article Camp analysed the effects of three different systems and their 'adversaries' (DRM proponents and opponents) according to his copy-accuracy functions:

1. Adobe's eBook and Elcomsoft's Advanced eBook Processor
2. the CSS of DVD players and DeCSS
3. Giovanni (a system embedding labels by watermarking content) and free content

Camp concluded that during the creation of his article (in 2003) no system supported the set of the copy-accuracy functions. However Camp admitted that the set of design requirements was not trivial and that designing a DRM system satisfying these requirements would include secure storage, micro-credit, archiving, distributed caching, censorship-proof publishing, and reputation systems.

3.3.5. Payment

Credit card fees play an important role when the transaction volume is small, which is typically the case for paid download. This is clearly in contrast to online orders of physical goods where in addition to the costs of the goods additional costs for transportation play an important role. Therefore different micro payment systems have been developed reducing the fees for online transactions, which is important for digital contents.

As discussed in [Buente04] and [IWW03] consumers have different expectations on the payment systems including:

- The payment system should be well known and commonly used to avoid difficulties.
- Paying should be comfortable, e.g. difficult registrations should be avoided.
- Payment should be anonymous.

In [IWW02] different payment systems are distinguished, as shown in **Figure 1**:

- *Pre-Paid*: Pre-paid payment systems can be generally considered as not as customer friendly as other systems as they require a monetary transfer before receiving the content. Pre-paid methods can be hardware- or software-based.
- *Pay-Now*: Cash on delivery and debit is comfortable payment systems for consumers. Consumers only have to transmit their address and no credit-card information has to be exchanged. Further pay-now methods are based on mobile payments or payment per email.
- *Pay-Later*: These methods include credit card, invoice or billing systems.

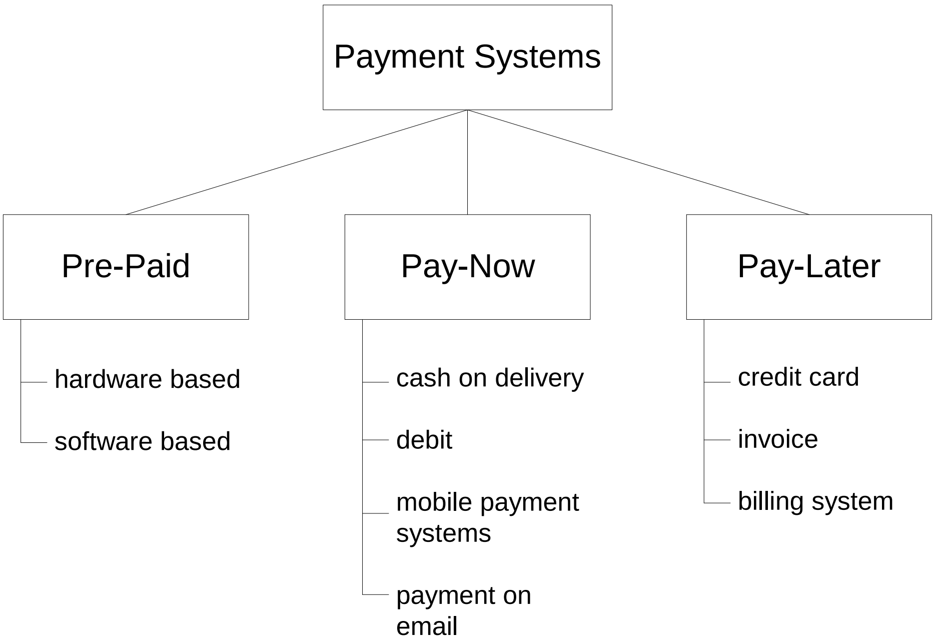

Figure 1: [IWW02] differs between pre-paid, pay-now and pay-later payment systems. The individual groups have specific (dis-) advantages for consumers or content providers. A cost efficient payment system is essential especially when relative cheap content is sold online. Otherwise the costs for the payment strongly distract costumers from any online purchase.

3.4. Summary

This report showed that the requirements of the different parties involved in content distribution and usage are not always in line. Apparently, they are incompatible – at least at first sight. A balancing of the different needs is necessary. But this is a standard process on the market. Merchants offer goods and users can decide if they buy it or not. The situation with DRM is similar: Customers can decide if they buy content wrapped in certain DRM containers, which enforce the requirements of certain content owners and providers. Yahoo recently started a service called “Yahoo! Music unlimited” where customers have unlimited access to subscription music catalog for less than 5$ per month if paid on an annual basis. This is very in line with what consumers are expecting.

4. Different Business Models and Possible Technological Support

Distribution of content is directly related with business models. Yet, we do not intend to discuss and judge different business models. The objective of this chapter is to describe how DRM can support different business models. For further information we suggest the reader to consult [Rosenblatt2002], [DT2004], and [Bockstedt2005].

4.1. Traditional music industry value chain

A simplified traditional music industry value chain is shown in Figure 2. Its purpose is to exemplify the influence of digital representation and DRM on content distribution. For specific content like audio or sheet music the content value chain varies. Different chain links can be identified in the general content value chain:

1. Composition
2. Selection, production, and recording
3. Copyright and licensing
4. Marketing and promotion
5. Manufacturing
6. Distribution
7. Sales
8. Consumption
9. Innovation

We also consider the value chain as value circle: Existing content is typically the starting point for innovation, which is already the case for the traditional value chain.[19]

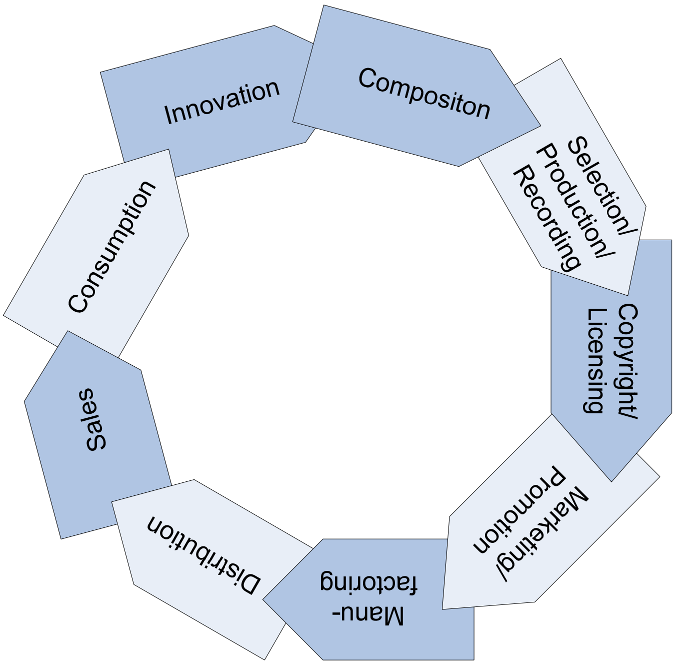

Figure 2: The traditional music value chain involves different players for composition, selection, production, and recording, copyright and licensing, marketing and promotion, manufacturing, distribution, sales, consumption, and innovation.

[19] There are different opinions on this on other areas, e.g. [Marion1998]. However, for the digital value chain this might be more evident, as content available in digital format can be processed more easily. Thus the cycles are rigorously shorter.

4.2. Digital music industry value chain

The digital content representation strongly influences the production and distribution of music. Music has become or is becoming a digital good. As a consequence of the digital representation of music, the processing and distribution possibilities are extended. These new possibilities not only blur the boundaries in the traditional content value chain. The result is a downsized content value chain, as shown in Figure 3:

1. Composition, production, and recording
2. Copyright and licensing
3. Marketing and promotion, Distribution, Sales
4. Consumption
5. Innovation

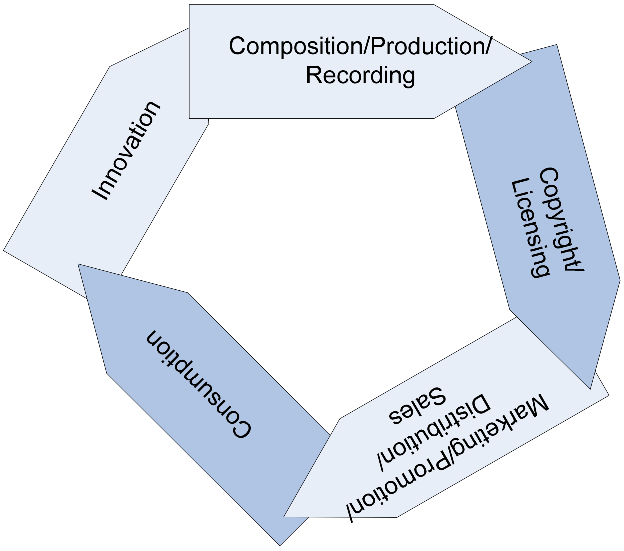
Composition/Production/ Recording
Copyright/ Licensing
Marketing/Promotion/ Distribution/ Sales
Consumption
Innovation

Figure 3: The digital music industry value chain is downsized through the possibilities of digital content representation and its distribution. From content and rights owners' point of view, this allows more efficient content distribution to customers. Furthermore, due to the loss of hardware costs and the capabilities of the computers, more tasks can be performed with less equipment. Obviously, the cycles are rigorously shorter than in the traditional content value chain.

4.3. Influence of DRM on the digital music industry value chain

In Figure 3 we showed the influence of digitalisation. DRM provides further potentials for content creators and content owners: DRM enables control on content usage. Thus content consumption and innovation can be influenced or controlled with DRM. As the basis for DRM are digital (representation of) license, copyright and licensing can be simplified also as shown in Figure 4. This is so far ongoing development. For example in the AXMEDIS project the simplification of licensing issues is a central aspect [AXMEDIS].

Traditionally, a content creator benefits from the composition of the new content and its sale or derived contents thereof. Due to the digitalisation the content creator benefits as selection, production, and recording, marketing and promotion, manufacturing, and distribution is easier and stronger connected. DRM furthermore has potentials in copyright and licensing, consumption, and innovation. This is shown in Figure 4.

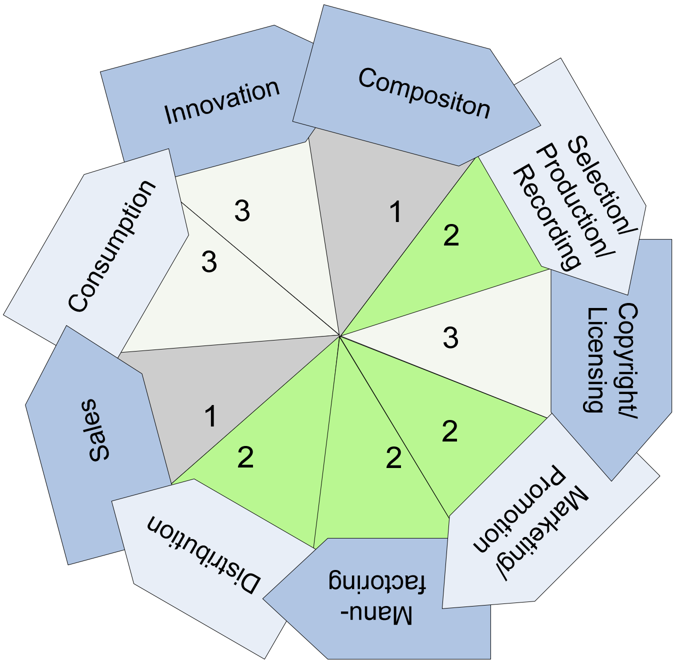

Figure 4: Influence of digitalisation and DRM on the content value chain: Traditionally, a content creator benefits from the composition of the new content and its sale or derived contents thereof (labelled with ‘1’). Due to the digitalisation the content creator benefits as selection, production, and recording, marketing and promotion, manufacturing, and distribution is easier and stronger connected (labelled with ‘2’). Due to DRM potentials can be exploited in the areas copyright and licensing, consumption and innovation (labelled with ‘3’).

4.4. Business and License models

Different business and corresponding license models can be implemented considering the potentials of digital distribution and DRM. In this section we will address the common ones. Further business and license models are described in [DT2004]. [DT2004] especially focuses on the influence of emerged P2P legal distribution of free content and illegal distribution of copyright protected content.

4.4.1. License per content and license per collection of content (paid downloads)

This business model is the digital equivalent of the commerce of physical goods. In this case DRM approximates the rights model well known from the physical world. Rosenblatt et al. identified three different problems of this business model:

- the complexity of the purchase (e.g. registration and related identification processes)
- the complexity of the technologies’ usage
- people are not used to render traditional content on computers (traditional “look & feel” is important)

While we agree on the first and the second problem, which can be addressed in the design of the solution, the third problem is already vanishing: People are used to download music from P2P-networks. Also digital audio players like Apple’s iPod are common. This might also happen to eBooks.

Considering the complexity of purchase efficient micro payment mechanisms are vital for the future of commercial online content distribution.

4.4.2. License per rendering (pay-per-view, pay-per-listen, …)

The sources for this business model stem from the physical world and are the typical model for live performances like theatres or concerts and also for cinemas and jukeboxes. Some cable-television providers have adopted this model, which is reflected in the term view-on-demand is equivalent to pay-per-view or pay-per-listen for audio-visual content.

The security of the delivered content strongly depends on the content itself. The protection level of time dependent content, e.g. a soccer match or latest news, is different from content whose value is more or less independent of time, e.g. a movie or a concert performance recording.

4.4.3. License for a specific number of rendering or for a specific time frame

In addition to the previously listed license per rendering extended models exist which allow a certain number of renderings or the rendering of content within a certain time frame. This strategy can also be applied to business documents to avoid rendering of information outside a validated time frame.

This business model is also applied to use content as promotional content. Consumers are allowed to render content for free within a certain time frame. The objective of this business model is to wake the customers' appetite for a certain product and after the free period the customer will by the content or the rights for rendering it. Interestingly the same idea is applied in a software copy protection mechanism called "Fade", which continuously removes functionality from illegal game copies after a certain period of time.

4.4.4. Distributed retail by distributing content to retailers (super distribution)

The content is distributed between more than two organisations either via peer-to-peer or via a multi-tiered distribution. Problems arise due to certain degrees of freedom (e.g. the parties involved). In the super distribution scenario DRM is very important as the probability of loosing control over content increases drastically with the number numbers of parties involved in the distribution.

Super distribution in P2P environments

P2P environments are very demanding for protection technologies. Generally, distribution via P2P networks is a form of super distribution on a special kind of infrastructure. Yet, the parties participating in the distribution do not necessary have any information of each other.

4.4.5. Subscription based services

In current subscription models the user registers via username and password. He pays a regular fee for accessing content. This regularity makes a subscription model interesting for content providers, as it ensures a certain revenue stream over time. Only few companies have succeeded in establishing subscription based online services. Different reasons can be identified:

- the Internet is known for free information
- people appreciate the "look & feel" of physical products
- information is determined by its value, timeliness, and uniqueness (values depends on a dedicated group of customers who relies on some information and is willing to pay for it and its delivery under certain circumstances, e.g. time delay)

Interestingly the Internet provides a new service to the audience of music: some users regard the Internet as a huge jukebox, which provides all different kinds of music ever recorded. Thus subscription-based services provide new possibilities. Similarly streaming audio and web radio will replace the traditional DJ who guaranteed for a certain kind of quality. Also current discussions about levies are addressing similar issues known from subscription based business models. Not to forget subscription based services of cable television. Thus DRM has to support subscription based business models.

4.4.6. License according to usage

Usage metering is well known from the physical world like gas or electricity. Yet, consumer tends to prefer a subscription-based model as monthly rates are more predictable. Nevertheless a trade-off has to be found between the customers' and the providers' risks. Furthermore this business provides an alternative to the subscription-based services as it implements the costs-by-cause principle and is more flexible than the license-per-rendering model.[20] Consumers actually pay for what the really consume. Additionally, the usage metering can be used to distribute revenues from flat rates or royalty collecting societies.

Internet service provider extended this model by providing a certain connection time or data transfer for free. Additional connection time or data transfer has to be paid for. Similarly, mobile phone service providers extended this model by providing a certain number of minutes for talking for free and selling additional minutes.

Another solution that is currently discussed is the usage of DRM systems in subscription-based services providing the possibilities to distribute fees adequately among right holders. A DRM solution can support this business model as it is capable of calculation of the metering. Additional information can be acquired, e.g. for marketing. Yet, privacy concerns have to be considered.

4.4.7. Licensing rights

Instead of distributing the content the rights can be "sold". Of course digital rights management also should address this business models as selling rights involves rights transactions among commercial organisations.

4.5. Summary

The success of a business model is decided by the customers' acceptance. Not only as DRM provides the possibility to implement no business model, e.g. based on the content consumption, is the success of DRM and business models coupled: The success of DRM is also decided by the customers' acceptance. Furthermore, a successful DRM solutions support business models and not the other way round. It doesn't matter if the business models are adopted models from the physical world, new business models, or a combination of both. Naturally, the business models must be derived from the needs of the customers, which is a well known fact from the physical world. Yet, new technologies provide possibilities for further products and services.

We also like to stress that only for a few content creators their primary income is based on the commercial distribution of there music or songs. A huge part lives from secondary source like life performances or ring tones. Thus, limiting access to content is not in the interest for these artists. As a consequence, each artist has to decide carefully the personal pros and cons before applying existing DRM technologies to her/his content.

[20] under the assumption that license-per-rendering are less convenient and more complex in handling

5. Technological Overview

In chapter 2 legal foundations of Intellectual Properties are explained. Chapter 3 describes requirements of the content creators, distributors, providers, and consumers. Chapter 4 generally explains basic business models and how DRM influences the different business models. In this section the basics of DRM are explained by giving an overview of the different technologies involved and how they interact. More details of the individual technologies are elaborated in chapter 6.

Various technologies are necessary to establish a complete DRM system. In this chapter we shortly explain the individual components of a DRM system and their relationships.

5.1. Digital rights management systems

According to object oriented software design and development a system can be characterized by use cases (e.g. [Booch1986] and [Oestereich1998]), which describe functional aspects from a user's point of view. Another important issue is the modelling of entities within a system. Therefore we summarize the discussion of the functional and information architecture by Iannella [Iannella2001].

5.1.1. Functional aspects

As DRM systems are designed for managing content[21]. Functional aspects of DRM architectures can be grouped as follows (which is shown in Figure 5):

- *IP asset creation and capture:* When content is created or captured rights are asserted. This includes rights validation, rights creation and rights workflow.

- *IP asset management:* Content is archived in an asset management system. Furthermore, meta data describing the content and the associated rights are stored. This meta data is needed for repository and trading functionality.

- *IP asset usage:* After trading the content the usage has to be managed, which includes permission management and tracking management? The permission management ensures that certain rights are honoured. The tracking management is needed e.g. to record usage if payment for each use is fixed.

[21] Thus the main purpose of DRM is tracking and controlling access to content based on the identity of the consumer

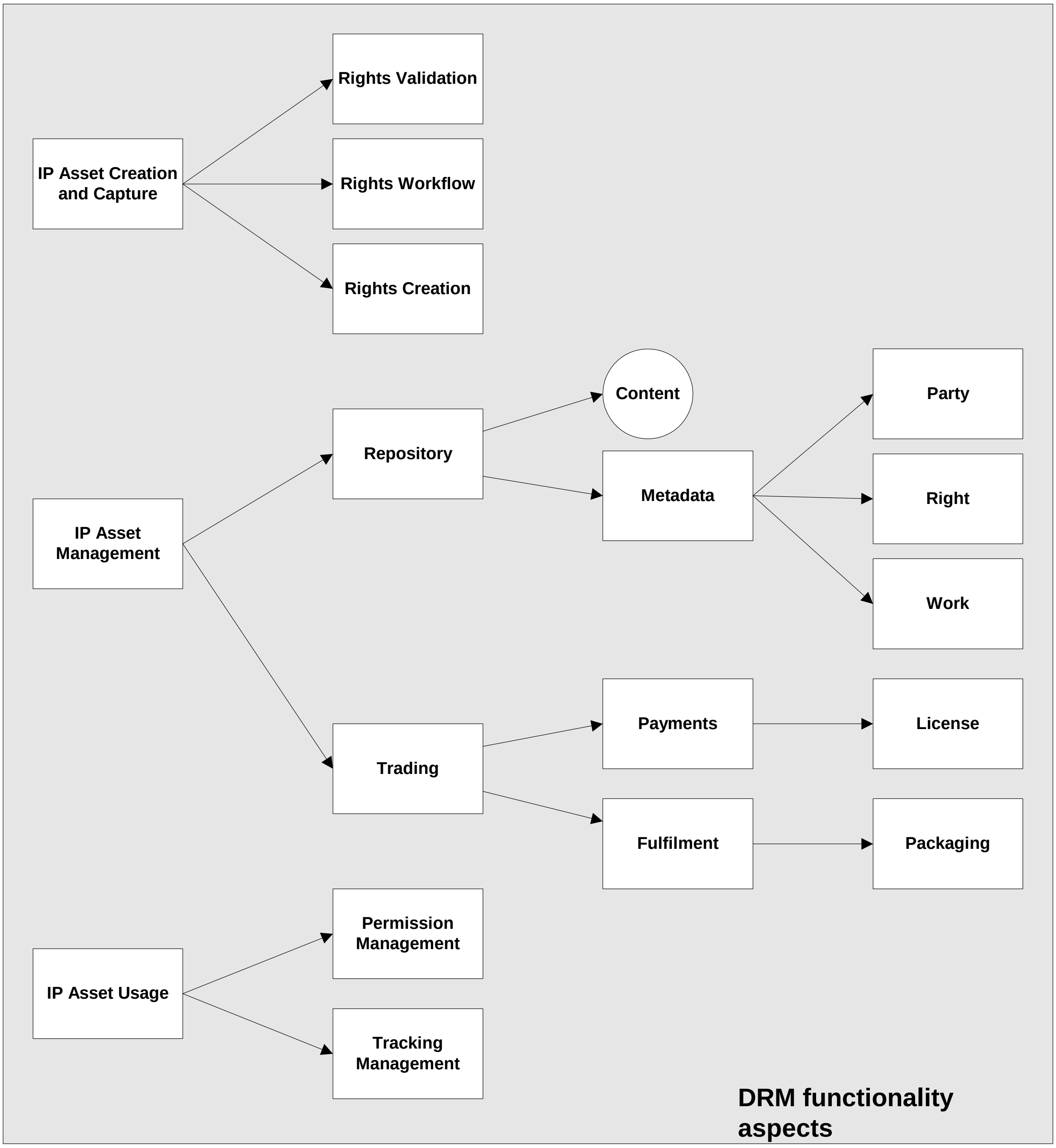

Figure 5: Functional aspects of a DRM system according to Iannella [Iannella2001]: IP asset creation and capture, IP asset management and IP asset usage are the core functionalities of each DRM system.

5.1.2. Information aspects

Information aspects of a system describe how entities are modelled within the system framework. Thus, relevant entities (and their relationships) have to be identified and modelled appropriately. Within a DRM system three identities occur:

- *Users* includes all possible types of users.
- *Content* is any type of content and its aggregations.
- *Rights* expresses the permissions, constraints, and obligations.

These are the core entities as identified in the <indecs> project, which are shown in Figure 6.

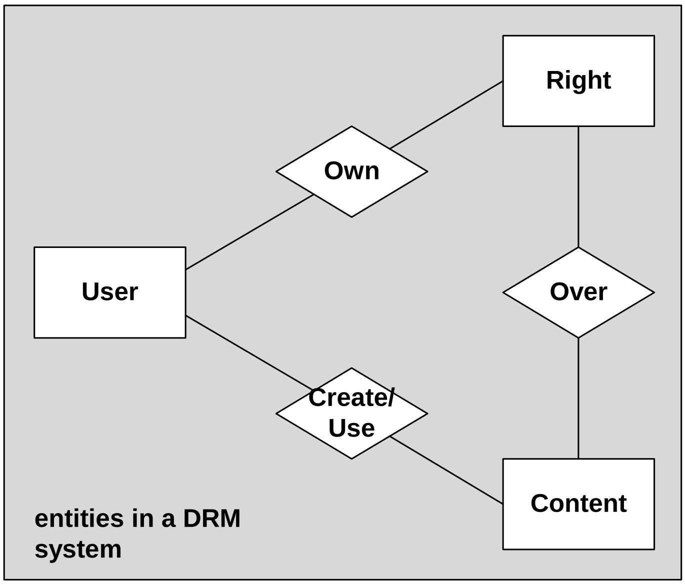

Figure 6: Entities in a DRM system according to Iannella [Iannella2001]: A DRM system manages content, users and the rights a user owns over content.

For identification of entities different standards are available, e.g.:

- URI [URI2396]
- DOI [DOI2003]
- ISTC [ISTC]

Detailed information on content identification is elaborated in chapter 5.

Users can be modelled by describing people and organizations. In vCard [vCard1996] and [vCard:1998] an independent electronic business card is defined for PDA. A vCard consists of one or more vCard objects, which are encoded in a data stream. Although this specification provides a clear-text encoding that is intended to be based on the syntax used by the MIME specification (cf. RFC 1521 [MIME1993]) it gives valuable information how to describe people. However for some DRM applications a role based modelling might be necessary.

The most important issues when modelling content is that content can be considered at various abstraction levels, it might be available in different representations and it can be a conglomerate of various different sources. E.g. a video can consist of still images, moving pictures, sounds and speech. Furthermore a work can exist in several expressions e.g. the original text or a resulting translation or a screenplay. Therefore the IFLA [IFLA1998] defined a model, which allows content to be identified at the work, expression, manifestation, and item layer (as shown in Figure 7) where for example manifestations of a book could include hard- or soft cover and item is a certain purchased item. The important issue concerning rights is that different rights holders can be recognized for each individual item.

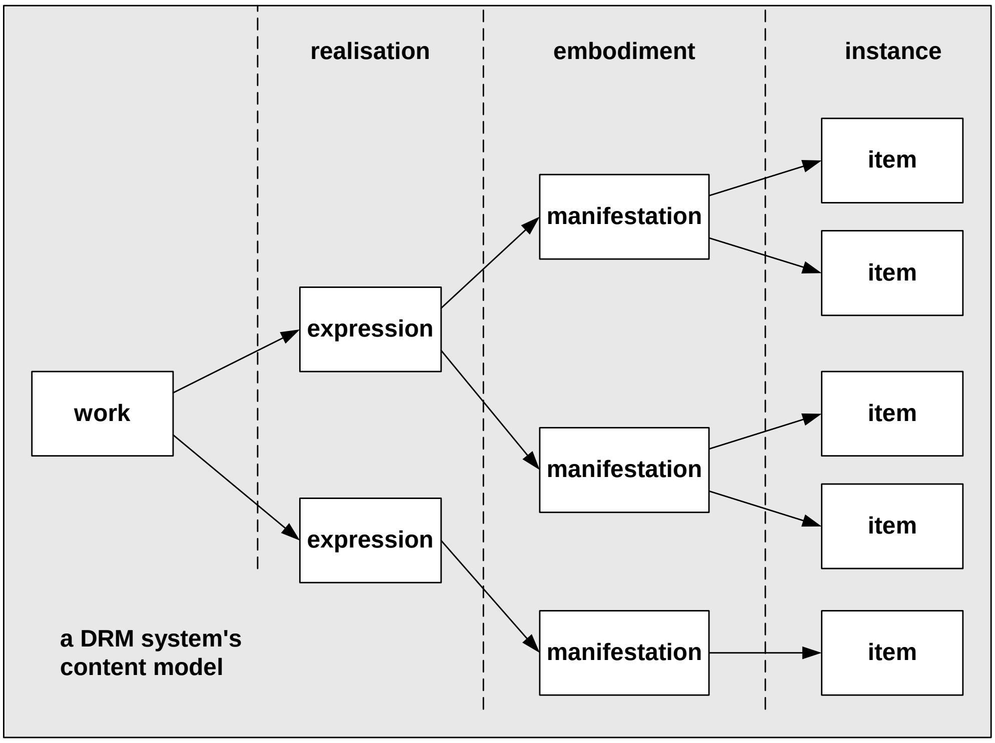

Figure 7: Example of a DRM system's content model as given by Iannella [Iannella2001]: A work can have different realizations (e.g. movie, book), different embodiment (e.g. hard or soft cover) and of course concrete instances (the individual item customers buy).

Similar to the user description, several standards exist for content description like:

- EDItEUR ONIX
- IMS Learning Resource Meta-data Information Model
- <indecs>

These models are shortly described in chapter 5.

5.2. Rights management

Typically access to content is related to usage permissions, which are expressed as rights. Digital rights management systems provide the functionality to manage rights digitally. Therefore rights have to be described as digital entities. The rights include information about allowable permissions, constraints, obligations, and other rights-related information like rights holders. They might even include information about rights transfer.

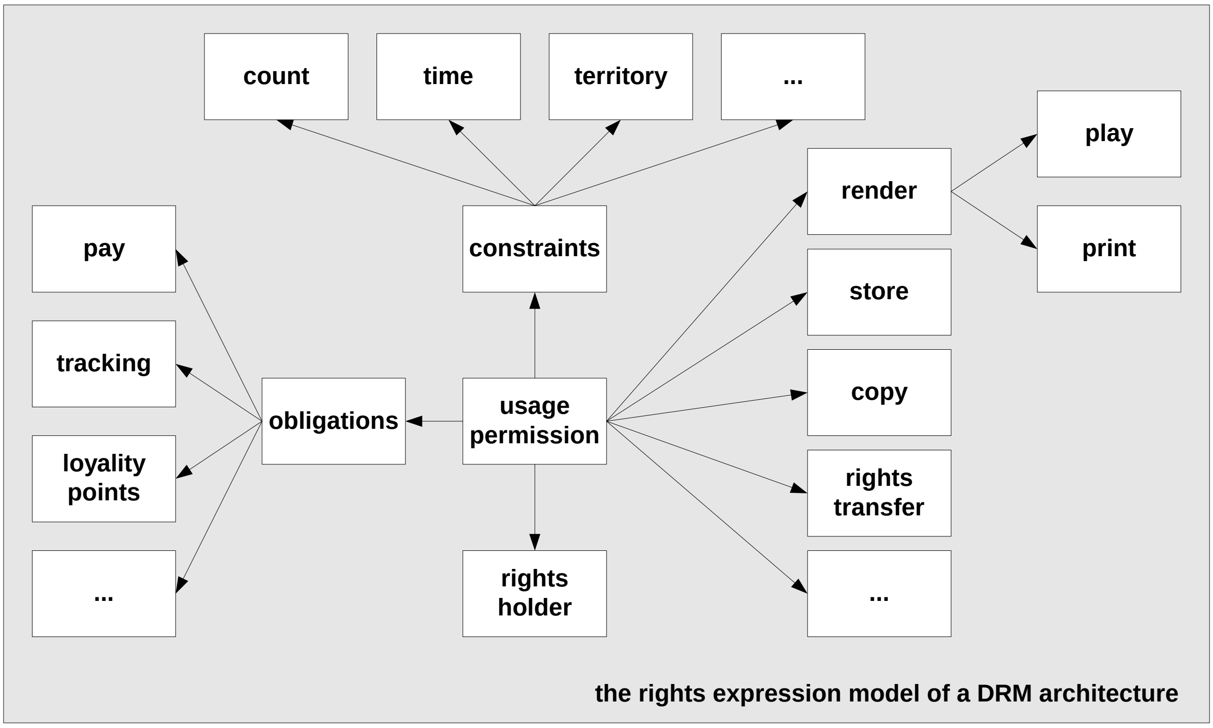

Figure 8: The rights expression model of a DRM architecture.

The rights expression model (as shown in Figure 8) can become quite complex for real world applications. Therefore different rights expression models[22] have been defined like the Open Digital Rights Language (ODRL) or the eXtensible Rights Management Language (XrML). Details about rights expression languages can be found below.

5.3. Protection technology

Whenever content with usage limitations is distributed via the Internet the content providers want to protect their content. Therefore different techniques have been developed to increase the content's security. These techniques limit the access to content as well as modification of content to ensure its integrity.

Considering protection technologies we can distinguish between:

- *active* protection, which impedes or stops illegal access
- *passive* protection, which is indirectly useable for protection of content

The following paragraphs are for introduction of the technical concepts. Details are presented below.

5.3.1. Active protection

Active protection prevents or impedes illegal access actively. This means access to content is not granted if the necessary permission is missing. Encrypting the content does this. For security reasons encryption is done with a key. As stated by Kerkhoff [Kerkhoff1883] the secrecy of the key and not of the algorithm is a necessary condition. Some existing DRM solutions keep their algorithms secret. This endangers the security of the system: Potentially security holes exist, which are well-known only in the closed community of attackers but common users are unaware of.

[22] These expression models are also called rights models. Their digital equivalents are called digital rights models and can be handled by digital devices.

Different encryption methods can be identified:

- **Symmetric encryption** schemes use the same key for encryption and decryption. There main advantage is their good performance. However key exchange is difficult.

- **Asymmetric encryption** schemes use different keys for encryption and decryption. For encrypting and decrypting a pair of keys is necessary. One of these keys is a so-called private key, which is only known to its owner. The public key is related to this private key and can be distributed freely. Data can be encrypted using the public key of an organization and decryption is only possible with the corresponding private key.[23] The main drawback of these schemes is their slow performance.

As symmetric encryption techniques suffer due to the key exchange typically keys are exchanged with asymmetric encryption schemes because of the smaller key length.

5.3.2. Passive protection

In contrast to active protection technology for passive protection do not actively protect content. A typical example for passive protection technology is watermarking: Watermarking techniques embed imperceptible qualifiers. These qualifiers do not directly protect content. But the qualifiers can be used e.g. to identify possible leaks in distribution chains. Fingerprinting or perceptual hashing techniques allow the identification of content without embedding an identifier.[24]

5.4. Summary

A DRM system is a complex software solution for the digital management of rights. If used properly it allows content providers not only to manage their content efficiently. When combining DRM systems with other software solutions, e.g. customer relationship management (CRM) tools, the benefit of a DRM system drastically increases. Yet, privacy is an issue, which has to be taken seriously. A lot of personal data can be collected in DRM systems. Solutions have to consider national laws to prevent this personal data from any illegal use.

Analysing the possible impact and success of DRM systems is generally difficult. However successful future eCommerce will be based on DRM systems with high functionality. Factors, which influence their success, are related to the unsatisfied expectations and wishes of the customers. Privacy is only one of these issues. Other user requirements include private copies, possibilities to transfer content flexibly to other devices. And another important aspect is the interoperability of DRM systems.

As soon as the possibilities of DRM solutions will be widely recognized and accepted customers and content providers will strongly benefit from DRM systems. Considering the aspect stated by Andrew Odlyzko [Odlyzko2001] and others content, customer relationship and rights management system will merge to testify that content is not king: “content is queen and service is king”.

[23] On the contrary data can be encrypted with the private key and only the corresponding public can decrypt the data. A typical application for this scenario is authentication and integrity verification.

[24] Unfortunately the term “fingerprinting” is also used in the watermarking context. There the meaning is to embed a “customer fingerprint” in the content on purchase. This is also called “transaction watermark”.

6. Basic technologies

In this chapter we describe the basic technologies need for development and implementing a DRM system. Some of the technologies are also relevant for other areas like the content identification and the linkage of content and meta data.

6.1. Content Identification, Content Description and Content Management

As already outlined below, content identification is an important aspect when linking content and meta data. This is a central aspect of libraries and archives. Thus, the some of the information, which is described here, is extended in [MN_ML].

Whenever data has to be accessed or retrieved two issues are important:

- content identification
- content description

These issues are independent of DRM. Therefore they are also described in [DE4.2.1] and [DE4.3.1]. As data have to be accessible by DRM solutions too, data and meta data have to be stored accordingly. Therefore different meta data standards have been defined to solve these issues.

6.1.1. Content Identification

Content identification should be accomplished with an open standardized mechanism. Several open standards have been created for this purpose in the digital world. But also existing content identification standards are well known in the physical world. We will explain some of both groups below.

As the data, which is exchanged via the Internet, should be readable on different systems, the “extended Markup Language” [XML] is used to describe the properties. This is not limited to identification but also includes other rights related information like the rights or the licenses.

a) ISBN

The International Standard Book Number (ISBN) is a unique machine-readable identification number, which marks any book unmistakably. This number is defined in ISO Standard 2108. and consists of ten digits. The ISBN is divided into four parts (group identifier, publisher prefix, title identifier, and check digit) of variable length:

ISBN	group identifier	publisher prefix	title identifier	check digit
ISBN	0	571	08989	5

The individual parts must be separated clearly by hyphens or spaces:

ISBN 0 571 08989 5
or
ISBN 90-70002-34-5

The number of digits in the first three parts of the ISBN (group identifier, publisher prefix, title identifier) varies. The number of digits in the group number and in the publisher prefix is determined by the quantity of titles planned to be produced by the publisher or publisher group. Fewer digits represent publishers or publisher groups with large title outputs.

The length of the ISBN is being expanded to 13-digits. The plan is to complete the standard by January 1, 2005. Implementation of the 13-digit ISBN, however, will not be mandatory until January 1, 2007. On January 1, 2007 all ISBN agencies worldwide will distribute only 13-digit ISBNs.

Detailed information is available at [ISBN2003], [ISBN2003b], and [ISBN2003c].

b) ISSN

Similarly to the ISBN, the International Standard Serial Number (ISSN) is an eight-digit number, which identifies periodical publications as such, including electronic serials. These are the Arabic numerals 0 to 9, except in the case of the last or check digit an upper case X can sometimes occur. Since ISSN are likely to be used in the same context as codes designed for other purposes, such as the ISBN or local control numbers, a distinction must be preserved in the form of presentation when written or printed. An ISSN is, therefore, preceded by these letters, and appears as two groups of four digits:

ISSN	group identifier	publisher prefix
ISSN	0317	8471

The two groups are separated by a hyphen, for example:

ISSN 0317-8471

For more information we suggest visiting the homepage of [ISSN2003].

c) ISMN

The International Standard Music Number (ISMN) consists of the letter M followed by nine digits. The letters ISMN precedes the number. The ISMN is divided into four elements (distinguishing element, publisher identifier, item identifier, and check character), the second and third of which (publisher and item identifier) are of variable length. The check character is a single digit at the end of the ISMN that provides an automatic verification of the validity of the ISMN, for example:

ISMN	distinguishing element	publisher identifier	item identifier	check character
ISMN	M	3452	4680	5

ISMN M-3452-4680-5

More detailed information can be found at the national Canadian library [ISMN2003].

d) Uniform Resource Identifiers (URI)

According to RFC 2396 [URI2396] is “a Uniform Resource Identifier (URI) is a compact string of characters for identifying an abstract or physical resource.” (cf. Wikipedia). This string indicates a name or an address and is often used to refer to an abstract or physical object. The URI syntax and semantics are derived from other WWW concepts. It was designed to meet the recommendations laid out in "Functional Recommendations for Internet Resource Locators" (RFC 1736 [IRL1736]) and "Functional Requirements for Uniform Resource Names" (RFC 1737 [URN1737]).

The abbreviation URI includes the following definitions:

- *Uniform* semantic interpretation is important when different mechanisms are used to access resources, which is important for a great flexibility in usage.
- *Resource* is a conceptual mapping to an entity or a set of entity.
- *Identifier* is a reference to a resource.

A URI can be a locator (Uniform Resource Locator - URL), a name (Uniform Resource Name - URN) or both. A typical example for a URI is the http address of the homepage of the Interactive MusicNetwork: http://www.interactivemusicnetwork.org.

One of the main design criteria was global transcribability. Therefore a strongly limited set of character is used. Considering the typical usage a URI is a string of characters must be typeable with a keyboard and must be easily remembered by people. Details about the syntax of an URI can be found in RFC 2396 [RFC2396].

e) Digital Object Identifiers (DOI)

The digital object identifier as developed by the International DOI Foundation [DOI2003]. It is an implementation of an URI and “is a system for persistent identification and interoperable exchange of intellectual property on digital networks”. A handle system is used for resolution of the identifier (the so-called DOI directory), and the <indecs> framework for the resolution of the metadata description. The syntax of the DOI is specified by a NISO standard, (ANSI/NISO Z39.84). To overcome the main drawback of URLs, which are well known to everybody using the Internet, DOIs are mapped to URLs. This mapping can be changed dynamically.

The DOI consists of two parts: the prefix and the suffix. They haven’t any length limitations and are separated by a forward slash. The prefix depends on a specific organization while the suffix identifies the entities.[25]

For example the DOI “10.1223/0810322188” can be resolved manually at http://dx.doi.org/ [DOI2003b]. It resolves to the document “Contemporary Musicians, Volume 10: Profiles of the People in Music” that is published by Thomson Gale. Here the prefix “10.1223” identifies the publisher (Thomson Gales) and while the suffix ”0810322188” corresponds to the ISBN (0-8103-2218-8). The direct advantage of the split between the prefix and the suffix is that there is a central registration of each document is not necessary. Besides the manual resolution “resolver plug-ins” for different web browsers are available at http://www.handle.net/resolver/ [DOI2003c].

f) ISO International Standard Textual Code (ISTC)

The ISO Project 21047 “is to develop an International Standard Text Code [ISTC] for the unique, international identification of individual textual works. The ISTC will provide a way for textual works to be uniquely distinguished from one another within computer applications and for the purposes of administering rights to such works.” As ISTC is focused on textual work, we will not elaborate details.

An ISTC must be allocated by the IST registration agencies. It consists of a 16 hexadecimal[26] digit identifier. The four elements represent the registration agency element; the year element; the work element and a check digit:

ageny element	year element	work element	check digit
0A9	2002	12B4A105	6

6.1.2. Content description

Within a DRM system the identification of content is more important than the description of content. However functionalities are merging and therefore we will also shortly address the issue of content description. According to Iannella [Iannella2001] content description should be based on the most appropriate metadata standard for each genre. However, any overlap with other metadata systems might result in difficulties in the implementation due to redundant information.

a) EDItEUR ONIX

The “Online Information Exchange” [ONIX] is targeting at books and was developed by EDItEUR [EDItEUR]. “ONIX for Books” includes three record types that are represented in XML. These record types are the Product record, the Main Series record, and the Subseries record. ONIX is mainly addressing the needs of publishers and online vendors.

The following Product record example is taken from [ONIXb]. One can clearly see that the content description is mixed with other information like the price:

```
<Product>
        <RecordReference>1234567890</RecordReference>
```

[25] Existing standard identifications can be incorporated into the suffix of DOI.

[26] numerals 0-9 and letters A-F

```
<NotificationType>03</NotificationType>
<ProductIdentifier>
        <ProductIDType>02</ProductIDType>
        <IDValue>0816016356</IDValue>
</ProductIdentifier>
<ProductForm>BB</ProductForm>
<Title>
        <TitleType>01</TitleType>
        <TitleText textcase = “02”>British English, A to Zed</TitleText>
</Title>
<Contributor>
        <SequenceNumber>1</SequenceNumber>
        <ContributorRole>A01</ContributorRole>
        <PersonNameInverted>Schur, Norman W</PersonNameInverted>
        <BiographicalNote>A Harvard graduate in Latin and Italian literature, Norman
        Schur attended the University of Rome and the Sorbonne before returning to the
        United States to study law at Harvard and Columbia Law Schools. Now retired
        from legal practise, Mr Schur is a fluent speaker and writer of both British and
        American English</BiographicalNote>
</Contributor>
<EditionTypeCode>REV</EditionTypeCode>
<EditionNumber>3</EditionNumber>


<Language>
        <LanguageRole>01</LanguageRole>
        <LanguageCode>eng</LanguageCode>
</Language>
<NumberOfPages>493</NumberOfPages>
<BASICMainSubject>REF008000</BASICMainSubject>
<AudienceCode>01</AudienceCode>
<OtherText>
        <TextTypeCode>01</TextTypeCode>
        <Text>BRITISH ENGLISH, A TO ZED is the thoroughly updated, revised, and
        expanded third edition of Norman Schur’s highly acclaimed transatlantic dictionary
        for English speakers. First published as BRITISH SELF-TAUGHT and then as
        ENGLISH ENGLISH, this collection of Briticisms for Americans, and Americanisms
        for the British, is a scholarly yet witty lexicon, combining definitions with
        commentary on the most frequently used and some lesser known words and
        phrases. Highly readable, it’s a snip of a book, and one that sorts out – through
        comments in American – the “Queen’s English” – confounding as it may
        seem.</Text>
</OtherText>
<OtherText>
        <TextTypeCode>08</TextTypeCode>
        <Text>Norman Schur is without doubt the outstanding authority on the similarities
        and differences between British and American English. BRITISH ENGLISH, A TO
        ZED attests not only to his expertise, but also to his undiminished powers to inform,
        amuse and entertain. – Laurence Urdang, Editor, VERBATIM, The Language
        Quarterly, Spring 1988 </Text>
</OtherText>
<Imprint>
        <ImprintName>Facts on File Publications</ImprintName>
</Imprint>
<Publisher>
        <PublishingRole>01</PublishingRole>
        <PublisherName>Facts on File Inc</PublisherName>
</Publisher>
<PublicationDate>1987</PublicationDate>
<Measure>
        <MeasureTypeCode>01</MeasureTypeCode>
        <Measurement>9.25</Measurement>
        <MeasureUnitCode>in</MeasureUnitCode>
</Measure>
<Measure>
        <MeasureTypeCode>02</MeasureTypeCode>
        <Measurement>6.25</Measurement>
        <MeasureUnitCode>in</MeasureUnitCode>
</Measure>
```

```
        <Measure>
            <MeasureTypeCode>03</MeasureTypeCode>
            <Measurement>1.2</Measurement>
            <MeasureUnitCode>in</MeasureUnitCode>
        </Measure>
        <SupplyDetail>
            <SupplierSAN>1234567</SupplierSAN>
            <AvailabilityCode>IP</AvailabilityCode>
            <Price>
                <PriceTypeCode>01</PriceTypeCode>
                <PriceAmount>35.00</PriceAmount>
            </Price>
        </SupplyDetail>
    </Product>
```

Besides price information copyright information like a “download copyright notice”, a “copyright owner”, or territorial rights can be included. It has to be mentioned that several online book traders (including Amazon) use this metadata standard.

b) IMS Learning Resource Meta-data Information Model

Learning materials are address by IMS [IMS], which identifies a subset of IEEE’s Learning Object Meta-data (LOM) meta-data elements as LOM defines a very large amount of elements. Yet, allows the extension to the LOM standard for certain purposes. Meta-data are also defined in XML to ease data exchange. Examples for IMS can be found at http://www.imsproject.org/metadata/.

c) DCMI

The “*Dublin Core Meta Data Initiative*” is also addressing the issue of interoperable online metadata standards. It consists of a simple and a qualified level. Simple Dublin comprises fifteen elements for

- describing content (description, type, source …),
- intellectual property (creator, rights …), and
- instantiations (format …).

Additional elements are included in Qualified Dublin Core (e.g. audience). The Dublin Core metadata describes one version of a resource (one-to-one principle). Also a client should be able to ignore any qualifier and use the values as if the were unqualified (dumb-down principle). Its goals include the “simplicity of creation and maintenance”, “commonly understood semantics”, “international scope”, and “extensibility”.

d) <indecs>

The “interoperability of data in eCommerce systems” [indecs] initiative was set up by international rights owners and resulted in a non-for-profit company. Its aim is to encourage metadata initiatives based on <indecs>. Its design is based on five axioms:

- “Metadata is critical”: Electronic trading strongly depends on the identification and description of content.
- “Stuff is complex”: An audiovisual content may contain numerous pieces of different intellectual property.
- “Metadata is modular”: Metadata can be considered as individual modules, which are connected in a certain way individually for each content.
- “Transactions need automation”: This is vital to reduce administrative overhead in the distribution of digital content.
- “Everything is a view”: Entities can be described and identified differently.

The <indecs> model “elaborates a logical and semantic framework for describing *entities*, their *attributes* and, where appropriate, *values* of each. Entities, attributes and values are referred to as types of metadata *elements*.” Three different views can be distinguished: percepts (“perceived by senses”), concepts ("conceived by mind"), and relations ("connections between multiple views"). Percepts are further subdivided in animate or inanimate (being or thing). Relations are subdivided in dynamic or static (event or situation). This general view is complemented by the commercial view, which is generally concerned how things are made (make, used by, do …). The legal view (make, used by, own …) finalised the view concept.

The above description explains <indecs>'s basic capabilities. It is used e.g. by [DOI] and [MUZE]. <indecs2> is a follow-on project creating a rights data dictionary.

e) EBU PMC Project P/Meta

The European Broadcasting Union is also addressing the problem of meta data exchange standards. Yet it is addressing the business-to-business media and meta data exchange. It identified several tasks (see [EBUPMeta]):

1. To establish understanding between EBU members of the media-related data interchange requirements of media commissioner/publishers (broadcasters), suppliers (producers) and consumers, using the BBC Standard Media Exchange Framework (SMEF) as the core information architecture.
2. To validate and extend the SMEF model as appropriate against members' requirements in terms of data and process, noting local synonyms (or translations), to create an "E-SMEF". This would extend the thinking to the development of a commercial process framework for exchange of media between EBU members.
3. Using E-SMEF, to apply emerging SMPTE metadata standards to the production and broadcast or distribution process, and study the feasibility of creating and adopting common exchange formats for essence and metadata.
4. To establish understanding of the use of unique identifiers in metadata e.g. the SMPTE UMID, as a crucial linkage tool between unwrapped data (metadata) and wrapped or embedded metadata in media files or streams, and develop protocols for their management between members.
5. As an aid to commercial and system interoperability between members, and in co-operation with standards bodies in related industries such as music and print publishing, to collate all relevant unique identifier schemes and map them against each other. This could be in collaboration with the EU INDECS project and the DOI Foundation, and extend to cover their data models too.

Their final draft is available at their web site.

f) SMEF

The "*Standard Media Exchange Format*" [SMEF] was defined by the BBC [BBC] for media asset management. It goes beyond the business areas and also addresses the delivery to the home. Its data model (SMEF_DM) is considered as a integration key information system that will evolve over time to cover more of BBC's business. SMEF-DM is available at BBC's website.

g) MPEG-4

MPEG-4 defines a stream management framework. This framework includes a rudimentary representation of metadata for the "description, identification and logical dependencies of the elementary streams" [MPEG4]. Thus the object descriptor protocol addresses the fact that content may have different sources. MPEG-4 includes this object content information as well as intellectual property management and protection.

h) MPEG-7

In contrast to MPEG-4, which is focusing on coding of audio-visual content, MPEG-7 addresses the describing of and searching for content. "MPEG-7, formally named "*Multimedia Content Description Interface*", is a standard for describing the multimedia content data that supports some degree of interpretation of the information's meaning, which can be passed onto, or accessed by, a device or a computer code." [MPEG7]

i) Others

Several other meta data standards exist. For a more extensive description of meta data standards we suggest further literature like the “Meta Data Reference Guide” [MDRG]. Interestingly for CDs users maintain several metadata databases. These communities collect information about music and make it publicly available. One of these community support meta data databases is MusicBrainz [MusicBrainz].

Also the Open Archives Initiative (OAI) “develops and promotes interoperability standards that aim to facilitate the efficient dissemination of content.” [OAI]. OAI developed the “OAI Protocol for Metadata Harvesting” [OAIPMH], which defines a mechanism for harvesting XML-formatted metadata from repositories. The Sheet Music Consortium [SMC] uses this OAI protocol for metadata harvesting with the aim of building an open collection of digitized sheet music.

6.2. Rights Management and Rights Description Languages

As DRM is the digital management of rights they have to be represented in a digital format to be digital manageable. These digital representations must consider several aspects as also described in [Rosenblatt2002]:

- content rights transactions: traditional business models
- components of rights models: types of rights and their attributes
- fundamental rights: render rights (print, view, play), transport rights (copy, move, loan), derivative work rights (extract, edit, embed)
- rights attributes (considerations, extends, types of users)

A general problem of DRM systems is the fact that they do not (yet) qualitatively distinguish between the different kinds of usage. For example copying for personal purpose and copying for friends or even unknown persons is represented as the same action within a DRM system. This is what Rosenblatt et al. expressed as “they [digital rights models] don’t do a great job of modelling the actual uses of content.” Maybe this is one of the necessary improvements of DRM systems in the future.

Licenses can have a strongly varying complexity reflecting everything from simple to complex rights situations. Therefore the language used for the description of rights should be able to model even very complex situations, which can appear easily when dealing with digital content (e.g. audio-visual material).

6.2.1. Rights description languages

Not only meta data description are stored in the XML format. Several rights description languages are based on XML too. An overview of different XML based rights description languages can be found at [CoverPages]. In this section we will shortly describe properties of some rights description languages.

a) DPRL

The “Digital Property Rights Language” [DPRL] was developed by Mark Stefik at Xerox Palo Alto. Xerox patented DPRL and a separate business unit attempted to commercialise it. This business unit became the separate company ContentGuard [ContentGuard]. ContentGuard modified DPRL and renamed it in XrML (cf. below). Besides supporting eCommerce DPRL main focus is to support the specification access and usage right or controls.

"DPRL is used to specify fees, terms and conditions governing the use of digital content. DPRL is extremely flexible and supports multiple business models and rights protection policies, giving publishers the flexibility they need for their current and future businesses. DPRL supports multiple pricing models: subscription-based, outright purchase, purchase of individual rights (view, print, copy, edit, etc.), metered usage, time-based usage, and membership pricing. DPRL defines syntax for specifying rights for a digital document. Rights such as 'play,' 'print,' 'copy,' 'edit,' etc. can be grouped into named 'rights groups'." [DPRL2001]

"The design goals for DPRL are: (1) To describe rights, fees, and conditions appropriate for the commerce models that are important to publishers and consumers in digital publishing. (2) To provide standard terms for usage rights specifications that have useful, concise and easily understandable meanings. (3) To provide operational definitions of specifications for vendors of trusted systems that distribute or render digital works, so that the compliance of systems can be tested and evaluated. (4) To provide a basis of extensibility to new language features in a manner that does not unduly compromise the other goals."

The following example was taken from [DPRL98]. The XML-based description is also readable for humans with bigger effort (depending on the file size). This requires some assumptions on the system, which interprets the rights, as the licensing information must not be modified. Therefore a "trusted" system is assumed, which handles the right information and the related content accordingly. The XML documents describe works and related rights issues like *owner* or *rights-groups*. The rights are defined on the content and the operation like *play*, *copy*, or *loan*.

```
<work>
    <description>
        <title>Moby Dog</title>
        <author>John Beagle</author>
    </description>
    <owner>Murphy-Books-ID12345-zxcvoiuyr</owner>
    <rights-group>
        <rights-group-name>Consumer</rights-group-name>
        <rights-list>
            <copy>
                <next-copy-rights>
                    <delete>Distributor</delete>
                    <access>
                        <security-class>3</security-class>
                    </access>
                    <fee>
                        <per-use>10</per-use>
                        <to>Account-ID-678-qwerqeruyt</to>
                    </fee>
                </next-copy-rights>
            </copy>
            <play>
                <fee>
                    <metered>
                        <rate>0.05</rate>
                        <per>1:0:0</per>
                        <to>Account-ID-678-qwerqeruyt</to>
                    </metered>
                </fee>
            </play>
            <delete></delete>
            <transfer>
            </transfer>
            <loan>
                <next-copy-rights>
                    <delete>Distributor</delete>
                    <remaining-rights>Distributor</remaining-rights>
                    <access>
                        <security-class>3</security-class>
                    </access>
                </next-copy-rights>
            </loan>
        </rights-list>
    </rights-group>
    <rights-group>
        <rights-group-name>Distributor</rights-group-name>
        <rights-list>
          :
          :
         </rights-list>
    </rights-group>
```

```
</work>
```

A tutorial on DPRL is available at [DPRL].

b) XrML

The “eXtensible Rights Management Language” [XrML] was derived from DPRL. Obviously the description of rights and licenses with XML is expressed in its name. Similarly to DPRL a XML document describes a work and related rights. XrML 2.0 is extensible to address specific needs and can include other elements like resource-level metadata standards (e.g. ONIX or RDF). Rights expressions are authenticated (XML Signature) and protected (XML Encryption). Its flexibility is an advantage as it supports different business models. The following paragraph summarizes some aspects from the XrML Specification [XRMLSpec] freely available at [XrML] (see also [XrMLFAQ]).

A XrML document contains a license. This license contains a set of grants. These grants convey (respectively contains information about) certain principal rights to certain resources under certain conditions. The rights specify a class of actions that are allowed to be performed on the associated resource. These actions include rendering, transportation, and derivative work but also file (backup, verify, directory, …) or software management (install, uninstall). Conditions can be attached to the rights including access limitations, time limitations, transaction limitations, and territory limitations. Furthermore XrML is also able to address issues of watermarking and tracking. A simple example taken from [XrMLSpec] show how the license files for printing a specific book might look like.

```
<license>
    <grant>
        <keyHolder>
            <info>
                <dsig:KeyValue>
                    <dsig:RSAKeyValue>
                        <dsig:Modulus>Fa7wo6NYf...</dsig:Modulus>
                        <dsig:Exponent>AQABAA==</dsig:Exponent>
                    </dsig:RSAKeyValue>
                </dsig:KeyValue>
            </info>
        </keyHolder>
        <cx:digitalWork>
        <cx:locator>
            <nonSecureIndirect URI="http://www.contentguard.com/sampleBook.spd"/>
        </cx:locator>
        </cx:digitalWork>
    </grant>
</license>
```

XrML is used in several commercially available products including Microsoft’s Unified solution, which is based on XrML. But more important are two other facts: First, MPEG-21’s Right Expression Language (REL) is based on XrML. Regarding MPEG-21, XrML had to beat two further competitors: the Open Digital Rights Language ODRL and Real Networks’ extensible Media Commerce Language (XMCL). ContentGuard also submitted the eXtensible rights Markup Language Version 2.0 to the the Right Language TC [OASISRLTC] of OASIS [OASIS].

c) ODRL

The “*Open Digital Rights Language*” [ODRL] also allows the expression of terms and conditions related to the usage of digital content. It is also independent of the content type and is also extensible. In contrast to XrML ODRL is an open free standard.

The ODRL rights information considers several core entities, including assets, rights, parties offers and agreements. Assets include any type of content that can be uniquely identified. The rights modelling considers permission, constraints, requirements, and conditions. Parties include rights holder, end users, and roles.

The ODRL specification was submitted to W3C. Before, XMCL (RealNetworks) was merged into ODRL. ODRL is the officially accepted standards rights expression language of the Open Mobile Alliance (OMA), which is again shows its role as competitor to XrML and Microsoft.

d) XMCL

RealNetworks submitted the “eXtensible Media Commerce Language” to MPEG-21 as a competitor to XrML. But shortly before the MPEG-21 meeting took place RealNetworks dropped XMCL. XMCL was merged with ODRL.

e) MPEG-21

Although MPEG-7 is more focused on meta data description but contains IPMP (Intellectual Property Management and Protection) meta data, MPEG-4 was the beginning the integration of DRM related functionality. In MPEG-4 interfaces (“hooks”) are defined. Based on MPEG-4, MPEG-21 models digital items and the interactions of users with these items (Digital Items Declaration, Digital Item Identification and Description, Content Handling and Usage, IPMP, Terminals and Networks, Content Representation, and Event Reporting). It introduces a Rights Data Dictionary and a Rights Expression Language (XrML). A detailed introduction can be found at [MPEG21].

6.2.2. Rights processing

Expressing the rights is only the first step. Ideally the rights are processed automatically whenever content is created, derived, or exchange. This cannot be achieved yet as different terminology – especially when dealing with multinational content – and even different legal foundations complicate an automation process. Thus a rights ontology or thesaurus is inevitable.

6.2.3. Current status of REL standardisation

As described before, MPEG chose XrML for the MPEG REL. Nevertheless, OMA was in favour of ODRL. This competition between XrML and OMA is very interesting, as XrML is patented and ODRL is royalty-free. Nevertheless, “ContentGuard asserts that because its patents cover DRM implementations based on any rights language, even ODRL implementations should be subject to patent licensing from ContentGuard. The OMA tacitly disagreed with ContentGuard's assessment when it chose ODRL; the issue has yet to be tested, in the courts or otherwise.” [DRM2003].

6.3. Encryption

Whenever data are transmitted over an insecure channel, which indeed is the Internet, the only possible protection mechanism to guarantee confidentiality is encryption.[27] The methods used for encryption can be attacked. But attacks are not limited to the encryption algorithm itself. Also attacks are possible against keys or protocols. In this chapter we will address some general aspects of encryption to allow a basic understanding of distribution systems’ requirements. Further details on encryption can be found at [Menezes96], [Schneier96], or [Wobst00]. Several brief introductions are available, e.g. in [Wobst03].

6.3.1. Cryptography

Cryptography is the art of encryption and is several thousand years old. Encryption transforms the content by using an encryption algorithm or a cipher. Retransformation of the original message (or plain text) from the encrypted form (or cipher text) is known as decryption. To prevent others from reading the cipher text the method could kept secret or the algorithm uses a secret to determine the transformation. Kerckhoff [Kerckhoff1883] already formulated in 1883 that security by obscurity is not possible: Keeping the encryption method secret doesn't increase the security of the method. The security of an algorithm therefore must not be based on its secrecy but on the usage of a key.

Different methods exist:

[27] Besides confidentiality other relevant aspects might be authentication, integrity, or copyright protection, which has to be addressed using different techniques.

- **symmetric** encryption methods
- **asymmetric** encryption methods

6.3.2. Symmetric encryption methods

Whenever data is exchanged communication partners agree on a common key for the encryption of the data as shown in figure Figure 9. As the same key is used for encryption and decryption by symmetric encryption methods (see also Table 1) everybody who has access to the key can decrypt encrypted data.

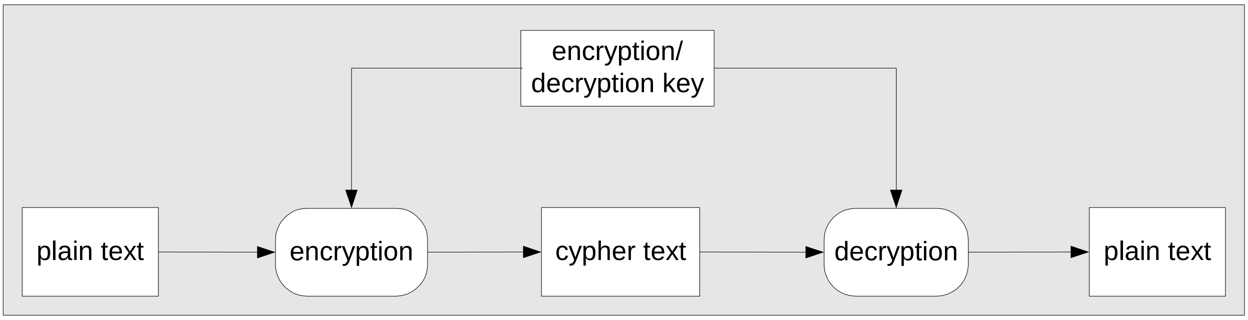

Figure 9: Symmetric encryption methods use the same key for encryption and decryption. The key determines the transformation for the plain text to the cipher text. Thus everybody who has knowledge about the secret key can decrypt the cipher texts, which have been encrypted with this key.

The *substitution algorithm* is probably the most famous symmetric encryption method: By using a table every character is replaced by another one. However, statistical attacks considering the distribution of digits in natural text can be used to attack this simple method.

A similar method is based on the *Vignere method*: Instead of using a fixed table a password determines the mapping. Each letter determines a certain "distance". With this defined mapping the password values are added to the initial certain "distance" data. The recipient can use the same key to decrypt the received data.

One severe attack is the knowledge of an example of encrypted and the decrypted data, that allows the calculation of the mapping and therefore the decryption of other encrypted messages. But also statistical attacks can be applied. Of course the security of this system depends on the length of the password or key. If the key has the same length as the message maximum security is achieved. In this case the key is also called a one-time pad.

There are two main types of symmetric encryption algorithms that differ in the size of the data the cipher works on[28]:

- **Block ciphers** process a number of bits simultaneously.
- **Stream ciphers** process a single bit a time.

a) Block ciphers

Modern methods partition the message into blocks of a certain size. For each of these blocks a secret message with the same size is generated. To minimize the potential success of attacks the transformation from the message to the secret message considers the plain text and the key. Typically this transformation is repeated with a different key[29]. Typical block based algorithms are DES, 3DES, IDEA, AES, Blowfish, Twofish and RC6.

[28] Yet this distinction is somewhat hazy as block ciphers can be used as stream ciphers and vice versa.

[29] Different keys are used in different rounds. Therefore the keys are also called "roundkeys" and are generated from the general key.

- **DES** was originally developed by IBM, modified by NASA and NIST and adopted as a federal standard. DES is a block cipher with the block size of 64 bits. The length of the key is also 64 bits, but as eight bits are used for parity the effective key length is 56 bits. Encryption: The plaintext block is split in two bitstrings with the lengths of 32 bits. One encryption process consists of 16 rounds. In each round a encryption function F is applied to one half with a certain independent round key of 48 bits length. For each round the independent round key is generated from the 56 bit original key. The result is XOR with the other half. The two halves are swapped and the process is repeated. In the last round there is no swap. Decryption is similar to the encryption process. However, the input subkey are applied in reverse order.

- **3DES**: Nowadays a simple DES encryption is no longer secure. Thus 1999 NIST defined 3DES, which consecutively applies three stages of DES. The effective key length of 3DES is 168 bits.

- **AES** replaced DES in 2001 and is a modified Rijndael encryption algorithm (with fixed block size). AES has a symmetric structure and can also be used on smart cards. Several rounds operate on the blocks. Each round includes:

  - **ByteSub:** Individual bytes are transformed with a high non-linear function.
  - **ShiftRow:** Rows are shifted over four different offsets.
  - **MixColumn:** Bytes in columns are linearly combined.
  - **Round key addition** makes round function key dependent.

  As this new standard has been specified most systems will likely switch to that standard soon.

- **IDEA** is a block cipher for a block size of 64 bits and was developed at the ETH-Zurich in 1992. Its key length is 128 bit. The algorithm is base on mixing operations from different algebraic groups (XOR, addition modulo 2^{16} and multiplication modulo $2^{16}+1$). The same algorithm is applied for encryption and decryption. The mixing operations operate on 16bit subblocks, which was due to the fact that the operations should be also efficient on 16bit processors. It is faster than DES and considered as more secure.

- **Blowfish** was designed by Bruce Schneier with the aim to have a not patented encryption algorithm. It can handle a variable key length and its block size is 64 bits. The first part of the algorithm expansions the input key length by creating several subkeys. In the second part of the algorithm the data is encrypted by using a 16-round Feistel network[30].

- **Twofish** is a 128 bits block cipher. It accepts key lengths up to 256 bits. Twofish originated from an attempt to improve Blowfish. As Blowfish it is also not patented. It was a finalist in NIST's call for the AES algorithm.

- **RC6** was also among the finalists in NIST's call. It is a rather simple algorithms and the knowledge gained from RC5's analyses work incorporated. However, its performance is weaker than the Rijndael algorithm on certain hardware, e.g. including 8 bit and 16 bit processors. The algorithm is patented by RSA Security Inc.

b) Stream ciphers

Stream based encryption methods create a pseudo random bitstream by using a secret key. This bitstream is combined with the plain text with an XOR operation to create the secret message. The recipient repeats the same opertations to recover the plain text. One of the most important issues of this methods is the randomness of the bitstream. This method is used e.g. by A5 or RC4, which is used by the SSL-protocol. Block based methods can be also used as a stream based method.

[30] A Feistel network is key dependent mapping from an input string to its permutated output string.

- **RC4** was developed in 1987 by Ronald Rivest and was initially kept secret. It was designed for bulk encryption and is faster than most other symmetric functions such as DES. RC4 uses a variable length key that is used to generate a pseudo-random stream. This pseudo-random stream is XOR-ed with the plaintext.

name	*type*	*key length*	*speed*	*security*	*application*	*comments*
One-Time Pad	stream	plain text length	high	perfect	exceptions	the only proofable secure algorithm
DES	block	56 bit	HW: high SW: low	special HW attacks	common	key length is weak point
3DES	block	112 bit	HW: high SW: low	no attack known	common	-
IDEA	block	128 bit	Faster than DES	very high	common	Patented
RC5	block	variable	SW: high	Practically secure	some products	US patent, improved: RC5a
RC6	block	variable	SW: high	no attack known	some products	improved version of RC5
Blowfish	block	variable	SW: high	no attack known	common, e.g. Open Source	Free
Twofish	block	variable	HW/SW: fast	more secure than Blowfish	-	Free
AES (Rijndael)	block	128-256 bit	HW/SW: very fast	Theoretical weaknesses	common	DES's successor

Table 1: Symmetric encryption algorithms

6.3.3. Asymmetric encryption methods

The general problem of the symmetric schemes is the exchange of secret keys. As the secret keys has to remain secret transmission of keys in plain text is not possible. This problem is addressed by public-key or asymmetric encryption methods.

Asymmetric encryption methods use two keys (as shown in Table 2):

1. The public key is for the encryption of data. This key can be distributed freely.
2. The private key is used for the decryption of the data.

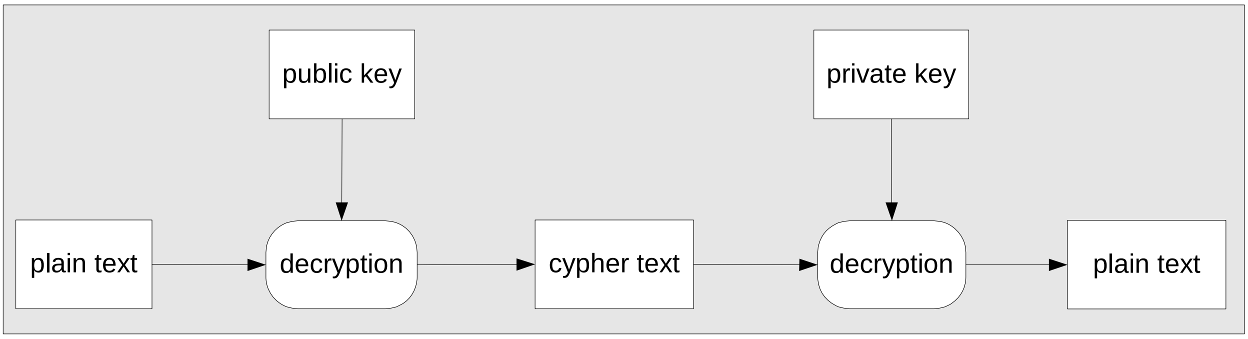

Figure 10: In contrast to the symmetric encryption algorithm the asymmetric encryption methods use different keys for encryption and decryption. The public key can be accessed by everybody interested in encrypting a message for a certain receiver. The private key is kept secret.

Thus, no keys have to be exchanged. One can even think of a "telephone book" that publishes the emails addresses and the corresponding public keys. However, public key encryption is computationally expensive.

The existing solutions for the asymmetric methods are based on the computation of mathematical calculations which are extremely difficult for very large numbers.

- **ElGamal**
- **RSA**
- **Elliptic Curve Ciphers** (ECC) probably will replace RSA in the future.

name	*key length*	*speed*	*security*	*application*	*comments*
RSA	mainly 1024 or 2048 bit	very low	till now: secure	most important method	based on factorisation
ElGamal	mainly 1024 or 2048 bit	very low	till now: secure	Broadly used	based on discrete logarithm
Diffie-Hellmann	none	very low	till now: secure	broadly used (IPsec, SSH)	like ElGamal but only for interactions

Table 2: Asymmetric encryption algorithms

6.3.4. Key length

Generally, longer key lengths provide higher security. The comparison of different ciphers based on their key lengths is nevertheless meaning less: The security is influenced by the design of the ciphers. One example is public key algorithms' key length: They require much longer key lengths than symmetric algorithms.

6.3.5. Cryptoanalysis

Cryptoanalysis deals with the analysis of cryptographic methods. For example, the "brute force" attack is a straight forward attack that calculates and verifies all possible keys. Of course this can be very time-consuming but for certain encryption algorithms hardware was developed to speed up this task and even distributed calculations that use a huge amount of computers connected via the Internet are performed. A method can be considered as secure when the most effective attack is the "brute force" attack. However, cryptoanalysis is not limited to the decryption of the secret message: collecting any kind of information, which provides more information about the secret message, represents an attack.

6.3.6. Dangers and attacks

The security of all asymmetric encryption methods depends on the complexity of the computation of mathematical problems. Therefore a "tricky" calculation or quantum computers might endanger the security of all asymmetric encryption methods in the future.

Besides this potential risk modern encryption algorithms don't have any potential security leaks that can be exploited. Therefore attackers exploit other leaks like the above mentioned randomness of a PRN generator. Other possible leaks are cryptographic protocols, chosen keys, short pass phrases, etc. Even more sophisticated attacks are applicable like the ones based on the power consumption or the time delay of cryptographic coprocessors.

6.3.7. One-way encryption

Encryption with one-way algorithms[31] cannot be reversed. Typical applications are scenarios, where the plain text must not be recovered and include the storage of passwords. One of those one-way hash algorithms is the secure hashing algorithm (SHA) that creates a 160 bit hash value. As these one-way

[31] These algorithms are also known as one-way hash algorithms.

encryption functions typically base their calculations on a password they can be used to sign data with a digital signature.

Depending on the application – for example like for authentication/verification of digital content – the security of one-way encryption is very significant. Recent attacks on MD5 [MD5Attack] or on SHA-1 [SHA1Attack] show, that collisions are possible. MD5 and SHA-1 can no longer be considered secure.

6.3.8. Applications in DRM systems

Encryption technologies are primarily used to secure the communication between different parties and the storage at the parties' storage media. While this makes generally sense in business environments, concerns has to be raised to the encrypted storage of content at the consumers' side. As consumers access the encrypted data an unencrypted version must be temporarily available in the memory of the computer. Consumers capable of handling debugging software are able to access this decrypted content as long as "trusted solutions" are not available (cf. below).

Besides the secure communication and storage of content encryption technology is used for further applications:

- verifying content based on digests
- verifying identities based on certificates
- verifying identities and content based on signatures

6.4. Watermarking

Besides the active protection technologies like the encryption described in the previous chapter passive protection technologies provide further possibilities. They address the identification of content or the identification of content owners. Thus they do not prevent copying per-se. However, these mechanisms can be used for the detection of IPR infringements as shown in the latest movie piracy case: Caridi distributed several Oscar screeners - among them were „The Last Samurai", „Shattered Glass", and „In America" – illegally, which were further distributed on the Internet in illegal file-sharing networks [ScreenersCBS, ScreenersFOX]. This chapter describes digital watermarking techniques, which are techniques that actually mark content. The intention of embedded marks depends on the application. For the application of content protection it is typically an identifier for the content owner. In other applications, e.g. for transaction tracing, it might be a customer identifier.

6.4.1. General principle

Digital Watermarking embed data in digital media either perceptibly or imperceptibly. Perceptible watermarking techniques influence the quality of the content. Additionally, as they are visible, a successful removal can be easily verified by an attacker. (A very important attack is the so-called "in-painting attack" [Huang2004]). Therefore we will limit this discussion on imperceptible watermarking techniques.[32]

Imperceptible digital watermarking methods and steganographical methods embed information in a carrier. This carrier can be abstracted as an information carrier. Therefore theories well-known in communications engineering can be applied to this type of communication. Steganography's most important requirement is that the communication remains undiscovered. In contrast to this information about the communication can be available for watermark techniques. This knowledge leads to increased requirements on the robustness and the security of the communication respective of the embedded message. Thus, a good watermarking system maximizes robustness for a constraint perceived quality degradation.

The application scenario determines the content of the watermark. For the protection of intellectual property typically information about the rights holder is embedded. Although information about the content itself or a link to this meta data can be embedded, which supports the identification of content.

[32] More or less a perceptible watermark in music scores already exists: the copyright information.

Other scenarios embed information relevant for authentication[33] or even information related to marketing and PR.[34]

6.4.2. Characteristics and requirements

The general principle of watermarking methods can be compared with the symmetrical encryption. Both methods require the same key for encoding and decoding the information. A watermarking system consists of two sub-systems: the watermark writer (encoder) and the watermark reader (decoder).

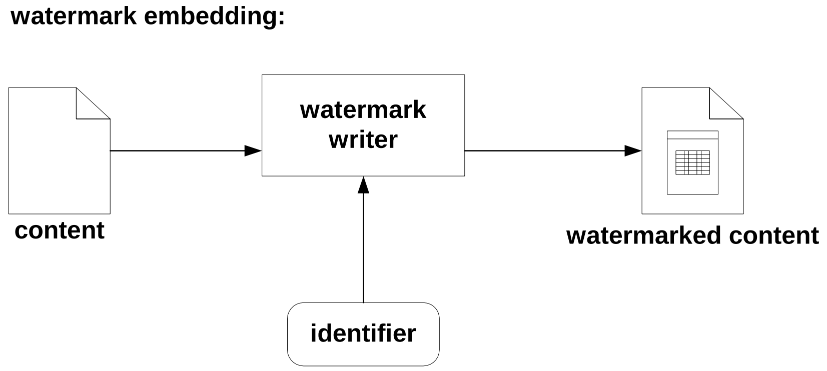

Figure 11: During the watermarking embedding process the watermarking message is interwoven with the original content.

The embedding process is shown in Figure 11: Watermarking technologies most important characteristic is the active embedding of a watermark message (the identifier) in the content. Thus, the content is modified (imperceptibly). This is the message, which is read during the retrieval process as shown in Figure 12. This has severe implications to the protection scenario as content that is already distributed has to be considered carefully.

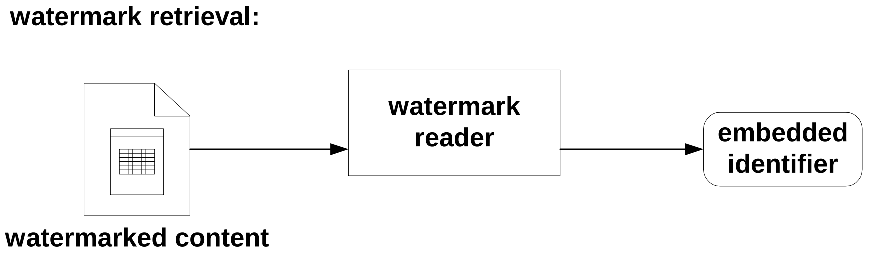

Figure 12: During the retrieval process the embedded watermark message is restored.

The retrieval processes (as shown in Figure 12) differ in the detection itself and the number of input parameters. Blind[35] detection schemes require only the marked content and the detection key for the detection. In contrast to the blind detection schemes the non-blind[36] methods require in addition to the previous parameters the original and sometimes the embedded watermark message. Semi-blind methods require in addition to the blind detection schemes the watermark message as a retrieval parameter.

Non-blind methods are practically only interested for a very limited number of application scenarios due to the necessary input of the original. In the typical application scenarios – like broadcast monitoring or the automatic identification of the copyright owner – the original is either not known or not immediately accessible.

[33] Typically a soft-hash or perceptual hash value is embedded, which is another term for fingerprinting.

[34] A watermark in an image or audio can be used to start a plug-in in a web browser for automatic linking the content to a certain website.

[35] Blind watermarking schemes are also called “public” watermarking schemes.

[36] These are also called “private” watermarking schemes.

As already described before, watermarking techniques have additional requirements on the robustness of the embedded watermark and the security of the watermarking system. General requirements on a watermarking technique are:

- The *quality* can be considered as the most important criteria. In general the embedding of a message into the content should not affect the perceived quality of the content. As perceived quality always depends on the media type watermarking techniques have to be developed or adapted to individual media types.

- The *robustness* is defined by the types and numbers of operations (and their parameters) applied to the watermarked content, which can be survived by the watermark message. From a watermark developer's and user's view these processing operations are called attacks. Depending on the intention of the operations they can be distinguished between intentional and unintentional attacks. Although an attacker has numerous attack operations available, their combination and their parameters can not be chosen arbitrarily as the result also has to fulfill a certain quality requirement. The operations a watermarking scheme should be robust against are defined by the individual application scenario. For the identification of content and protection of IPR robustness can be considered as the second most important criteria.

- The *capacity* is the amount of information, which can be embedded in the content. It is the third most important criteria. Due to the mutual dependencies between quality, robustness and capacity, a certain quality level is defined (according to the application scenario) and the robustness is chosen dependent on the deserved quality. Capacity is finally defined by quality and robustness.

- The *complexity* of an algorithm is important for certain application scenarios where real time embedding or detection is important.

- The *security* of a watermarking scheme does not only depend on the robustness but also on other issues like the message embedded. Also its implementation and integration into the overall system cannot be neglected.

We do not go into details of the individual technologies. General information on watermarking techniques can be found in [Katzenbeisser]. Cox et al. [Cox2002] provide a detailed technical inside on watermarking schemes for images. A application oriented introduction and detailed information about requirements and application scenarios can be found in [Arnold2003].

6.4.3. Limitations

Although watermarking schemes have some obvious advantages for certain application scenarios as they can embed arbitrary information direct into the content. Also they can survive processing and media conversion, which makes them very suitable for embedding meta data information. But compression techniques can be regarded as competitors as they eliminate imperceptible information thus future developments might have strong effects on the embedded content.

For the usage together within IPR protection scenarios they have some drawbacks. For example the robustness of watermarking schemes might not be sufficient and an attacker can be able to remove – or maybe copy – a watermark message. However, he cannot be 100% secure about the success of his attack. Additionally content has to be watermarked before retrieving a watermark message is possible. Whenever data is already distributed, which is the case for all current media types, a redistribution of watermarked data is necessary. Surely this can be done if new media formats like SACD or DVD-Audio are established.

As watermarking methods always have to respect the perceived quality the have to be developed or adapted for each individual media type. Yet for some media types (e.g. text or music scores) a watermark embedding is difficult.

Currently objective tests and performance analysis of existing watermarking techniques available are only addressing a limited scope. These benchmarking suites like [stirmark] or [Certimark] do not fully consider practical requirements. Here standardized application scenarios defining requirements would be advantageous. Another limitation is the missing standardisation of the embedded information, which can be solved easily.

6.4.4. Applications in DRM systems

Although watermarking techniques must be developed for individual media types a broad range of watermarking algorithms are available for various media types including, audio, images, video, geometry data, text, music scores, etc. Several requirements can be addressed by integrating watermarking techniques into DRM solutions (see also [Rosenblatt2002]):

- *Source identification* can be achieved by imperceptible watermarking techniques, which do not affect the perceived quality. The information embedded links to the content owner or to a rights owner.

- *Tracking and tracing* by embedding so-called transaction watermarks, which is information about people involved in transactions, might allow the detection of leaks within the distribution chain.

- *Meta data* labelling is probably the most interesting application of watermarking. The watermark message stores a link to a database containing meta data information.

From a security point of view we consider applications involving encrypted watermarks and encrypted files with watermarks critically if they are used for access control in end user devices. Yet, Rosenblatt et al. concludes “a scheme that incorporated both encryption and watermarking is not foolproof, but (all else being equal) it’s the best DRM scheme available” [Rosenblatt2002].

6.5. *Fingerprinting*

In contrast to watermarking techniques, which modify content, fingerprinting techniques can identify content without prior modifications. Thus they have an inherent advantage if used in application scenarios where content is already distributed without a watermark but an identification of the content is necessary. In this chapter we explain shortly the idea and application of fingerprinting technologies.

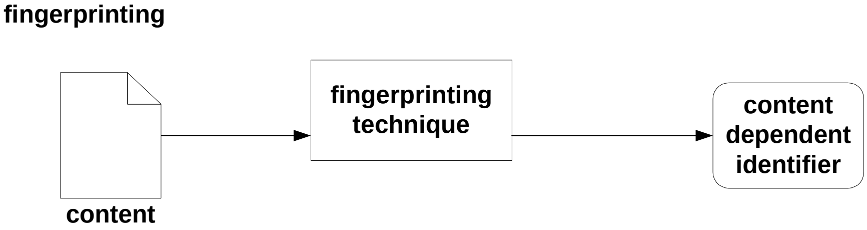

Figure 13: The fingerprinting method calculates the content dependent identifier directly from the original content. Thus the content has not to be modified.

6.5.1. General principle

Fingerprinting techniques calculate a content dependent identifier as shown in Figure 13. This content dependent fingerprint can be compared with a human fingerprint: It is a unique identifier for renderings and the original content cannot be created from the identifier. Thus these techniques are also related to the cryptographic hashing functions. But cryptographic hashing functions have the important property that closes input values to not result in close hash values. For fingerprinting techniques the opposite requirement must hold. Therefore they are also called perceptual or soft hashing functions.[37] Perceptual hash reflects the fact that perceptual similar content should result in a similar hash value.

[37] Sometimes even the term “passive watermarking” is used, which we consider as misleading as no mark is embedded.

Due to these properties fingerprinting solutions are very suitable for automatic play list generation, broadcast monitoring (e.g. [AudioID]). But other applications can be thought of e.g. tracking the content flow or even restricting the content flow (e.g. in corporate networks). Due to these characteristics fingerprinting techniques attract increased attention recently [Cano2002].

6.5.2. Characteristics and requirements

Fingerprinting techniques are related to content based retrieval (CBR). CBR methods also create a content dependent signature directly from the content, which also depends on the perception of content. This signature is also compared to pre-calculated and stored content signatures. Figure shows the principle steps necessary for the calculation of a unique identifier. First, features are extracted from the content. These extracted features typically have very high dimensions and are processed further resulting in unique identifiers.

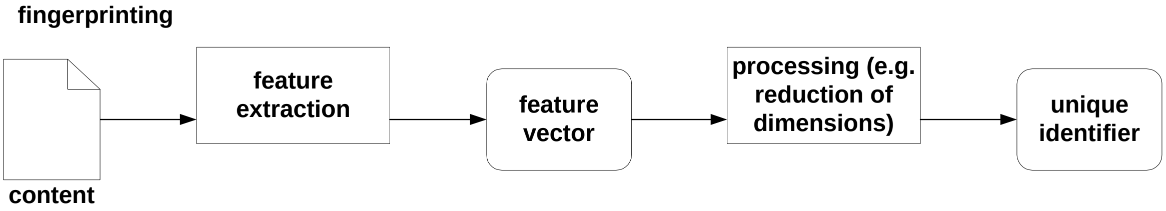

Figure 14: For calculating a unique identifier (perceptually) relevant features are extracted. These features are processed to reduce their dimensionality.

The feature extraction process itself can be quite close to the human perception and extract features which are directly perceived by humans, like the frequency distribution for audio. On the contrary features which do not directly depend on the human perceptions can also be used, as long as they allow the discrimination of content. A typical example is the sign of the difference between neighbouring energy bands as proposed by Philips [Philips].

If the complete information is used, the dimensionality of the feature vector would be very high. Therefore the dimensionality is reduced by removing redundant information. During this processing step further improvements, e.g. error resilience, can be achieved. The resulting feature vector should fulfil the previous listed requirements for fingerprints. A good feature vector has a increased robustness against noise resulting from the content acquisition (e.g. recording).

In addition to the feature vector a suitable distance measure is necessary. This is also related to CBR methods, where similarity has an important role. As typically a huge amount of data has to be identified, the scalability is important. This influences the features' choice, the distance measure as well as the retrieving architecture. Typical distance measures used are the Euclidean or related distance measures or distance measures based on correlation. The retrieving architecture also strongly influences the complexity and the scalability of the fingerprinting technique. Efficient spatial access structures were developed like indices or application oriented approach like the ones used for DNA information processing. A final hypothesis test calculates the probability of the correct identification of the content.

As the sole purpose of fingerprinting techniques is the identification of content, a good performance in discriminating a huge a mount of data and corresponding fingerprints is crucial. Similarly to watermarking techniques requirements can be identified:

- The *robustness* can be defined by the types and numbers of operations and their parameters applied the content, which does not effect the retrieval of the content. Typical operations depend on the application scenario where the fingerprinting method will be integrated in. For example when a system should be able to recover the song from a radio transmission that is recorded via a mobile phone the fingerprinting system should be capable of the reduced frequency band available due to the mobile phone. Also small audio extracts somewhere within the song must not result in misidentification as humans will rather realize in the middle or at the end of the song that is worth being remembered or purchased. Finally a noisy background will probably be the general recording place e.g. in a car, bar, club, or café.

- The *scalability* is an important criterion. For general data, e.g. millions of different types of audio content exist. Some of them are even available in different editions, e.g. studio or live performance recordings. Ideally a system is capable of handling all available works in a reasonable amount of time, where "reasonable" is again defined by the application scenario.

- The *complexity* of an algorithm is important for certain application scenarios where real time identification is important.

6.5.3. Limitations and comparison to watermarking

Different limitations have to be considered when integration fingerprinting technology. As already mentioned, fingerprinting techniques do not modify the content but calculate an identifier directly from the content itself. This is an obvious advantage when content is already available in an non-marked version. Yet, this is also a drawback in comparison to watermarking schemes. Personalisation is not possible. This has an influence e.g. an the tracking. Although content can be tracked, tracking users is not possible as content is generally not unique for individual users.

Instead of being marked content must be registered. That means that only content can be identified if its fingerprint was previously calculated and stored in a database.

Another limitation of these fingerprinting techniques have to consider when using fingerprinting controlling the data transfer networking infrastructure: encrypted content or scrambled content can not be identified. Identification is only possible with content that is accessible as it is intended for rendering.

A comparison between the different properties of watermarking and fingerprinting is shown in Table 3.

	Watermarking	**Fingerprinting**
Development	Has to be developed for individual media types	
Availability	Audio, video, images, 3D, music scores	Various media types with a focus on audio, video, images
Alteration	Content is altered by embedding	Not necessary but registration in database necessary instead
Registration	Not necessary (cf. alteration)	Prior to identification
Attacks	Vulnerable	Limited vulnerability (perceptual features)
Capacity	Varying on content (minimum requirement should be 64bit for creating a link)	Indirectly in the content and the method's ability to discriminate content
Infrastructure	Depending on application	Needed

Table 3: Principle characteristics of watermarking and fingerprinting schemes are summarised.

6.5.4. Applications in DRM systems

Besides the above listed applications of fingerprinting systems in automatic play list generation, broad cast monitoring, content tracking and content flow limitations another application is very interesting for fingerprinting techniques: royalties distribution. Content can be monitored in peer-to-peer networks with the help of fingerprinting techniques. This information can be combined with other information available e.g. meta data within the peer-to-peer networks used by humans for content identification. Keeping in mind the future revenue stream new possibilities can be created when new technologies are considered as discussed in chapter 11.

6.6. Summary

For each of the different basic technologies different realisations exist. This allows some flexibility for system developers in combining the different. For example, a DRM system can be implemented as an open source system. Nevertheless, this flexibility provides difficulties especially for the compatibility of the different DRM systems.

From a security point of view, it has to be considered that the whole system is as secure as its weakest part. This does not only address the individual components but also their interactions. Thus, components as well as their integration have to be chosen carefully.

7. DRM Technologies

In this chapter we describe the principle components of DRM systems. This general principle is more or less underlying each implementation of a DRM system. The typical parties involved are the content owner who distributes content, the customer or the consumer who purchases content, and a clearing house that manages licenses. For simplicity we assume that the content owner is also the content distributor, which is not generally the case. If this is not the case, the relationship between the content distributor and the content owner will influence the DRM architecture as content can be exchanged between these two parties at different security levels.

7.1. General aspects

Sellers of traditional goods benefit from online shops as they accessible without any time constraint. Product information as well as purchase related information can be made available. But not only traditional goods can be sold on the internet. Especially content providers of digital content have a general interest in and strongly benefit from online distribution. Several advantages can be identified including:

- availability: 24 hours a day and 7 days a week
- reduced costs: not only complete collections are sold
- try before buy: customers can have a pre-listening/preview
- customer relationship: direct contact to customers like personalized offers, increased feedback possibilities, ...
- reduction of shipping costs
- only a small storage space is need: data fits on a hard disk and must be stored only ones

Due to the fact that the content itself is valuable content providers deserve a secure distribution. Therefore content is encrypted before distribution. Distribution can be done in various ways among them is download or email transmission. For rendering content a licences is needed which can be stored locally or on a remote server. Also the customer is not limited to certain devices. As mobile phones become more and more multi-media devices potential customers might also want to access data via mobile phones. This is a general problem today. Customers don’t want to be restricted by protection solutions. As most available distribution platforms strongly restrict customers (e.g. content can be rendered only on one certain device) in the customers’ view DRM is the acronym for “digital restriction management”.

When analysing the security of a system, different assumptions have to be made as described in [Arnold2003]. These assumptions include the knowledge of the attacker. However, this is quite difficult to estimate as software patches (“hackz” or “crackz”) can be often downloaded from the Internet. This allows even users with almost no knowledge to circumvent certain protection mechanisms. Furthermore the applied security solutions can be secure while the runtime system isn’t secure at all. This allows potential hackers to successfully attack the runtime system while not interfering with the applied security solutions. Thus, a secure system is vital for the security of content. Therefore the hardware industry is targeting at secure devices[38].

7.1.1. DRM architecture

The general architecture of a DRM system is shown in Figure 15. Primary technology components can be identified (according to):

- *Packagers*[39] collect license information, meta data and the requested content in encrypted files. These secure files are called packages, containers, etc.
- *Controllers*[40] realise local rights management systems at the client side and are responsible for authentication of the device or the user, decryption of the content, provision of access to the content and sometimes for financial transactions.

[38] These secure devices are also called trusted devices reflecting the assumption that trusts in the security of the systems can be provided.

[39] Typically content servers provide this functionality.

- *License servers* or clearing houses are run by third trusted parties and create and distribute licenses that grant access to the requested content via the local rights management system and can also contain access conditions.

As described by Rosenblatt et al. a broader definition of DRM encompasses everything that can be done to define, manage, and track rights to digital content. Thus further elements are included in this definition:

- *Business rights* (or contract rights) are typically associated with some content in certain scenarios. E.g. the right to use a certain audio sequence in a commercial spot might be granted while processing of the audio sequence is prohibited.
- *Access tracking* or tracking of operations on content provides valuable information for content providers even if they do not charge for access to the content. This information also helps to improve business models or relationships to customers.
- *Rights licensing* is an important issue especially when content can be modified and is redistributed. However technical solutions are strongly limited, e.g. when the modification is translation.

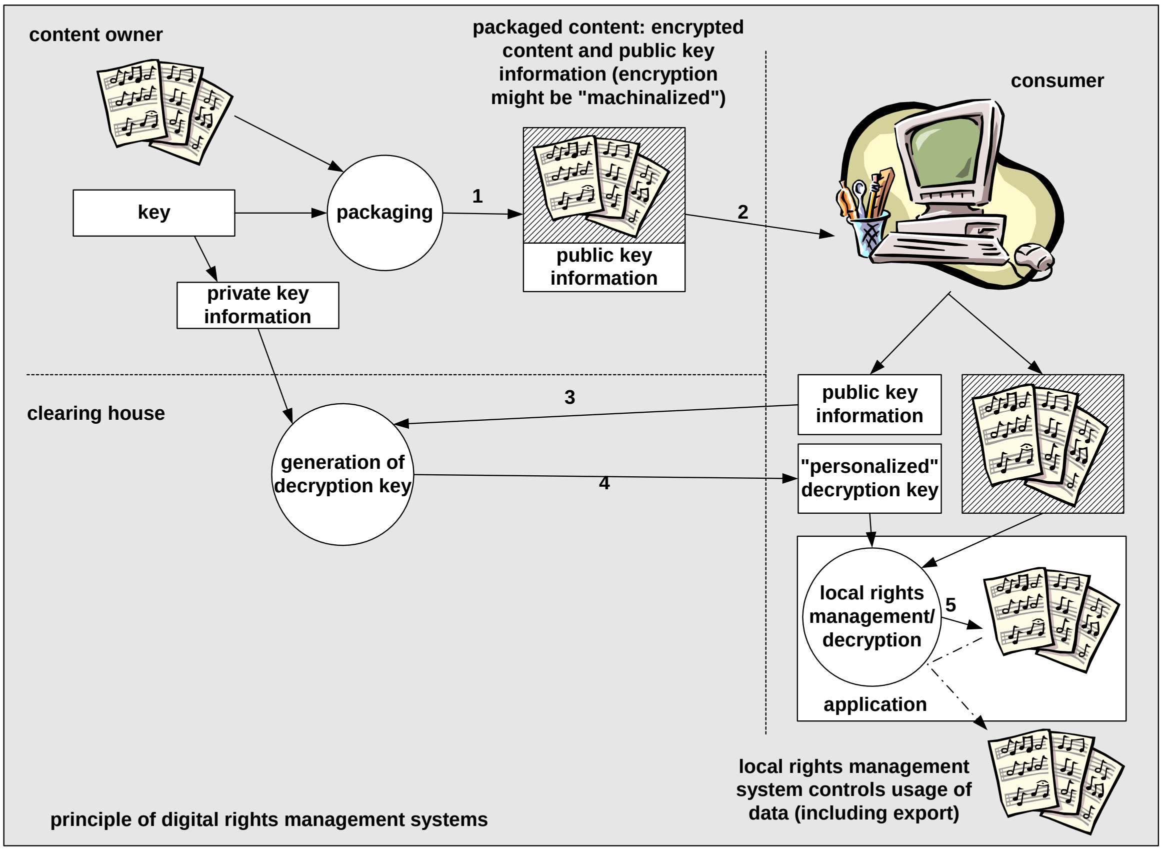
content owner
packaged content: encrypted content and public key information (encryption might be "machinalized")
consumer
key
packaging
1
2
public key information
private key information
clearing house
3
public key information
generation of decryption key
4
"personalized" decryption key
local rights management/ decryption
5
application
local rights management system controls usage of data (including export)
principle of digital rights management systems

Figure 15: This figure illustrated the principle architecture of a DRM system. The important aspect is that content is always encrypted outside of the DRM environment. Whenever an application wants to access information, the local rights management system is called to decrypt the content and it also influences the functionality of the application. Thus a user cannot access any data outside the DRM system.

7.1.2. Content owner

Whenever content is distributed this content is encrypted using the methods described in chapter 7 and the encrypted content is transmitted to the customer with public information about the encryption key. This process is called "packaging" and is step "1" in the figure. However, this is just a very minimalist view on the package and the packaging. Typically rights information is also included in the package to permit or to restrict certain types of operations, certain operations intervals, or the amount of operations as well as

[40] Controllers are sometimes also called "DRM controllers".

additional product information (metadata). This rights information is stored in the license. Possible rights description languages are described in chapter 6.

Content is stored in a repository. Either the repository is built within the DRM solution or it is part of a CMS system. If a CMS stores the content and the packaging system is not able in managing arbitrary file types the storage format of the content must be chosen according to the capabilities of the packaging respective the DRM system.

Again, it is also necessary to protect the content distribution system. Typical attacks might come from the Internet. These attacks can be faced by a well configured firewall. Yet, attacks from users with physical access to the content distribution system are also possible. Thus, trust in the people working at the content distributor's side is also necessary.

After packaging, content is distributed to the consumers. This can be done using different transmission channels. The Internet via download is probably the most common channel. But also a transmission via email, floppy disk, or CD is possible. The transmission processes is indicated in step "2".

7.1.3. Consumer

Whenever the consumer receives the content it is initially useless for him as it is encrypted. Thus, he needs the decryption keys. Of course it is possible to distribute the keys directly to the customer. Yet, this would reduce the security of the system drastically. Therefore a local rights management component is responsible of this task. This component requests they keys from the clearing house (step "3"), which is a third trusted party. To increase the security this local rights management component is unique and can be identified. Thus personalised keys are send to the local rights management component (step "4"), which makes them only useable for one certain local rights management component.

After receiving the decryption key the content is decrypted. For security reasons neither the decryption key nor the decrypted content[41] must be stored locally. Therefore a strong connection between the local rights management component and the application rendering the content is necessary, as content exchange is not only possible via files but also through other channels, like the clipboard or via screenshots.

We'd like to stress that the previous described functionality is not restricted to a personal computer. It can also be deployed in other devices. But certain – e.g. mobile – consumer devices will result in certain requirements on the complexity of the involved algorithms as there computational power is weaker and the usability of devices is directly correlated to the execution speed of certain operations.

One important aspect – not only when dealing with mobile devices – is the problem if the DRM solution should also be functional in an offline environment. This requirement increases security threats considerably.

7.1.4. Clearing house

The clearing house enables the consumer to render the content. The minimalist version transmits "personified" decryption keys to consumers. A more sophisticate version considers licensing issues: The valid content usage period or the amount of rendering. The clearing house is also able to initiate financial transaction, e.g. when pay-per-use is demanded in the license.

7.1.5. Rendering applications

As described above, a strong connection between the local rights management is necessary. In [Rosenblatt2002] different rendering applications are distinguished: standalone, plug-in, and java rendering applications.

[41] Local storage of the decrypted content depends on the business model. Some business models might allow this. Some might only allow local storage with poor quality (e.g. strongly compressed audio files).

- *Standalone* rendering applications allow a maximum control of the content. Yet, this advantage has to be paid with several drawbacks: First, the software has to be distributed to the consumers. Second, the consumer has to install the proprietary software on his hardware. Generally, users prefer ready-to-use solutions. They don't want to be bothered with technical details.
- *Plug-in* rendering applications are common solutions, which integrate themselves into existing software. As a direct consequence the functionality of the "hosting" software is augmented. In the case of DRM plug-ins it is able to render a increased number of files types. Of course, the plug-in has to modify the "hosting" software's behavior to control data exchange and to avoid any content leakage.

Unfortunately these solutions have to be developed for each hardware platform. From a content distributor's point of view *Java* combines the advantages of standalone and plug-in applications and additionally throws away the hardware dependency as Java programs are not run directly on the microprocessor but are executed on a simulated processor, which is called the Java Virtual Machine (JVM). DRM solutions implemented in Java can be run on every processor for which a JVM exists.[42] Today this is the case for most web browsers. Although [Rosenblatt2002] et al. raise the problem of incompatibilities, we think that an efficient platform independent DRM solution implemented in Java is possible.[43]

7.1.6. Security issues

Above we already addressed relevant security issues. But as the main purpose of a DRM solution is the protection of content respectively its license conform usage we further investigate this problem within this section. Security is always related to certain assumptions. For example, the above described assumption of the technical skills of an attacker. But other security issues are directly related to the user and the involved hardware and software platforms.

Digital rights management systems for general content distribution scenarios require **the identification of the user.** E.g. this is very important for secret information exchanged within a company. Similarly a identification of a customer is important in the music distribution scenario as consumers can be seen as business partner. For the business transaction a credit card number might be sufficient. Practically content usage cannot be limited to the person who purchased it. Thus, information about the person rendering the content is necessary. This information may be a simple email address, a user ID, a password, or other personal information. In other application scenarios biometric identification systems are used. E.g. one can think of personalized mobile devices with biometric sensors: a "lost" mobile device is useless for its "finder". Yet, simple biometric solutions – and these are all current solutions which can be integrated into mass products for monetary reasons – can be easily fooled. Other solutions exist, like the "typewriting style" are considered by music distribution solution providers [MUSICRYPT]. For identification other possibilities include digital certificates (created by a third trusted party) or smart cards.

Besides user identification **device identification** plays an important role. This can be done e.g. by a unique identification number or by the Media Access Control (MAC) address[44]. The advantage of using the MAC address instead of the IP address is the fact that IP addresses can be dynamic addresses and also an IP addresses can correspond to multiple users.

Device identification is not sufficient at all. One aspect that is generally neglected is the device integrity. The device integrity includes hardware as well as software integrity, which is very difficult. First, hardware and software are under total control of a user.[45] But even if the customer is trustworthy, "external influences" like Trojan horses might violate the device's integrity.

[42] Of course the processing power must be sufficient.

[43] The incompatibilities between Microsoft's Java version and Sun's Java version were mainly due to a "misinterpretation" of the Java specification.

[44] The MAC address is a unique value associated with a network adapter and are also known as hardware addresses or physical addresses.

[45] At least this is the case nowadays. This might change in the future if the "trusted computing" initiatives succeed. Yet consumers have to pay for this technology and they do not only benefit from it.

The problem of the device integrity is addressed by the “trusted computing” activities like the “Trusted Computing Group” [TCG], “Trusted Computing Platform Alliance” [TCPA], or “Next Generation Secure Computing Base” [NGSCB]. This is typically assumed as a precondition, e.g. in [DPRL98]: “DPRL assumes a trusted environment, and part of Xerox's licensing activity centres around toolkits that enable construction of that environment. ’Trust' simply means that the agents performing users' actions on an object must honour the rights specification for that object --- the agent must charge the user if that is specified, or prevent the action if the appropriate right code is not present. Trusted implementations can obviously range from individual trusted rendering tools all the way to a fully trusted network environment.” Yet, this is difficult to achieve, especially whenever the hardware and software cannot be fully controlled, which is the usually the case whenever a consumer owns a device.

The “trusted computing” idea, which is supported by the most hardware and software players, aims to a standard for a “more secure” PC. Although this goal is very important in commercial scenarios (e.g. document security, information assurance …) such a standard is ambivalent for consumers [TCFAQ]. The danger is that control of individual hardware is transferred from the hardware owner to other parties like the software vendor implemented the operating system or the content industry in general. While this is interesting for content distributors, consumers might neglect this standard as from there point of view the system is less trustworthy and what is even more important: somebody has to pay for the additional components. The resulting trusted devices will not allow access to decrypted data, e.g. through debugging software, will not start modified software, and they will also control the input and output devices.

7.2. Integrating DRM systems with existing systems

Although DRM systems can be used as stand-alone solutions it is more fruitful to combine DRM systems with other systems to maximize their common benefit. As DRM systems manage content access they can be used whenever content is involved. Thus DRM systems address the complete content “life cycle” and related tools or systems, including:

- Content Creation Tools
- Content Management Systems (CMS)
- Customer Relationship Management (CRM)
- Web publishing systems
- Access Control
- …

In companies typical a certain workflow process was established. As modifications of an existing workflow process is very expensive or maybe not possible, deploying DRM systems mustn’t result in any change. This is even more important when techniques or solutions are applied for the protection of content. The protection level of some protection technology is time depending – it might depend on the time and effort attackers spent in breaking it. If some content requires the highest protection level, the involved protection technology must be updated regularly. Therefore changes of the workflow process are not manageable. But DRM systems must not only fit in the workflow process but should also support it.

The general interest in DRM system is reflected in Microsoft’s ambitious goal to include a complete DRM System within their next operating system release called Longhorn. Yet, this complexity of this task led to some procrastination [CRN2004]. However, there are strong concerns about the integration of DRM functionality in operating systems [Anderson2003, Anderson2004, EFF2004].

7.2.1. Content creation and management

In business application scenarios dealing with content creation and management DRM technology can be integrated in the content creation tools and the content management system. The main motivation for this is that content is always stored together with meta data. This meta data may include contract rights or licensing rights.

As an alternative, rights meta data can be created by a manual input. Yet, manual input is expensive as well as error-prone. Thus a DRM system allows the automation of meta data creation and improves its consistency even if compound works are created. For example an audio visual presentation might contain several individual images, video sequences, songs and speech, which have their individual rights. Content creation and authoring software involving a DRM system can automatically deal with these rights issues and also solve problems when extracts of such a kind of audio visual sequence are created.

Besides the storage of rights in a DRM system fingerprinting and watermarking technologies can link media to the corresponding set of rights. Thus even a link between the rights and the rights is possible when a media break happened. These Content Management Systems (CMS) integration issues are addressed in [Rosenblatt2003a] and [Rosenblatt2003b].

7.2.2. Web publishing and customer relationship management

Deployment of DRM solutions in consumer related areas typically involves the sales of digital content. This has to be done via an online catalogue or portal. DRM solutions provide the necessary technologies to achieve different business models that better suit the wishes of customers. These business models may include subscription based services, free time-limited trials, or pay-per-rendering and can be chosen independently for different customers.

Further improvements are possible when DRM technologies are integrated with Customer Relationship Management systems. Therefore the offers can be chosen exactly matching the customers’ behaviour. E.g. whenever a customer purchases a rendering right for a certain content, free time-limited trial rights can be created for related content. Also the prices for products can be adapted to the usage allowing a subtle change between pay-per-rendering and subscription based services. [Rosenblatt2003a] and [Rosenblatt2003b] also address these distribution issues.

7.2.3. Access control

Access Control is a desired criterion for content providers and content owners. Yet, this is not a desired criterion for customers as they generally do not accept any restrictions on content they purchased. Also, access control might also interfere with privacy as discussed in [Cohen2002] and considered in [EUDirective]. Thus we don’t go further into details of this issue.

Another aspect of access control is from a company’s point of view that wants to keep confidential material within the company. Thus Enterprise Content Management (ECM) can be regarded as an application which very strongly demands efficient rights management systems. Thus [NGSCB] and [TCG] lay the necessary foundation for a secure environment within business applications.[46] As the computers involved in this area are under the control of one administrator the security assumptions within this scenario are different from the previous scenario. Also DRM systems do not interfere with privacy in this scenario. But DRM systems might interfere with other laws as access to information can be limited to a certain time-interval.

7.3. Examples for conflicts between security and consumer issues

We also like to give two examples how the security intention of DRM systems can interfere with consumer issues and sometimes even with law. These incompatibilities can be created artificially for the protection of content e.g. in the case of Macrovision. Also a proprietary format can result in incompatibilities, e.g. in the case of Sony.

- Macrovision’s [Macrovision] video copy protection system [MVVCP] is a popular product for protecting video content. It was originally developed for video home systems (VHS). An additional copy protection signal is inserted in the part of the video signal used to control the TV (vertical blanking interval and extra synchronisation pulses). The idea is that this kind of noise doesn’t interfere with the screen representation of the visual content. But if a video cassette recorder (VCR) tries to make an exact copy of the video signal containing the copy protection signal it will fail drastically (for the visual content).

[46] Other possible consequences, e.g. software monopoles, have to be considered carefully and a thorough observation is necessary to avoid negative effects to economy.

Interestingly this idea worked fine with TVs produced before Macrovision's protection system was developed. However with the growing numbers of DVD devices people found out that for some TV sets the only possibility is to connect the DVD to the screen via the VCR. Although the signal is passed only through the VCR in this case, some activate their video-scrambling chip leading to the same distortion as descried above. Additionally some TVs are not capable of resolving the Macrovision signal due to the bas synchronisation pulses. And the Macrovision's video copy protection system delayed the development of DVD players with a progressive[47] output signal.

- Not only Apple insists on proprietary format. Also does (or did) Sony. BETAMAX is an example where Sony failed with a proprietary format. Sony founder Akio Morita saw the reason in the missing license possibilities resulting in the fact that the inferior VHS system reached a critical mass. Besides BETAMAX MicroMV was another proprietary format, which was abandoned although it was introduced recently in 2002. Another proprieraty format is ATRAC3, Sony Minidisc format. Even the memory sticks used in Sony's digital cameras and PDAs are proprietary.

Incompatibility as it regularly has happened with Macrovision's video copy protection system is also an issue for the protection of music CDs. Incompatibilities interfering with a trouble-free enjoyment led to the creation of "negative lists" like [UnCD]. Proprietary formats are always critical. For example Microsoft Office documents can hardly be exported to software products produced by other vendors. But for protected content this is even more critical. On the one hand content is encrypted. On the other hand the representation is unknown. Potential problems can be foreseen not only in case a proprietary format: Customers will not be happy if a proprietary format is abandoned. But furthermore there is one aspect, which is never considered by industry. Archives must provide access to content even after years of its creation and distribution. They will fail poorly as today it is already a problem to access content in old formats stored on outdated devices as hardware and software for access is missing. This problem will become much more severe with encrypted content whose decryption keys are not accessible anymore.

7.4. Further criteria

In addition to the above mentioned characteristics further criteria can be evaluated either for complete systems or for individual components. These criteria include:

- *Degree of protection*: As described before, one has to be clear who the potential attackers are and what kind of attacks can be performed. On the one hand typical customers should not be able to break the system. On the other hand commercial oriented product pirates should also not be able to attack a DRM-system successfully. Both groups can be distinguished by their knowledge and the available tools. Especially for commercially oriented pirates there is almost always a way to break the security of a DRM-system as they expect a monetary benefit. Firstly, they can hire professional security experts[48] who have the necessary knowledge. Secondly, they can buy the necessary equipment, which is sometimes expensive. Therefore a huge variety of attacks can be performed including attacks penetrating hardware.[49]

- *Known attacks*: Considering the security of DRM-systems, one important question is: Are there any know attacks against the complete DRM-system or against individual components? As any DRM system is as strong as its weakest component one has to consider this aspect carefully. In some cases the weakest points might even be humans. For example if people are interested in hacking a server sometimes the easiest way might be to bribe its administrator for creating security holes, which can be exploited easily. Besides the knowledge of successful attacks details

[47] Typically a TV sets uses interlacing, which combines two "half"-images into one. DVD players are capable of producing a progressive output signal – one complete frame at once.

[48] Due to their motivation "semi-professional" hackers can be considered as a big threat.

[49] Thus people interested in the protection of their content have to be aware that the higher the monetary benefit is, the bigger is the potential danger that an attacker has commercial interests.

about the attack itself are important including the effort and the consequences. On the one hand a successful attack might take a lot of time, involve expert knowledge, and has to be performed on each digital item. On the other hand an exploit of the system might have been discovered resulting in a software patch available on the Internet. Balancing the negative effects it is obvious that the second kind of attack is much more severe and might almost destroys the security of the whole DRM-system. This is not a theoretic or potential threat. The software industry experienced that hackers[50] react fast and sometimes publish new exploits within a few days in the Internet.

- *User acceptance - usability*: Any hindrance to content access caused by DRM-systems directly reduce user acceptance. Thus, an ideal DRM-system should not be experienced by any user unless a user has the intention to violate the licensing conditions. Unfortunately this is practically not realisable as operations cannot be qualified in (current) DRM-systems. For example, a DRM-system cannot distinguish between a legal[51] format conversion and an illegal one. As a consequence a DRM-system prevents all operations that potentially lead to a violation of licensing conditions[52]. One of these effects is the denial of copying in DRM-systems leading to strong impacts on accustomed ease of handling content.

- *User acceptance - compatibility*: An important aspect of usability is compatibility. The rendering of content should not be limited to a specific class of devices. This is a major obstacle of today's DRM systems. Although there are ongoing standardisation issues, no compatible DRM exists yet.

- *Current popularity*: Obviously content owners and distributors are in favour of DRM as it supports them in protecting content. Due to restrictions imposed by DRM systems and due to privacy issues most users are against DRM systems. However, the success of iTunes shows, that DRM solutions, which are not as restrictive or obvious, are acceptable for customers.

- *Future trends*: DRM is a relative young issue and which address not only rationality but also feelings. Also little experience was gained so far with its application. The development of new DRM systems with different kinds of restrictions will show what will be acceptable for customers practically.

7.5. Summary

Obviously, DRM addresses a wide range of technologies and also legal issues. This makes this topic quite complex. Its main purpose is the protection of content. Thus, security is a very important issue although not easy to achieve. As a consequence operating systems implement more and more functionality needed for the protection of content. Their initial implementations [TCG, TCPA] experienced strong resistance, e.g. as privacy and traditional content usage are not guaranteed.

As explained before, user acceptance is however crucial for the success of business models as well as for the success of DRM systems. Among the important aspects is compatibility and traditional content usage. This does not mean that customers will not accept DRM. Apple shows with its iTunes Music Store – it has a less restrictive content protection policy – that customers are actually willing to pay for DRM protected content.

[50] Sometimes this kind of hackers is also called crackers.

[51] For example archiving or providing access to visually impaired people are most often allowed by law.

[52] Interestingly in the physical world such a practise is not manageable or allowed. For example knives are still sold although people can potentially be hurt.

8. Towards the customers

Although music labels were strongly in favour of CD copy protection technologies, more and more music labels do not apply CD copy protection technologies anymore. Users did not appreciate the obstacles they realised.

This is something content owners and distributors have to understand. Maybe the following statement explains the users' restrictions to content owners or distributors best: "I will accept your DRM protected content if you accept my DRM-protected money!" Thus, new solutions are needed considering the customers' requirements and objections. Similarly, the decision of a French court against DVD copy protection shows that new approaches have to be developed. In this chapter we summarise recently developed and on-going developments that are better consider customers' requirements.

Obviously, DRM and content protection is still a hot topic. But as shown by Apple's iTunes MusicStore – and some others that want to get a share from Apple's success – users potentially accept content protection technologies. Nevertheless, there are ongoing developments, which are focus on the user requirements that have not been sufficiently considered yet.

8.1. Interoperable DRM

One of the major reason customers are very reluctant against is compatibility respectively the lack of compatibility. "Buy once, listen anywhere and anytime" is not possible with current DRM systems. Actually, this was one of the reasons why customers reject copy protected CDs: They cannot be played on all consumer devices (including computers).

In the digital world the situation is even more complex: Having different storage carriers, different media encodings and recently different DRM containers dramatically increases the difficulties in exchanging content.[53] And for ordinary users this is a big issue: they are interested in enjoying content – they neither want to be bothered with any technical detail nor with any problem.

As described before, there are ongoing efforts that address compatible DRM, which we will outline below.

8.1.1. CORAL

The Coral Consortium is "a cross-industry group to promote interoperability between digital rights management (DRM) technologies used in the consumer media market. The Consortium's goal is to create a common technology framework for content, device, and service providers, regardless of the DRM technologies they use. This open technology framework will enable a simple and consistent digital entertainment experience for consumers." [CORAL]

Two different member types exist: "Promoter" and "Contributor Members". Among the "Promoter Members" are:

- Hewlett-Packard Corporation
- Intertrust Technologies Corporation
- Koninklijke Philips Electronics N.V.
- Matsushita Electric Industrial Co., Ltd.
- NBC Universal, Inc.
- Samsung Electronics Co., Ltd
- Sony Corporation
- Twentieth Century Fox Film Corp.

[53] This is a general problem especially for digital archives even without DRM: Will any device to read the content stored on a specific carrier be available in twenty or thirty years?

The “Contributor Members” include

- Ardtully Technologies
- Cloakware Corporation
- DMDsecure
- EMI Music
- IFPI
- Kenwood Corporation
- NDS Americas, Inc.
- Pioneer Corporation
- Seagate Technology, LLC.
- Sony BMG
- Starz Entertainment Group LLC
- STMicroelectronics, N.V.
- Sun Microsystems
- Time Warner Cable
- Universal Music Group
- ViDeOnline, Inc.
- Warner Bros. Technical Operations Inc.
- Warner Music Group

According to CORAL’s FAQ, it “addresses the problem of interoperability between DRM and media format approaches by leveraging service-oriented architecture; this is not addressed elsewhere. The group's specifications will allow migration of media and user rights between different domains, and where possible, it will use existing specifications that are appropriate (e.g., web services specifications). The Consortium's specifications are transport and network-agnostic. There are other groups looking at DRM interoperability; these tend to focus on agreement of format, rights expression, and other technologies. Coral Consortium's approach supports these types of efforts but also allows for monolithic approaches to interoperate without changing their technology.” [CORAL].

At the beginning of March CORAL published the “Coral Consortium v1.0 Specifications” [CORAL].

8.1.2. DMP: The Digital Media Project

DMP is „not-for-profit organisation with the mission to "promote continuing successful development, deployment and use of Digital Media that respect the rights of creators and rights holders to exploit their works, the wish of end users to fully enjoy the benefits of Digital Media and the interests of various value-chain players to provide products and services.“

In his Digital Media Manifesto [DMM], Chiariglione identified different concerns against DRM:

1. From the existing value-chain business players’ view DRM does not allow protect already published or distributed unprotected content. Furthermore, it requires new distribution mechanisms and new end-user devices.
2. New value chain players are afraid of restriction potentially imposed to them due to disabling DRM features.
3. End-users experience restrictions on content usage. Furthermore, their privacy is violated.

According to [DMM] the result is a stalemate as the potential of the “Digital Media Experience” cannot be exploited fully. This stalemate results in an economic and a social damage.

As a consequence policy and technical actions have to be performed (for details please consult [DMM]). Identified policy actions are:

- P1: Mapping of rights and usages traditionally enjoyed by users to the Digital Media space
- P2: Phasing out analogue legacies applied to Digital Media
- P3: Deployment of broadband access
- P4: Improving development of and access to standards

Similarly, technical actions have been identified:

- T1: Interoperable DRM platforms
- T2: Interoperable end-user devices
- T3: End-to-end conformance assessment

Corresponding actions, e.g. which result in specifications or recommended practices, have to be identified and coordinated. This is done within the Digital Media Project (DMP).

Members in the DMP include:

- British Telecommunications (UK)
- CEDEO (IT)
- Enterprise of the Future (US)
- École Polytechnique Fédérale de Lausanne (CH)
- MPEG LA (US)
- Multimedia Architectures (JP)
- Sociedad Digital Autores y Editores (ES)
- Telecom Italia (IT)
- University of Tokyo (JP)
- Electronics and Telecommunications Research Institute (KR)
- DivX Networks (US)
- Pixtree Technologies (KR)
- Matsushita Electric Industrial Co.,Ltd. (JP)
- INESC Porto (PT)
- Mitsubishi Electric Corporation (JP)
- BearingPoint Consulting (US)
- Institute of Computing Technology, Chinese Academy of Science (CN)
- Victor Company of Japan, Ltd. (JP)
- Sisvel (IT)
- British Broadcasting Corporation (UK)
- ADETTI (PT)
- INKA Entworks (KR)
- Industrial Technology Research Institute (TW)
- National Computerization Agency (KR)
- Fraunhofer Gesellschaft (DE)

In May 2005, DMP published “Interoperable DRM Platform specification” [DMP_SPEC].

8.1.3. ISMA: The Internet Streaming Media Alliance

ISMA's goal is "to accelerate the adoption and deployment of open standards for streaming rich media content such as video, audio, and associated data, over Internet protocols." [ISMA]

Thus, ISMA is addressing a wide range of topics like:

- encoding (e.g. for audio and video streaming)
- exchange protocols
- DRM issues
- Solutions for content owners

Certainly, DRM is also among these issues. Different specification are available free of charge at [ISMA].

Member in ISMA are:

- Act, Inc.
- America Online, Inc.
- Analog Devices Inc.
- Apple Computer, Inc.
- California State University, Fresno
- Case Western Reserve University
- Cisco Systems
- Coding Technologies
- ContentGuard
- DMDsecure.com
- Dolby Laboratories Inc.
- Envivio
- France Telecom
- Fraunhofer Institute for Integrated Circuits
- Fujitsu
- Hewlett Packard
- Hitachi
- IBM
- Inka Entworks
- OPTIBASE Ltd.
- Philips Electronics
- Standby Program
- Sun Microsystems
- Telecom Italia Lab
- Thomson
- University of Washington
- Vbrick Systems, Inc.
- Widevine Technologies
- WIS Technologies Inc.

8.1.4. OMA: Open Mobile Alliance

Similarly to ISMA, which is not in limited to a specific technology but is in favour of a certain range of applications, OMA wants to promote the usage of mobile devices. Its mission is "to facilitate global user adoption of mobile data services by specifying market driven mobile service enablers that ensure service interoperability across devices, geographies, service providers, operators, and networks, while allowing businesses to compete through innovation and differentiation." [OMA]

There are numerous members, which are distinguished as sponsor, full member, associate, and supporters including most relevant partners in the areas of hardware manufacturing, software development, research laboratories, and content owners and providers.

Different specifications are available online [OMA] including DRM related publications like:

- Enabler Release Definition for DRM Version 2.0
- DRM Architecture Version 2
- Specifications OMA Requirements Document for DRM Version 2.0
- DRM Rights Expression Language Version 2.0
- DRM Specification Version 2.0
- DRM Content Format

8.2. *Less interfering DRM*

Developing interoperable DRM systems is only one direction for improving the usability of DRM protected content. Another direction is not to develop new formats and devices but to use existing formats and embedding customer information. This has been described before as transaction watermarks.

One example for this is the *Light Weight Digital Rights Management* [LWDRM]. It cooperates with consumers. It distinguishes between locally bound and signed content in which user certificates are enclosed. As these user certificates link the content to users, users are expected to be very reluctant in distributing this personalised content.

The philosophy behind this is quite simple like the car's license plate: In principle, the users can do anything with their content. There is no restriction unless the content is not distributed to others. If such personified content occurs on illegal file sharing networks, the responsible user can be identified and blamed for this. This is similar if a driver violates a speed limit and can be punished for this.

Besides the usage aspect – traditional content usage is not prevented – user awareness is increased: Users become responsible for the content the purchase.

8.3. *New Developments in P2P-networks*

There are also ongoing developments, which try to commercialise the distribution in P2P-networks.

8.3.1. Music2Share

In [Music2Share] each client integrates fingerprinting and watermarking techniques that allow the identification of the content exchanged. Simplified, before a client is allowed to receive content his request is evaluated from a trusted third party to identify, if he already licensed the content. If so, the content is transferred to the customer. This allows putting different business models on top of existing P2P-networks.

After receiving the content, the content is encrypted or put in a DRM container together with the licensing information retrieved from the TTP. Again, users experience restrictions when content is DRM protected. Although no technical details are available during writing this report, it seems that [SNOCAP] implements this architecture.

8.3.2. The "Social Distribution Network" (SDN)

User awareness and user responsibility are the key concepts of the so-called social distribution networks (SDNs) as presented at [SDN_IST] or [SDN_CAST][54].

[54] This and the resulting architecture was a direct result of the discussion within the MUSICNETWORK when looking for a possible decentralised solution for unknown musicians.

The authors motivate them by the following train of thoughts:

- Perfect content protection is not possible. There are always security leaks like the analog hole. This has to be considered when efforts are spent for the development, integration, or usage of DRM. This means that at least specialists “unprotect” DRM protected content.

- Content exchange via the Internet cannot be controlled.

- Unknown artists do not care about DRM and illegal distribution as their primary income is not from record sales but from performances, ring tones, etc. Nevertheless, they deserve a platform for the exchange and especially the promotion of their content. This platform requires the possibility to stop the delivering of content upon request.

- Users are not bad. They will not redistribute illegal copies to harm artists. Instead they are willing to pay a reasonable amount of money for music that is unrestricted in its usage.

- Users will support artists by promoting content. Additionally, they will create additional meta data. This additional meta data further promotes artists’ content.

A distribution system, which integrates consumers, is most attractive if it is based on P2P-networks: “Let them make work (pay) for you” is the direct benefit for artists. P2P users pay for storage and bandwidth. In [SDN_CAST] a P2P-based architecture was presented that considers the above issues and provides a framework for the secure exchange of (initially) unprotected content.

In contrast to SNOCAP, the content protection is initially not needed. Everybody who is registered can distribute content in the P2P-network. User awareness is achieved by the feedback to the customers: If the content that should be distributed is already registered as non sharable the user gets a message and cannot distribute this content. In contrast, if this content is not registered the user has to register it to him. After this registration content can be distributed freely within the P2P-network.

Due to the fact that content itself is not DRM-protected this distribution network is very interesting for the promotional distribution of content, especially for relatively unknown artists.

8.4. New licensing and business models

In addition to the technological developments new licensing and business models are being developed. In general, there are not limited to a certain distribution channel. Some of them are presented here.

8.4.1. Super distribution

The Potato-System [Potato] and WeedShare [WeedShare] are typical super distribution business models. The users who distribute content of artists gets money for the distribution if the recipient buys the music.

8.4.2. Creative Commons

Creative Commons uses “private rights to create public goods” [CC]. It main intention is that others can use others’ work only for non-commercial use. This license model is related to GNU GPL [GPL] and EFF Open Audio License [EFFOAL].

8.4.3. Fisher’s license model

Fisher’s license model is based on a low-rate subscription. Fisher showed in detail how such a model could work [Fisher2004a, Fisher2004b].

8.4.4. German Academic Publisher

German Academic Publishers [GAP] is developing a new model for the design and administration of electronic publications. It is especially interested in the scientist’s need for “Open Access”

8.5. Summary

Customers' acceptance is the most critical issue of content protection technology. Thus, current developments are looking for remedies for customers' reluctance. As protection technologies address a wide range of areas, these areas are also considered in current developments. Unfortunately, the presented developments have recently been finished or are still under development. An interesting aspects is to raise consumers aware and their responsibility while incorporating them in the distribution of content either buy online reputation systems or by using their resources. There is a huge potential in the user communities as examples in other areas show.

9. Outlook

Return on investment (ROI) or return on capital employed (ROCE) plays an important role for non-profit as well as for commercial organisations. Both judge solutions' and technologies' benefit according to their ROI. ROI is even more important if venture capital is involved or a company is listed in the stock-market.
One problem of general security solutions is to measure this return on investment. Costs for new technology can be measured accurately but what about the saved amount of money? The problem return on security invest (ROSI) is currently highly debated. Some information on ROSI can be found at [ROSI2003]. This situation is even compared with the problem of selling fire sprinklers at the end of the 19th century: "[Parmalee] realized that he could never succeed in obtaining contracts from the mill owners ... unless he could ensure for them a reasonable return upon their outlay," [ROSI2003b]. In [ROSI2003c] some guidelines are given including "How to do it", ROSI a spreadsheet for the ROSI Model and a references on contemporary research.

As DRM belongs to the category of security mechanism the same problems arise here. Yet, additional return on investment factors can be identified:

- cost saving resulting from electronic stock
- cost saving resulting from traditional content delivery (including packaging or redelivery)
- flexibility and scalability of the online solution (business model can be changed or adopted easily)
- improved services to customers (e.g. availability, transmission speed, …)
- improved customer relationship management
- improved monitoring capabilities
- improved brand loyalty

Again, returns are difficult to measure. But it should be clear that the benefit of a modern combined distribution and DRM solution is far beyond the return on investment by protection of content after the point of purchase.

In [Bomsel04] the economic characteristics of DRM are characterised. Two main economic functions of DRM are defined: content protection and versioning. Then, the mechanisms of DRM adaptations are analysed. Network effects are considered in this analysis. Interestingly, this analysis distinguishes between open and dedicated networks for content delivery. For example, mobiles are considered a one-way dedicated channel for content delivery. Although the analysis identified the DRM's significance for content delivery, three obstacles are identified for DRM's roll-out in open architectures (in contrast to dedicated networks).

1. "The current economic model of Internet access … does not favour non free open services." [Bomsel04].
2. "In broadband networks, pay content distribution conflicts with the network effects pulling the roll-out" [Bomsel04].
3. "Content owners may push alternative networks" [Bomsel04].

One consequence of the analysis is that "broadband open networks may give priority to two way communication services … rather than to pay models for digital media content distribution"[Bomsel04].

9.1. The future solution

In the previous chapter we described the general principles of DRM systems. Again we'd like to emphasize that DRM systems integration within other solutions like content management systems will increase the benefit most. Aspects that cannot be neglected in the design and decision process include the business models and the workflow process.

Currently there is a change in the hardware and software industry. Their tendency is going into the direction of “trusted computers” or “trusted devices”. Independently how long it takes to achieve these ambitious goals – which has some advantages and also some drawbacks – customers have to accept these solutions and also to pay for them. This development towards “trusted devices” is highly debated, as it seems to endanger the right for “free speech” and free information exchange. Future solutions of trusted computers might allow the customers a more flexible key management away from hardware keys stored in machines but with keys stored in smart cards. This will also be influenced by other standardisation activities like DMP, OMA, CRF or CORAL.

So what the future might bring is hard to say as the history already told us that not the best solution must succeed in the long run[55]. Nevertheless GartnerG2 and the Berkman Center for Internet & Society [Berkman2003] presented “five possible scenarios for copyright law applicable to digital media in the United States“. These scenarios predicted losses and gains for consumer values and costs and revenues for content owners, artists, technology CE vendors, and Internet service providers:

1. *The no-change scenario* is based on the assumption that DMCA is still enforced: „This scenario is the least likely to play out, as the entertainment industries are not likely to sit still and see their business models slowly destroyed. Media companies have already attempted to address piracy via legal, regulatory and technology solutions. They will continue to pursue solutions to what they perceive as an attack on their traditional business models. However, it is likely that the no-change scenario will prevail in the immediate future as efforts so far have yielded minimal results and piracy is still widespread.“ [Berkman2003]

2. *The taking property rights seriously scenario* is based on the assumption that content owners and providers strongly succeed in protection their IPRs. As a result the gains for content owners and artists will increase together with increased cost on the overhead with violation prosecution. Technology and Internet service providers will gain marginally and the consumers will be the losers. “This scenario certainly plays to the interests of those in the media industry and copyright holders who would seek to maintain existing business models based on complete control of the content. However, it is probably the one scenario that best illustrates the chasm separating content owners/media companies from large segments of the consumer population. It is also the scenario that, if realized, would most emphatically underscore the regional differences in intellectual property laws and enforcement. “ [Berkman2003]

3. *The effective technology defence scenario* assumptions are that content will be distributed physically and digitally. Content is copy protected while still meeting consumers’ needs. It also includes the assumption that copy-protection is an ongoing cycle, which is indeed the case. “This scenario can be described as “technology rescues the content industries from wanton copyright piracy.” However, the technological challenges are compounded by the numbers of increasingly tech-savvy consumers around the world. There is very little margin for error and the transition to universal copy protection must be relatively quick. Otherwise, media companies and artists may find that large numbers of consumers are seeking digital content from sources other than traditional music labels, movie studios and publishers.” [Berkman2003]

   The difference between this scenario and the second scenario is that the second scenario assumes legal reforms while the third scenario assumes technological changes.[56]

4. *The compulsory license scenario* assumes that the current copyright system is replaced by a system in which the creators and producers of content are compensated by the government in proportion to the “consumption” frequency. “While this scenario has its own risks—giving a government entity significant discretionary power and assuring the virtual annihilation of the

[55] One example is the success of VHS against Betamax or Video 2000 although VHS was inferior against its competitors.

[56] Although the second and the third scenarios are linked due to the results, the difference is in how rights are established and enforced.

physical retail market—the potential for reducing litigation, lowering the costs of enforcement and eliminating the incentive for an ongoing encryption "arms race" make it very attractive." [Berkman2003]

5. *The utility model scenario* considers digital content as a public utility. Regulations are enforced by a federal regulatory body. Concerning the estimated effects this scenario is most interesting. "Of all five scenarios presented here, this one countenances major legal, business and consumer behaviour changes. From a technology perspective, it is less complicated than might be considered. At least one technology provider currently has an offering that could track content distribution to the end user in much the same way power companies use meter-reading systems. However, music and movie producers and their businesses—not to mention conventional retail distribution entities—will be violently opposed. Music and movie producers would see their revenue models altered greatly, with the costs associated with distributing content and usage eliminated." [Berkman2003]

Thus the "utility model scenario" might be the best solution to the current problem of the content owner. But before such a final solution is publicly accepted and established, content providers have to find their individual solutions.

9.2. The evolution of P2P networks

P2P technology is constantly evolving. Thus, it is interesting to see what will be the next step in this evolution. Researcher from Microsoft expect that "interconnected small world darknets" [DarkNet2003] will come into existence. In this network type small groups of people exchange content within. The different groups are connected through people being a member of several groups. Due to the structure it is very difficult to control and therefore to stop exchange within it.

This trend is already indicated through communities like Friendster [Friendster2004]. This is already discussed in [Roettgers2004]. Communities were part of Napster. Current P2P rather satisfy the users' need for anonymity due to the legal pressure. "The Free Network Project" is probably the P2P-network addressing this need best [FreeNet2004]. It "is entirely decentralized and publishers and consumers of information are anonymous. Without anonymity there can never be true freedom of speech, and without decentralization the network will be vulnerable to attack." Although its intended aim is to stop censorship it can also be misused for illegal content exchange. This is in contradiction to the trust-based communities like Friendster. Incorporating trusted communities in P2P networks will result in "social P2P networks". They will exist in parallel to the anonymous P2P networks.

Besides legal measures and court trials, the evolution of P2P technology also resulted in the evolution of technology, which can be used as countermeasures against illegal distribution. One popular approach is the introduction of wrong or manipulated files in the P2P-networks. Fingerprinting solutions are used in commercial and educational environments as well as in the P2P-networks, e.g. in Napster. Also, the Internet traffic is statistically analyzed to identify potential P2P-applications.

Instead of fighting P2P-networks, advantages are more and more realized. For example, P2P networks can be used for promotion of new material. Additionally P2P-networks are a distribution channel as recently used by George Michael. Furthermore, content is exchanged between people. Statistical analysis can be performed on this exchange with the aim to identify new trends in music as done by Big Champagne [BigChampagne2004].

9.3. The analogue hole

DRM developments aim at trusted systems: Systems that cannot be "manipulated" by users. But there is a general flaw in trying to protect content: the analogue hole. There must be a version of the content that can be accessed by humans: Images and videos are visualized and audio is played. The resulting signal, which is intended for human spectators or listeners, can also be recorded in a digital format again. In this case, watermarking – if it is sufficiently robust – presents the only possibility to trace back the origin of the leakage. This might not be possible somewhere in the future, when electrodes directly stimulate the brain. But in the meantime an analog signal has to be presented to the ears or the eyes.

There are already companies trying to address exactly this problem. E.g. DarkNoiseTechnologies[57] tries to insert a "dark noise" [BlackNoise2004] in the signal with the aim that recorded versions of the signal suffer severe distortions.

9.4. Examples for Music Distribution

Within this document we provided an overview about the technological aspects of protection. As already addressed in the introduction in chapter 2.4, protection solutions have to form a unity with other technologies, e.g. CMS or CRMS, in distribution systems. Different online music distribution services are described in [MN_DCM], including Apple iTunes MusicStore and Real Networks RealPlayer Music Store. Microsoft's Music Store launched (the beta version of) its MSN Music Store at the beginning of September 2004.

9.4.1. Apple iTunes MusicStore

Apple iTunes Music Store was already described in [Lenzi2003]. Here we summarise again the protection issues:

- AAC: Songs are compressed in the new AAC format (Advanced Audio Coding, a big part of the MPEG-4 specification). It uses a 128 kbps bitrate and the resulted music files have a quality that can be compared with 160 kbps MP3 compressed files. AAC files are stated to rival CDs[58].
- Direct connection: online transactions are protected by encryption software.
- Authorisation: users can play the purchased music on up to three computers, enjoy unlimited synching with their iPods, burn unlimited CDs of individual songs and burn unchanged playlists up to 10 times each. Before listening the purchased music, the computer has to be authorised to play it: this happens the first time the account is configured or as soon as the bought track is played. This authorisation can be set up to three computers, and can be removed.
  If user's computer is connected to a local network, the purchased music can be shared with other five computers. Vice versa, user can set preferences to search for shared music.

Apple hasn't licensed their technology to any other company, yet. It seems that Apple wants to protect its marketing position. Some analysts consider this as repetition of a mistake Apple made years ago with their computer solutions, which mainly lead to Apple's weak position in the computer sector. Despite of Apples ambition RealNetworks was able to analyse the protocol between the iPod and the iTunes-Software.[59] Apple compared RealNetworks procedure with Hackers' methods [Harmony2004] (see also below at RealNetworks Music Store).

9.4.2. Real Networks RealPlayer Music Store

RealNetwork itself has developed its Helix DNA platform [Helix2004], which consists of several parts:

- Helix DNA Player (Client)
- Helix DNA Producer
- Helix DNA Server
- RealAudio and RealVideo codecs

Interestingly RealNetworks didn't limit its efforts on the development of a platform independent DRM system but also developed a technology for the "translation" of content between previously incompatible DRM systems, called Harmony [Harmony]. Harmony does not unlock content so it doesn't interfere with the DMCA. Musical content from RealNetworks can be transferred to iPod's and to Microsoft's WMA format. RealNetwork's aim of device independent content has come closer. Consumers will welcome this

[57] DarkNoiseTechnologies was bought by SunnComm (http://www.sunncomm.com).

[58] Although the quality improvement from MP3 to AAC can not be neglected, different analyses show that both formats can be distinguished from CD if bitrates up to 192kbps are used as encoding parameter.

[59] RealNetworks entitled this procedure as a "Clean Room" analysis that neither requires access to source code nor reverse engineering of it. RealNetworks already acquired WMA compatibility by the same procedure.

property – maybe as much as they will welcome the recently announced temporary price reduction to 49 cents per song download and 4.99 US-$ per album download, which is also a direct attack to Apple.

9.4.3. Microsoft Music Store

So far Microsoft only had cooperation with OD2. Microsoft Music Store is expected to have the same price structure as Apple iTunes MusicStore. However, this was before Real Networks reduction of the prices. In Microsoft Music Store users will experience increased interactivity comparable to the services in Amazon’s website. This will include recommendations, play lists, as well as chat possibilities. Microsoft expects that its portal MSN with 350 million visitors. Compatibility with more than 50 different portable players is expected. Further support will come from Philips and Samsung that will release devices capable of playing Microsoft’s file format and probably compatible to Microsoft’s DRM system Janus [Janus2004] within the next months.

At the time of writing this report, only few official information about Janus was available from Microsoft [Cohen2004]. According to different news, web-connected consumer devices can buy content directly without being plugged into a PC, which is a significant extension. However, only Microsoft’s Advanced Systems Format (ASF) [ASF2004] will be supported. Janus is based on a secure time stamp, which requires a tamper-resistant real-time clock and system-specific ID (or serial number). Additional security has to be provided to secure system buses and storage. The exchange via USB 2.0 is defined in the Media Transfer Protocol (MTP). MTP is a superset of the Picture Transfer Protocol (PTP), which is widely used for exchanging content with digital cameras. Janus will be part of Windows Media DRM 10 for Portable Devices.

9.5. Summary

In spite of all efforts the current situation is controversial: From a consumers perspective any usage restriction reduces the contents value. From a content owners perspective digital content cannot be distributed without any protection. Hence, a compromise must be found between the consumers and the content owners. So far DRM is not generally accepted.

Nevertheless, DRM has the potential to be part of this compromise. For example the versioning as identified in [Bomsel04] provides interesting opportunities. However, the content owners have to be aware that the new possibilities in usage control, which are offered by DRM, are neither wanted nor enjoyed by customers today. This might change but so far this cannot be foreseen.

Thus, each content owner has to perform an objective analysis on the individual DRM usage. This analysis has to consider his needs and the needs and the requirements of the customers as well. Only by this, realistic opportunities can be identified in contrast to the hopes and expectations that were initially created by technology developers. Only then, DRM has realistic chances to be a valuable technology.

Interestingly, technology is often used in different ways as initially intended by its developers. The potentials and the future usage of DRM might also be different from its initial intensions. Thus, it is also interesting to analyse new application scenarios initially not covered by DRM technology.

1. Appendix: Acrynoms

3DES	Triples DES (see below)
AES	Advanced Encryption Standard
AFS	Advanced System Format
ASCAP	The American Society of Authors, Composers, and Publishers
BMI	Broadcast Music International
CCC	Copy Clearance Center
CD	Compact Disk
CMS	Content Management System
DMCA	Digital Millennium Copyright Act
DES	Data Encryption Standard
DRM	Digital Rights Management
DVD	Digital Versatile Disk
HFA	Harry Fox Agency
IDEA	International Data Encryption Algorithm
IBM	International Business Machines
<indecs>	interoperability of data in e-commerce systems
IPR	Intellectual Property Rights
ISP	Internet Service Provider
LP	Long Playing vinyl disc
MC	Music Cassette
MPAA	Motion Picture Association of America
MSN	Microsoft Network
MTP	Media Transfer Protocol
NASA	National Aeronautics and Space Administration
NIST	National Institute of Standards and Technology
NMPA	National Music Publishers Association
OMA	Open mobile Alliance
ORM	old rights management
P2P	Peer-To-Peer (Networks)
PTP	Picture Transfer Protocol
RIAA	Recording Industry Association of America
SESAC	Performing Rights Organization For Songwriters and Publishers
SSL	Secure Sockets Layer
VHS	Video Home System
VCR	Video Cassette Recorder
WLAN	Wireless Local Area Network

2. Appendix: Further related European projects

Below is a short overview of relevant national and international projects and research. A complete list can be found in the MUSICNETWORK deliverable DE4.4.2 – Distribution Of Coded Music.

2.1. AXMEDIS

“Automating Production of Cross Media Content for Multi-channel Distribution”

”The AXMEDIS consortium (consisting of leading European digital content producers, integrators, aggregators, and distributors; and also information technology companies and research groups) is to create the AXMEDIS framework to provide innovative methods and tools to speed up and optimise content production and distribution, up to the production-on-demand capability, for leisure, entertainment and digital content valorisation and exploitation in general. AXMEDIS format can include any other digital formats and will exploit and improve other formats such as MPEG-4, MPEG-7, MPEG-21, as well as other de facto standards.”

http://www.axmedis.org/

2.2. EUAIN

The EUAIN project (European Accessible Information Network) is funded by the eInclusion thread of the European Commission 6th framework IST programme and co-ordinated by FNB Amsterdam. EUAIN aims to promote e-Inclusion as a core horizontal building block in the establishment of the Information Society by creating a European Accessible Information Network to bring together the different actors in the content creation and publishing indus-tries around a common set of objectives relating to the provision of accessible information. Accessibility for print im-paired people can be an increasingly integrated component of the document management and publishing process and should not be a specialised, additional service.

EUAIN will take the broadest definition of content creators and will provide the support, tools and expertise to en-able them to provide accessible information. This is now feasible due to recent developments at several levels. From a technical perspective, it is now possible to address key concerns of content creators and providers and coherently address issues such as: automation of document structuring, adherence to emerging standards, workflow support, digital rights management and secure distribution platforms.

http://www.euain.org/

2.3. HARMONICA

The HARMONICA project was an accompanying action on Music Information in Libraries under the TAP Libraries Programme. FNB co-ordinated this important music project and aimed to provide a solid strategic framework for networked access to music and related multimedia services, including technologies, existing and emerging standards, exploration of network options and improved interfaces.

The last HARMONICA Forum was held in Rome in May 1999. The project ran for three years between 1997 and 2000.

HARMONICA set out to improve access to music collections in libraries of different types, taking into account the needs of various groups of users in the evolving world of networked information and multimedia. By bringing together all interested parties through forums, studies and surveys, the project aimed to achieve consensus on the areas and topics to be developed for both the users and producers of music.

The Accompanying Action was focussed on libraries. There have been many fascinating areas of concern, especially as the technology has been developing so rapidly during the lifetime of the project, which could have been pursued in more detail under other sorts of projects. The interests represented in the project and the objectives agreed with the Commission have been broad and not always easy to reconcile with each other. The central role of the library, be it national or local, public or academic, information centre or archive, has been maintained.

http://projects.fnb.nl/harmonica/default.htm

2.4. INDICARE

"The INformed DIalogue about Consumer Acceptability of DRM Solutions in Europe"

http://www.indicare.org/

2.5. TIRAMISU

"The TIRAMISU (The Innovative Rights and Access Management Inter-platform Solution) project addresses the problem of creation, delivery and consumption of audio-visual media across a wide range of hybrid networks and platforms, where security issues, such as intellectual property rights protection, privacy, access rights and transaction tracing are of major concern. The objective of TIRAMISU is to unleash the full potential of digital media, addressing the complete consumption chain - media creation, delivery and consumption, while removing the Digital Rights Management (DRM) barrier."

http://www.tiramisu-project.org

2.6. WEDELMUSIC

WEDELMUSIC is an innovative idea to allow the distribution and sharing of interactive music via Internet totally respecting the publisher rights and protecting them from copyright violation.
WEDELMUSIC allows content distributor (publishers, archives, etc.), corporate consumers (theatres, orchestras, music schools, libraries, music shops), and users (students, musicians, etc.) to manage interactive multimedia music in WEDELMUSIC XML format.
WEDELMUSIC objects may include: multilingual cataloguing information, music notation scores, audio files (e.g., WAVE, MP3, MIDI), image of music scores (PNG, TIF, PDF, etc.), multilingual lyric (XML), video files (MPEG, AVI, MOV, QT, etc.), documents (DOC, HTML, XLS, PDF, PS, etc.), pictorial images (TIFF, GIF, PNG, JPEG, BMP, etc.), animations and sliding show (FLASH, PPT, etc.), synchronizations, etc., in any format.
WEDELMUSIC solution presents:

- reliable mechanisms for protecting multimedia content and Digital Right Management,
- tools for automatic building, converting, and storing, digital musical content,
- a unified XML-based format for modeling music including audio, symbolic, image, document, etc.,
- tools for distributing, sharing digital content according to several business and transaction models.

Any content, any where under WEDELMUSIC Digital Right Management and control
To distribute, share and receive music in symbolic format also allows to commercially exploit new functionalities for music consumers and, thus, it allows the opening of a new market for several specific applications: sharing of multimedia music objects among archives, librarires, publishers, music groups, etc.

http://www.wedelmusic.org/

3. Appendix: Standardization activities

In addition to the previously mentioned standardization activities on content identification and rights management several other organizations or standards exist. A more detailed list can be found in [NIST500-241], [EICTA] or in [CEN/ISSS2003].

3.1.1. CEN/ISSS

The European Committee for Standardization (*Comite Europeen de Normalisation*) [CEN/ISSS] develops European technical standards. CEN/ISSS set up a group to examine the standardization aspects of technologies for DRM (CEN/ISSS DRM Group) in October 2001. The final report is available at [CEN/ISSS2003].

3.1.2. CORAL

“The Coral Consortium is “a cross-industry group to promote interoperability between digital rights management (DRM) technologies used in the consumer media market. The Consortium's goal is to create a common technology framework for content, device, and service providers, regardless of the DRM technologies they use. This open technology framework will enable a simple and consistent digital entertainment experience for consumers.” [CORAL]

3.1.3. CRF

The *Content Reference Forum* [CRF] is a recently formed standards group of technology and content-related companies. It‘s aim is to develop a universal way to distribute digital content across various media and geographies (“a dynamic marketplace where participants can promote, sell and legitimately share content; consumers can get the right content for their location, platform and preferences; and the underlying commercial agreements and rights surrounding the content are respected”). “Founding and current member companies of the Content Reference Forum are ARM, Ltd., ContentGuard Inc., Macrovision Corporation, Microsoft Corporation, Nippon Telegraph and Telephone Corporation, Universal Music Group and VeriSign, Inc.”

3.1.4. DMP

The *Digital Media Project* [DMP] was launched by Leonardo Chiariglione. Its aims are published in the Digital Media Manifest (DMM): “The Digital Media Manifesto identifies the need for coordinated policy and technical actions needed to achieve this fuller realisation of Digital Media. The policy actions include reviewing the Digital Media standardisation process. The technical actions require, as explicit critical success factors, the development of specifications for interoperable Digital Rights Management (DRM) platforms technically open to value-chain players and for interoperable end-user devices, and the development of recommended practices for end-to-end conformance assessment.”

3.1.5. IETF

The *Internet Engineering Task Force* [IETF] has a specialized DRM group. This Internet Digital Rights Management Group (IDRM) was concluded. Besides IDRM other groups deals or dealt with DRM related aspects. Among these groups are Group Domain of Interpretation rekey protocol (GDOI) and Multimedia Internet KEYing (MIKEY) within the Multicast Security (MSEC) working group. Also the working group Intellectual Property Rights (IPR) is dealing with a DRM related activity.

3.1.6. IFPI

IFPI represents the international recording industry and is closely related to RIAA. As it fights piracy it is in favour of DRM technologies (cfg. [IFPI]).

3.1.7. ISMA

The *Internet Streaming Media Alliance* [ISMA] wants to accelerate the adoption of open standards for streaming media types over the Internet. These standards are also addressing protection issues. Therefore it released a content protection specification for peer review, which is based on open standards and technology. It is build upon the general ISMA version 1.0 specification.

3.1.8. MPEG

The *Motion Picture Expert Group* [MPEG] is an ISO/IEC working group for standards developments of coded representations of digital audio and video. Several specifications are directly or indirectly addressing the area of DRM, like MPEG-4 IPMP (intellectual property management and protection), MPEG-7 (content description) or MPEG-21 (multimedia framework).

3.1.9. OMA

The Open Mobile Alliance [OMA] is “to facilitate global user adoption of mobile data services by specifying market driven mobile service enablers that ensure service interoperability across devices, geographies, service providers, operators, and networks, while allowing businesses to compete through innovation and differentiation”.

3.1.10. RIAA

The *Recording Industry Association of America* [RIAA] also is strongly involved in anti-piracy activities. Four specific categories of piracy are addressed: pirate recordings, counterfeit recordings, bootleg recordings and online piracy. Thus DRM is also related to RIAA.

3.1.11. SDMI

The *Secure Digital Music Initiative* [SDMI] is a forum with the aim to develop an open technology for the protection of digital music. Due to several reasons SDMI can be considered as a failure. A very interesting cause for the reasons was the public challenge on the protection system and the strong limitations and restrictions not only on the achieved results but also on the information about the deployed technology. This shows once more, that security cannot be achieved by obscurity.

3.1.12. W3C

The *World Wide Web Consortium* [W3C] held a workshop on DRM. Yet it seems that its activities slowed down. Additionally W3C is addressing related areas like within the Resource Description Framework (RDF).

3.1.13. WIPO

The *World Intellectual Property Organization* [WIPO] “is an international organization dedicated to promoting the use and protection of works of the human spirit. These works - intellectual property - are expanding the bounds of science and technology and enriching the world of the arts.”

4. Appendix: Vendor list

The following list taken from [DCITA] (with some minor modifications) collects several vendors of DRM related technologies.

Vendor Name	Country	URL	Product Name	Description	Formats	Copyright Protection	Watermarking	Interoperability
Adobe	• USA • Australian Office	http://www.adobe.com/products/contentserver/main.html	• Adobe Content Server • eBook Reader	eBook exchange, packaging and protection system. Requires eCommerce connection	Acrobat	Yes, encrypted One time URL or PDF Merchant PC specific key	Use other Windows based technologies	Open: Supports OEBF and ONIX
Aladdin Knowledge Systems	USA	http://www.ealaddin.com	Privilege Rights Manager plus HASP or eTOKEN hardware devices	Copyright protection for distributiion of software	Software applications	Privelege	–	N/A
Alchemdia	USA	http://www.alchemedia.com now: http://www.finjan.com/products/mirage.cfm	Mirage 3.1	MirageTM Enterprise 3.1 – Mirage provides Secure Display, Secure Printing and Secure Auditing! It offers control information as it is being used	Documents	Mirage	–	–
Digimarc	USA	http://www.digimarc.com	Digimarc MarcSpider® image tracking Digimarc MediaBridge™ Print to Web Watermarking Solutions	Digimarc ImageBridge watermarking enables images to carry embedded information such as image copyright notices, licensing requirements, usage restrictions, contact information and a link to a specific web page	• Gif • Jpeg • Photoshop • video	–	Digimarc MediaBridge™ Print to Web Watermarking Solutions	Market leader in watermarking
Digital Rights Exchange	• Perth • WA	http://www.dr-ex.com.au	DR-Ex Content Owner	DR-EX handles the entire DRM process for the sale of music in digital format including: • Encryption and packaging • Hosting and distribution • License control • Transaction processing • Royalty and profit distribution	Windows Media Player	Through Microsoft WMP technology	–	Microsoft based

Vendor Name	Country	URL	Product Name	Description	Formats	Copyright Protection	Watermarking	Interoperability
eMeta Corp	• USA • UK	http://www.emeta.com	eRights	eRights is a complete information commerce enterprise software solution for online content providers. It provides user authentication and access control, and drives successful strategies for the sale of content by providing the flexibility to experiment and implement extensive business and sales models	–	X	–	Little known
IBM	• USA • Australian Office	http://www-3.ibm.com/software/data/emms/features/	EMMS (Electronic Media Management System)	EMMS is a software suite of seven components that interact to provide content owners, businesses, retailers and consumers with a unique set of solutions for their digital distribution needs. These components can be purchased and integrated together to create a new EMMS value network, or purchased individually and integrated with an existing EMMS value network	–	X	Available	Supports Open standards when established
IPR Systems	Sydney, NSW	http://www.iprsystems.com	Digital Book Xchange	Provides complete bookshop and eCommerce system using Adobe Acrobat	Acrobat, Learning Objects	Currently uses Acrobat PDf Merchant but can support Content Server and Microsoft Reader	Included	Open: • Java • XML • Supports • ODRL • OEBF • ONIX
Liquid Audio	USA	http://www.liquidaudio.com	LiquidAudio SP3	Proprietary digital Music distribution and copyright protection system	–	X	–	Proprietary

Vendor Name	Country	URL	Product Name	Description	Formats	Copyright Protection	Watermarking	Interoperability
MacroVision	USA	http://www.macrovision.com	• MacroSAFE • FLEXlm • SafeAudio • SafeDisc • SafeCast	Macrovision made its name in VCR copy protection systems and now provides products for digital content	• Video • Audio • Software	X	–	Proprietary
MarkAny	Korea	http://www.markany.com/eng/default.htm	• Esignia¢ • Video MAIM 2.0 – • MarkAny Image Watermarking • DOCUMENT SAFER MAO 2.0 • MarkAny Audio Watermarking	–	• Video • Audio,	X	–	Little known
MediaSec Technologies	• Germany • USA	http://www.mediasec.com	• MediaSign™ Authentication/ Authenticity • MediaPrint™ Printed Documents • MediaBrand™ Brand protection solutions	Content and multimedia security using digital watermarking, digital labeling, self-authentication, and smart encryption technologies	• Image • Video	Yes	Yes	
Microsoft	• USA • Australian Office	http://www.microsoft.com/reader/info/sdk.asp and http://www.microsoft.com/reader/info/das.asp	• Microsoft eBook Reader • Digital Asset Server	–	Digital Books	Yes. XrML based Key and Licence Server	Use other Micorosft .net Technologies	Uses XrML and OEBF
Microsoft		http://www.microsoft.com/windows/windowsmedia/drm.asp	Windows Media Rights Manager SDK, Windows Media Format SDK	–	• Music • Video	Microsoft Multimedia Player	MMP	Emerging
OverDrive	USA	http://www.overdrive.com/serv_overview.asp	Overdrive System and Service	Provides complete bookshop and eCommerce system based around Microsoft Digital Asset Server (DRM) and Microsoft Reader services and Adobe Content Server	Digital Books	Uses Adobe and/or Microsoft	Provided	Uses XrML and OEBF

Vendor Name	Country	URL	Product Name	Description	Formats	Copyright Protection	Watermarking	Interoperability
Real Networks	• USA • Australian Office	http://www.realnetworks.com	• Helix Universal Server • Helix media Gateway • Helix Producer	Open, comprehensive platform of digital media products and applications for any format, operating system or device	Stream and cache all major media types – including: • RealAudio/ RealVideo • Apple's QuickTime • MPEG-2 • MPEG-4 • Windows Media	Helix Universal Server	Helix Universal Server	Widely supported player
Rightsmarket	Canada	http://www.rightsmarket.com	• RightsPublish • RightsVault	General (digital content publishers) (RightsPublish) and B2B (RightsVault)	–	X	X	Proprietary
Rumble Group	Sydney, NSW	http://www.rumblegroup.com	RNI Enterprise	Digital Asset Management Service with rights management within the architecture	Video, Audio and Images	Uses Intertrust	–	X
SealedMedia	• UK • USA	http://www.sealedmedia.com	SealedMedia Digital Rights Management Solution	Copyright Protection technology using special SealedMedia plug-ins	• PDF • Word • Excel • PowerPoint • HTML • GIF • JPEG • MP3 • QuickTime	–	–	X
Verance	USA	http://www.verance.com	Verance Audio and Watermarking ConfirMedia monitoring service	Broadcast Detectable video and audio watermarking	–	X	–	–

5. Appendix: Further Information Sources

5.1. ACTeN

"ACTeN is a EU-funded thematic network with a total volume of 1 Mio. Euro for two years (September 2002 - August 2004). It is part of the EU Programme "Information Society Technologies" (IST) which is a single, integrated research programme promoting a user-friendly information society.

In ACTeN, 11 partners from 10 countries cooperate to build an enlarged business and industry community in the area of multimedia technologies and e-content applications and tools. With this, ACTeN provides an East-West collaboration by addressing the opportunities and challenges of the enlargement of the EU towards Central and Eastern Europe."

http://www.acten.net

5.2. BEUC – The European Consumers' Organisation

"BEUC, the European Consumers' Organisation, is the Brussels based federation of 38 independent national consumer organisations from the EU, accession and EEA countries. Our job is to try to influence, in the consumer interest, the development of EU policy and to promote and defend the interests of all European consumers.

The activities of BEUC are financed mainly by contributions from our member organisations. We also receive financial support from the European Commission under the general framework programme for financing activities in favour of consumers."

http://www.beuc.org/

5.3. Content Village

"The Content Village is an Accompanying Measure funded under the European Community "eContent" programme - a market oriented programme which aims to support the production, use and distribution of European digital content and to promote linguistic and cultural diversity on the global networks.

The overall objective of this non-profit service is to disseminate and promote existing best practice and results of the eContent programme to all interested parties in the digital content and language industry, and the public sector."

http://www.content-village.org/

5.4. DRM Watch

"DRM Watch analyzes the latest developments in the emerging field of Digital Rights Management. Our goal is to help IT managers be prepared to make decisions that will affect the intellectual property of their corporations."

http://www.drmwatch.com/

5.5. eContent

"eContent is a market oriented programme which aims to support the production, use and distribution of European digital content and to promote linguistic and cultural diversity on the global networks."

http://www.cordis.lu/econtent/

5.6. eEurope - High Level Group on Digital Rights Management

“The establishment of a High Level Group to address current issues arising from Digital Rights Management (DRM) was announced by the Commission in its Communication "Connecting Europe at high speed: recent developments in the sector of electronic communications", adopted on 3 February 2004.”

http://www.europa.eu.int/information_society/eeurope/2005/all_about/digital_rights_man/high_level_group/index_en.htm

5.7. European Digital Rights (EDRI)

“European Digital Rights was founded in June 2002. Currently 17 privacy and civil rights organisations from 11 different countries in Europe have EDRI membership. Members of European Digital Rights have joined forces to defend civil rights in the information society. The need for cooperation among European organizations is increasing as more regulation regarding the internet, copyright and privacy is originating from the European Union.”

http://www.edri.org/

5.8. Rightscom News Briefing

“Rightscom is a consultancy that specialises in the provision of solutions for the management, trading and protection of intellectual property rights and digital content in the network environment.”

http://www.rightscom.com/

5.9. The Register

“Offers news, views, opinions and reviews on what's latest in the IT industry.”

http://www.theregister.co.uk/internet/rights/

6. Appendix: Bibliography

[ALA2005] American Library Association, “Digital Rights Management and Libraries”, May, 2005, http://www.ala.org/ala/washoff/WOissues/copyrightb/digitalrights/digitalrightsmanagement.htm

[Alliance] Alliance Entertainment, http://www.aent.com/

[Anderson2003] Ross Anderson, “Trusted Computing – Frequently Asked Questions”, 2003, http://www.cl.cam.ac.uk/~rja14/tcpa-faq.html

[Anderson2004] Ross Anderson, “Economics for Information Security”, 2004, http://www.cl.cam.ac.uk/~rja14/#Econ

[Arnold2003] Michael Arnold, Martin Schmucker, Stephen Wolthusen, “Techniques and Applications of Digital Watermarking and Content Protection”, Artech House, 2003

[ArtistPro] Music Copyright, Business and Legal Issues (Forum), http://www.artistpro.com/index.php?name=PNphpBB2&file=viewforum&f=12&sid=a3c7133cbb6bd7b9064fe3416763b79c

[ASF2004] Specification, Revision 01.20.02, Microsoft Corporation, June, 2004

[AudioID] E. Allamanche, J. Herre, O. Hellmuth, B. Froba, and M. Cremer, "AudioID: Toward content-based identification of audio material," in Proc. 110th AES, Amsterdam, The Netherlands, 2001.

[AXMEDIS] http://www.axmedis.org

[BBC] British Broadcasting Cooporation, http://www.bbc.co.uk

[Bechtold2002b] Stefan Bechtold, “Vom Urheber- zum Informationsrecht --- Implikationen des Digital Rights Management, Verlag C.H. Beck, München, Germany, 2002.

[Berkman2003] Five Scenarios for Digital Media in a Post-Napster World, http://cyber.law.harvard.edu/publications

[BigChampagne2004] Big Champagne, http://www.bigchampagne.com/

[BlackNoise2004] Gary Andersen-Jones, “PLUGGING THE ANALOGUE HOLE - How Q-Spoiler™ closes the remaining music anti-piracy gap”, DNT Whitepaper, DarkNoiseTechnologies, Autumn 2003, http://www.2and2.net/Uploads/Documents/DarkNoiseWhitePaper.pdf

[Bockstedt2005] Jesse C. Bockstedt, Robert J. Kauffman and Frederick J. Riggins, “The Move To Artist-Led Online Music Distribution: Explaining Structural Changes In The Digital Music Market”, Proceedings of the 38th Hawaii International Conference on System Sciences, 2005, http://misrc.umn.edu/workingpapers/fullpapers/2004/0422_091204.pdf

[Bomsel04] Olivier Bomsel, Anne Gaelle Geffroy, “Economic Analysis of Digital Rights Management Systems (DRMs)”, MediaNet Project Paper, December, 2004, http://www.cerna.ensmp.fr/Documents/OB-AGG-EtudeDRM.pdf

[Booch1986] Grady Booch, “Object-Oriented Development”, IEEE Trans. Software Eng. 12(2), 1986

[Buente04] Oliver Bünte, Heimgezahlt – Paymentsysteme im Einsatz, c’t 2004, Heft 3, 26. Januar

[C4MusicLibrarians] Copyright For Music Librarians, Music Library Association, *http://www.musiclibraryassoc.org/Copyright/copyhome.htm and* http://www.lib.jmu.edu/org/mla/

[Camp2003] L. Jean Camp: First Principles of Copyright for DRM Design. IEEE Internet Computing 7(3), 2003

[Cano2002] Pedro Cano, Eloi Baltle, Ton Kalker, Jaap Haitsma: A review of algorithms for audio fingerprinting, IEEE Workshop on Multimedia Signal Processing, 2002

[CC] creative commons, http://creativecommons.org/

[CEN/ISSS] Information Society Standardisation System, http://www.cenorm.be/isss

[CEN/ISSS2003] CEN/ISSS “Digital Rights Management-Final Report”, October, 2003, http://www.cenorm.be/isss

[Certimark] Certimark – Certification Of Watermarking Techniques, http://www.certimark.org

[CGov] United States Copyright Office, http://www.copyright.gov/

[CGuru] Copyright Guru, http://www.copyrightguru.com/

[CInMusic] Copyright In Music http://www.sls.lib.il.us/reference/workshop/suite6.html

[CIssue] Copyright Issues for Music, Music Library, University at Buffalo, http://ublib.buffalo.edu/libraries/units/music/copyright.html

[CMyths] Brad Templeton, 10 Big Myths About Copyright explained, http://www.templetons.com/brad/copymyths.html

[Cohen2002] Julie E. Cohnen, “DRM and Privacy”, 2002 Research Paper Series, Research Paper No. 372741 Georgetown University Law Center, 2002, http://ssrn.com/abstract_id=372741

[Cohen2004] Josh Cohen, “A General Overview of Two New Technologies for Playing Protected Content on Portable or Networked Devices”, Whitepaper, Microsoft Corporation, June 2004

[Cox2002] Ingemar J. Cox, Matthew L. Miller, and Jeffrey A. Bloom. “Digital Watermarking”. The Morgan Kaufmann Series in Multimedia Information and Systems. Morgan Kaufmann Publishers, San Francisco, CA, USA, 2002.

[ContentGuard] Content Guard, http://www.contentguard.com

[CORAL] Coral Consortium, http://www.coral-interop.org/

[CoverPages] Cover Pages (hosted by OASIS), “XML and Digital Rights Management (DRM)” http://xml.coverpages.org/drm.html

[CPrimer] Copyright primer on Computer music files, http://www.reach.net/~scherer/p/copyrit1.htm

[Craver2001] Scott A. Craver, Min Wu, Bede Liu, Adam Stubblefield, Ben Swartzlander, Dan S. Wallach, Drew Dean, and Edward W. Felten. “Reading Between the Lines: Lessons from the SDMI Challenge”, Proceedings of the 10th USENIX Security Symposium, Washington D.C., USA, August 2001.

[CRF] Content Reference Forum, http://www.crforum.org/

[CRN2004] “Microsoft Shelves NGSCB Project As NX Moves To Center Stage”, CRN, http://www.crn.com/sections/breakingnews/dailyarchives.jhtml?articleId=18841713

[DarkNet2003] *P. Biddle, P. England, M. Peinado, and B. Willman (Microsoft Corporation),* “The darknet and the future of content distribution”, 2002 ACM Workshop on Digital Rights Management, http://crypto.stanford.edu/DRM2002/darknet5.doc

[DCMI] Dublin Core Meta Data Initiative, http://dublincore.org/

[DCITA] A Guide To Digital Rights Management, DRM vendor spreadsheet, http://www.dcita.gov.au/drm/

[DDB] The collection mandate of Die Deutsche Bank, http://www.ddb.de/wir/sammelauftr_e.htm

[DE4.2.1] The Interactive Musicnetwork, DE4.2.1: “Music Representation for Music Libraries”, February, 2004

[DE4.3.1] The Interactive Musicnetwork, DE4.3.1: “Multimedia Standards for Music Encoding”, February, 2004

[DOI2003] Digital Object Identifier System, http://www.doi.org/index.html

[DOI2003b] “Resolve A DOI”, http://dx.doi.org/

[DOI2003c] “CNRI Handle System Resolver”, http://www.handle.net/resolver/

[DMM] Leonardo Chiariglione, “The Digital Media Manifesto”, http://www.dmpf.org/manifesto/dmm.htm

[DMP] The Digital Media Project, http://www.chiariglione.org/oldfiles/project/index.htm

[DMP_SPEC] “Interoperable DRM Platform specification”, http://www.dmpf.org/

[DPRL] “The Digital Property Rights Language – Manual And Tutorial”, Version 2.00, November, 1998, http://xml.coverpages.org/DPRLmanual-XML2.html

[DPRL98] John Erickson, “Xerox DPRL and Rights Metadata”, 1998, http://xml.coverpages.org/jericksonDPRL1998.html

[DPRL2001] Digital Property Rights Language (DPRL) , Technical Report, June 20, 2001, http://www.oasis-open.org/cover/dprl.html

[DRM2003] Bill Rosenblatt, “2003 in Review: DRM Standards”, January 5, 2004, http://www.drmwatch.com/standards/article.php/3295291

[DT2004] Magali Dubosson-Torbay and Yves Pigneur and Jean-Claude Usunier, “Business Models for Music Distribution after the P2P Revolution”, WEDELMUSIC '04: Proceedings of the Web Delivering of Music, Fourth International Conference on Web Delivery Of Music, IEEE Computer Society, Washington, DC, USA, 2004

[EBU] European Broadcasting Union, http://www.ebu.ch

[EBUPMeta] European Broadcasting Union, PMC Project P/Meta, http://www.ebu.ch/departments/technical/pmc/pmc_meta.html

[EDItEUR] EDItEUR, http://www.editeur.org/

[EICTA] European Industry Association, “Standards initiatives”, http://www.eicta.org/levies/resources/legalresources.html

[EFF2004] Electronic Frontier Foundation (EFF), http://www.eff.org/

[EFFOAL] Electronic Frontier Foundation (EFF) - Open Audio License, http://www.eff.org/IP/Open_licenses/eff_oal.html

[EUDirective] Commission Staff Working Paper, “DIGITAL RIGHTS - Background, Systems, Assessment”, SEC (2002) 197, February, 2002, Brussels

[EW2005] Jessica Rudish, “Illegal filesharing lawsuits dismissed; Emory witholds defendants' names”, The Emory Wheel Online, April 15, 2005 http://www.emorywheel.com/vnews/display.v/ART/2005/04/15/425ed47899e53

[Felten2002] E. Felten, “Statement at the fourth international information hiding workshop in Pittsburgh”, 2001, http://www.cs.princeton.edu/sip/sdmi/sdmimessage.txt

[Felten2003] E. Felten, “DRM, and the first rule of security analyis”, Freedom-To-Tinker, 2003, http://www.freedom-to-tinker.com/archives/000317.html

[Fisher2004a] William Fisher, “Promises to Keep – Technology, Law, and the Future of Entertainment”, http://www.tfisher.org/PTK.htm

[Fisher2004b] Andrew Orlowski, “Free legal downloads for 6$ a month. DRM free. The artists get paid. We explain how …”, The Register, February, 2004 http://www.theregister.co.uk/content/6/35260.html

[Freenet2004] Freenet, 2004, http://freenet.sourceforge.net/

[Friendster2004] Friendster, http://www.friendster.com/

[GAP] German Academic Publishers, http://www.gap-c.de

[Gayer] Gayer, A., and O. Shy, "Publishers, Artists, and Copyright Enforcement." 27. January, 2005, http://econ.haifa.ac.il/~ozshy/piracyconflict11.pdf

[GPL] GNU Public License, http://www.gnu.org/copyleft/gpl.html

[Grokster] Grokster, http://www.grokster.com

[Harmony] Harmony, RealNetworks, http://www.real.com/harmony

[Harmony2004] http://www.prnewswire.com/cgi-bin/stories.pl?ACCT=104&STORY=/www/story/07-29-2004/0002221065&EDATE=

[Helix2004] The Helix Community, https://helixcommunity.org/

[Huang2004] Chun-Hsiang Huang and Ja-Ling Wu, “Attacking Visible Watermarking Schemes”, IEEE Transaction on Multimedia, Vol. 6, No. 1, February 2004

[Iannella2001] R. Iannella, “Digital rights management architectures”, D-Lib Magazine 7, 6 Juni, 2001, http://webdoc.sub.gwdg.de/edoc/aw/d-lib/dlib/june01/iannella/06iannella.html

[IETF] Internet Engineering Task Force, http://www.ietf.org

[IFLA1998] IFLA Study Group on the Functional Requirements for Bibliographic Records, "functional requirements for bibliographic records", K . G. Saur München, 1998, http://www.ifla.org/VII/s13/frbr/frbr.htm

[IFPI] IFPI, http://www.ifpi.org

[IMS] IMS Global Learning Consortium Inc., http://www.imsproject.org/metadata/

[indecs] <indecs> Framework Ltd, http://www.indecs.org/

[IRL1736] Network Working Group, “RFC 1736: Functional Recommendations for Internet Resource Locators”, The Internet Society, 1995, http://www.ietf.org/rfc/rfc1736.txt

[ISBN2003] International ISBN Agency, http://isbn-international.org/

[ISBN2003b] International Standard Book Number, http://www.isbn.org

[ISBN2003c] ISO Project 2108 on revision of the International Standard Book Number (ISBN), „Frequently Asked Questions about changes to the ISBN“, http://www.nlc-bnc.ca/iso/tc46sc9/isbn.htm

[ISSN2003] International Standard Serial Number, http://www.issn.org

[ISMA] Internet Streaming Media Alliance, http://www.isma.tv/home

[ISMN2003] International Standard Music Number (ISMN) users’ manual, http://www.nlc-bnc.ca/ismn/s12-200-e.html

[ISTC] International Standard Text Code, ISO/TC 46/SC 9 WG3 Project 21047, http://www.nlc-bnc.ca/iso/tc46sc9/wg3.htm

[IWW02] “Internet-Zahlungssysteme aus Sicht der Verbraucher”, Institut für Wirtschaftspolitik und Wirtschaftsforschung (IWW), Universität Karlsruhe, February, 2002, available at: http://www.iww.uni-karlsruhe.de/izv4/Infoseiten/index.html

[IWW03] Kay Leybold und Karsten Stroborn, “Internet-Zahlungssysteme aus Sicht der Verbraucher”, Institut für Wirtschaftspolitik und Wirtschaftsforschung (IWW), Universität Karlsruhe, February, 2003, available at: http://www.iww.uni-karlsruhe.de/izv4/Infoseiten/index.html

[Janus2004] John Borland, „Microsoft unveils new antipiracy tools“, May, 3th, 2004, http://news.com.com/2100-1025_3-5203004.html

[Katzenbeisser] Stefan Katzenbeisser and Fabien A. P. Petitcolas, editors. “Information Hiding: Techniques for Steganography and Digital Watermarking”. Artech House, Boston, MA, USA, 2000

[Kerkhoff1883] Auguste Kerkhoffs. “La Cryptographie Militaire”. Journal des Sciences Militaires, 9th series:5-38,161-191, January February 1883

[Kretschmer] Martin Kretschmer , “Artists’ earnings and copyright: A review of British and German music industry data in the context of digital technologies”, First Monday, volume 10, number 1 (January 2005), http://firstmonday.org/issues/issue10_1/kretschmer/index.html

[LWDRM] Light Weight Digital Rights Management, http://www.lwdrm.com/

[Lenzi2003] Riccardo Lenzi, Martin Schmucker and Francesco Spadoni: “Apple iTunes Music Store”, Technical Report, Interactive MusicNetwork, June, 2003

[Lewis2003] Dr. Gerard J. Lewis, “The German E-music Industry”, Leonardo de Vinci, Faculty of Business Administration, European Union, December 2003, University of Applied Sciences, Dresden, Germany, http://imec.hud.ac.uk/imec/iMEC%20GermanFINALreport110902.pdf

[MacroVision] Video Copy Protection, Macrovision, http://www.macrovision.com/products/video/index.shtml

[Marion1998] Ann Marion and Elizabeth H. Hacking, “Educational Publishing and the World Wide Web”, Journal of Interactive Media in Education, 98 (2), 1998, http://www-jime.open.ac.uk/98/2

[MC] RIAA crackdown shows signs of success, 2005, http://www.managementconsultancy.co.uk/news/it/1151791

[MCTable] Music Copyrights Table, http://www.tomwbell.com/teaching/Music(C)s.html

[MD5Attack] Xiaoyun Wang and Dengguo Feng and Xuejia Lai and Hongbo Yu, “Collisions for Hash Functions MD4, MD5, HAVAL-128 and RIPEMD”, Cryptology ePrint Archive, Report 2004/199, 2004, http://eprint.iacr.org/2004/199

[MDRG] “Meta Data Reference Guide”, MIT Libraries, http://libraries.mit.edu/guides/subjects/metadata/standards.html

[Menezes96] A. Menezes, P. van Oorschot, S. Vanstone: “Handbook of Applied Cryptography”, CRC Press, 1996

[MIME1993] Network Working Group, “RFC 1521: MIME (Multipurpose Internet Mail Extensions) Part One: Mechanisms for Specifying and Describing the Format of

Internet Message Bodies", The Internet Society, 1993, http://www.ietf.org/rfc/rfc1521.txt

[MN_DCM] Francesco Spadoni, Riccardo Lenzi, Martin Schmucker: "Distribution of Coded Music", DE4.4.1, The Interactive MusicNetwork, June, 2004

[MN_ML] Bernhard Günther: "Music Coding for Music Libraries", DE4.2.1, The Interactive MusicNetwork, January, 2004

[MPAA2003] Taylor Walton, "'Golden Age of Free Music' vs 'Copying is Stealing'", 08, 2003, http://www.theregister.co.uk/content/6/32199.html

[MPEG] The MPEG Home Page, http://www.chiariglione.org/mpeg/

[MPEG4] MPEG Systems FAQ, http://www.chiariglione.org/mpeg/faq/mp4-sys/sys-faq-sys4gen.htm

[MPEG7] ISO/IEC JTC1/SC29/WG11/N523, "MPEG-7 Overview", Pattaya, March, 2003

[MPEG21] ISO/IEC JTC1/SC29/WG11/N523, "MPEG-21 Overview", Shanghai, October, 2002

[MUSICAL1.2] MUSICAL - Multimedia Streaming of Interactive Content Across mobiLe networks, "Deliverable D.1.2: Technology Requirements Specification", eContent : EDC-22131 - MUSICAL / 27193, 2002

[MusicBrainz] MusicBrainz, http://www.musicbrainz.org

[MUSICRYPT] MusicCrypt, http://www.musicrypt.com

[Music2Share] T. Kalker, D.H.J. Epema, P.H. Hartel, R.L. Lagendijk, M. van Steen, "Music2Share—Copyright-Compliant Music Sharing in P2P Systems", Proceedings of the IEEE, vol. 92, no. 6, pp. 961 - 970, 2004.

[MusicNetwork] Interactive Musicnetwork, http://www.interactivemusicnetwork.org

[MUZE] Muze, http://www.muze.com

[MVVCP] "Method and apparatus for processing a video signal so as to prohibit the making of acceptable video tape recordings thereof, Inventors: Ryan; John O. (Santa Clara, CA) Assignee: Macrovision (San Jose, CA)
Appl. No.: 724006 Filed: April 17, 1985

[Napster] Napster, http://www.napster.com/

[NapsterCases] Napster Case, http://www.riaa.com/news%5Cfilings%5Cnapster.asp

[NGSCB] Microsoft, "Next Generation Secure Computing Base" http://www.microsoft.com/resources/ngscb

[NIST500-241] Gordon E. Lyon, A Quick-Reference List of Organizations and Standards for Digital Rights Management, NIST Special Publication 500-241, http://www.itl.nist.gov/div895/docs/NIST241assm.9oct.pdf

[OAI] The Open Archive Initiative, http://www.openarchives.org/

[OAIPMH] The Open Archive Initiative Protocol for Metadata Harvesting, http://www.openarchives.org/OAI/openarchivesprotocol.htm

[OASIS] OASIS, http://www.oasis-open.org/

[OASISRLTC] OASIS Rights Language TC, http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=rights

[Odlyzko2001] Andrew Odlyzko, "Content is not king", First Monday, February 2001, http://firstmonday.org/issues/issue6_2/odlyzko/index.html

[ODRL] Open Digital Rights Language, http://www.odrl.net

[ODRLb] Open Digital Rights Language, Version 1.1, W3C, http://www.w3.org/TR/odrl/

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

[ONIX] EDItEUR ONIX for Books, http://www.editeur.org/onix.html

[ONIXb] ONIX for Books, Product Information Message, Main Series Record Format, Release 2.1 June 2003, EDitEUR

[ONIXc] ONIX for Books, Product Information Message, Main Series Record Format, Release 2.1 June 2003, EDitEUR

[Oestereich1998] Bernd Oestereich, Objektorientierte Softwareentwicklung: Analyse und Design mit der UML, 5.Auflage, Oldenbourg, 2001

[OS] Oz Shy, „Netzpiraten vs. Medienmogule - Der Nutzen von illegalen Kopien für den Künstler", WZB-Mitteilungen, Heft 107, March 2005, http://www.wz-berlin.de/publikation/pdf/wm107/26.pdf and http://www.ozshy.com/

[Potato] The Potato System, http://www.potatosystem.com/

[PEW] Mary Madden, Lee Rainie, “Music and Video Downloading Moves Beyond P2P”, Pew Internet & American Life Project, 2005, http://www.pewinternet.org/pdfs/PIP_Filesharing_March05.pdf

[Pinola] The Pianola Institute , http://www.pianola.org/

[Pinola1899] http://mmd.foxtail.com/Archives/Digests/200406/2004.06.05.03.html

[Pinola1908] U.S. Supreme Court, WHITE-SMITH MUSIC PUB. CO. v. APOLLO CO., 209 U.S. 1 (1908), 209 U.S. 1 WHITE-SMITH MUSIC PUBLISHING COMPANY, Appt., v. APOLLO COMPANY. Nos. 110, 111. Argued January 16 and 17, 1908. Decided February 24, 1908. http://caselaw.lp.findlaw.com/scripts/getcase.pl?navby=case&court=us&vol=209&page=1

[Philips] Jaap Haitsma, Michiel van der Veen, Ton Kalker, Fons Brueker, “Audio watermarking for monitoring and copy protection”, ACM Multimedia Workshops, 2000

[REGDVD] Andrew Orlowski, “French court bans DVD DRM”, The Register, 26/04/2005, http://www.theregister.co.uk/2005/04/26/french_drm_non/

[RIAA] Recording Idustry Association of America, http://www.riaa.org/

[Rosenblatt2002] B. Rosenblatt, B. Trippe, S. Mooney: Digital Rights Management – Business and Technology

[Rosenblatt2003a] Bill Rosenblatt and Gail Dykstra: Technology Integration Opportunities, http://www.drmwatch.com/resources/whitepapers/article.php/11655_3112011_3

[Rosenblatt2003b] Bill Rosenblatt and Gail Dykstra: Integrating Content Management with Digital Rights Management - Imperatives and Opportunities for Digital Content Lifecycles, GiantSteps, Media Technology Strategies , Technical Report, http://www.xrml.org/reference/CM-DRMwhitepaper.pdf

[ROSI2003] Adel Melek, “Security Return on Invest”, Partner National Leader Security Service, http://www.issa-toronto.org/FSF03/Melek/

[ROSI2003b] Scott Berinato, “Finally a return an security spending”, http://www.cio.com/archive/021502/security.html

[ROSI2003c] Return on Investment for Information Security Guideline – Summary, http://www.oit.nsw.gov.au/pages/4.3.37-ROSI.htm

[Roettgers2004] Janko Roettgers, “Social networks: The Future of P2P file sharing”, 2004 http://freebitflows.t0.or.at/f/about/roettgers

[Schneier96] Bruce Schneier, Applied Cryptography, John Wiley & Sons, 2nd Edition, 1996

[ScreenersCBS] Arrest In 'Screener' Upload Case, CBS News, OS ANGELES, Jan. 23, 2004, http://www.cbsnews.com/stories/2004/02/18/entertainment/main600881.shtml

[ScreenersFOX] FBI Arrests Internet Movie Pirate, Friday, FOX News, January 23, 2004, http://www.foxnews.com/story/0,2933,109272,00.html

[SDMI] Secure Digital Music Initiative, http://www.sdmi.org/

[SDN_CAST] Peter Rantasa, Martin Schmucker, „Ein soziales Verteilungsnetzwerk – Beispiel eines alternativen Distributionsmodells“, CAST-Workshop, February 2nd, 2005, Darmstadt, Germany

[SDN_IST] Martin Schmucker, „Enlightening the DarkNet“, IST-Workshop, November, 15th, 2004, Den Hague, Netherlands

[SHA1Attack] Xiaoyun Wang, Yiqun Lisa Yin, Hongbo Yu, “Collision Search Attacks on SHA1”, http://theory.csail.mit.edu/~yiqun/shanote.pdf

[SMC] Sheet Music Consortium, http://digital.library.ucla.edu/sheetmusic/

[SMEF] Standard Media Exchange Format, http://www.bbc.co.uk/guidelines/smef/

[SNOCAP] SNOCAP, http://www.snocap.com/

[stirmark] Fabien Peticolas, stirmark benchmark 4.0, http://www.petitcolas.net/fabien/watermarking/stirmark/

[StreamCast] StreamCast Networks, http://www.streamcastnetworks.com/

[TCFAQ] Ross Anderson, “Trusted Computing” – Frequently Asked Questions, V1.1 August, 2003, http://www.cl.cam.ac.uk/~rja14/tcpa-faq.html

[TCG] Trusted Computing Group, https://www.trustedcomputinggroup.org/home

[TCPA] Trusted Computing Platform Architecture, http://www.trustedcomputing.org/home

[TP] Ralf Grötker, Internetpiraten in der Netzwerk-Ökonomie, March, 2005 http://www.heise.de/tp/r4/html/result.xhtml?url=/tp/r4/artikel/19/19679/1.html

[UnCD] "Un-CDs, nein danke!!", heise, http://www.heise.de/ct/cd-register/

[URI2396] Network Working Group, "RFC 2396: Uniform Resource Identifiers (URI): Generic Syntax", The Internet Society, 1998, http://www.ietf.org/rfc/rfc2396.txt

[URN1737] Network Working Group, "RFC 1737: Functional Requirements for Uniform Resource Names", The Internet Society, http://www.ietf.org/rfc/rfc1737.txt

[W3C] World Wide Web Consortium, http://www.w3c.org/

[WeedShare]

[WIP2P] Wikipedia, Peer-To-Peer, http://en.wikipedia.org/wiki/Peer-to-peer

[WIPO] World Intellectual Property Organization, http://www.wipo.org/

[WIPODRM] Standing Committee on Copyright and related rights, "Current Developments in the field of Digital Rights Management", Tenth Session, Geneva, November 3 to 5, SCCR/10/2, August, 2003, Geneva

[Wobst00] Reinhard Wobst, "Abenteuer Kryptologie", Addison Wesley, 2000

[Wobst03] Reinhard Wobst, "Harte Nüsse – Verschlüsselungsverfahren und ihre Anwendungen", c't, Heise Verlag, Heft 17, 2003

[XML] eXtensible Markup Language, http://www.xml.org

[XrML] eXtensible rights Management Language,http://www.xrml.org/

[XrMLFAQ] eXtensible rights Markup Language, - Frequently Asked Questions, http://www.xrml.org/faq.asp

[XRMLSpec] extensible rights Markup Language (XrML) 2.0 Specification, ContentGuard, November 2001