Blekinge Institute of Technology
Department of Software Engineering and Computer Science
In co-operation with SonyEricsson, Lund, Sweden

DRM – Digital Rights Management

Bachelor thesis in Computer Science

Autumn - 2001

Authors: Johan Bengtsson, ia98
Emma Hansson, is98

Supervisor: Larry Henesey, Blekinge Institute of Technology

Examiner: Gouhua Bai, Blekinge Institute of Technology

Abstract

In recent years, technological developments have led to digital files being more easily distributed, for example through Napster (a file sharing service on the Internet). In order to manage and control the distribution of digital files, a new concept has been developed, called DRM (Digital Rights Management). The purpose is to set every single file with individual rights that are extremely hard to break, and consequently make people pay and use the files legally. The file will then be fully protected from intrusion and alteration until the set rights expire.

The goal of this thesis is to look into and summarise DRM of today. We have concentrated on the mobile DRM market, and especially mobile phones. Especially the solutions/applications that already exist and their functionality and properties, but also requirements regarding security levels, compatibility etc. We have also added predictions of the near future, ours as well as others.

Existing applications for DRM are well made but few are constructed for mobile phones. Mobile phones will however be a good and secure platform for DRM. At present there is no DRM application inserted in mobile phones in Europe. The third generation (3G) network will push the progress with the capability of broader bandwidth, with capacity of downloading more content to the phone.

Since the mobile phone software is embedded and the mobile phones are within a trusted network, the security level of a DRM application in a mobile phone can be discussed. A lower level of security would make it easier for managing content but also open up the market for hackers that wish to trespass. With a lower level of security you always have to consider the consequences and often it creates more problems than it solves.

We believe the DRM market and its value will increase exponentially over the next few years. The number of players on the mobile Internet DRM market will be less than on the Internet DRM market, due to the complexity of getting applications into the phone. The latter will consist of many more players, and remain fragmented, since it is an open market.

Acknowledgement

Grateful thanks are extended to our supervisor Christer Sandahl at SonyEricsson for guidance and many interesting conversations and as well to Stefan Andersson who has helped us with technical questions and constructive feedback.

We would also like to express our gratitude to our supervisor Larry Henesay and our examinator Guohua Bai at Blekinge Institute of Technology, for their support and encouragement during the process.

Also a grateful thanks to Mårten Ulfsbäck at Europolitan and Ulf Baldhagen at Tele2 for participating in our interviews, by giving us the mobile operators' point of view on DRM.

Lund, 21st of December 2001

Emma Hansson
Johan Bengtsson

Table of context

1 Introduction

1.1 Background

With the recent developments in technology, problems of different kind have appeared. With downloading speeds becoming faster and faster, more files are distributed over the Internet. It could for example be music, books, pictures, movies, or basically anything that comes in digital form. Not all of these files are currently shared legally. Usually a person, who has a license for a product, can copy and sell/give it to other people, all over the world, within minutes without too much trouble. It is hard to detect and stop these transactions.

Digital Rights Management (DRM) was introduced to stop the unwanted and uncontrolled copying of a product. The DRM technology makes the file unable to open (i.e. play) if not given the correct license template (key). You can still copy and share files with everyone, but they cannot be opened. On top of this, specific rights can be set. For example you can buy a song with the right to listen to it four times and copy it once within the next twelve days. A strange example, but the point is there are no specification limits. The International Data Corporation (IDC) group defines DRM like:

"Digital rights management (DRM): The chain of hardware and software services and technologies confining the use of digital content to authorised use and users and managing any consequences of that use throughout the entire life cycle of the content. DRM is one kind of content protection technology." [1]

1.2 Problem definition

The problem is that today there is no way to effectively stop the copying and sharing. Leading publishers, distributors etc are therefore eager to find a solution. They want to charge for distribution of the content of which they own the rights for, as well as they want to control the distribution.

Sometime during next year (2002) the new third generation (3G) network will be up and running in Sweden. This will make the mobile phones capable of more services and faster connections. The phones therefore have to be developed in order to get the capacity of handling these new possibilities.

Another problem that has been raised is to consider what level of protection that will be appropriate for mobile Internet in order to cover the demands from the content providers.

Sony Ericsson Mobile will develop new mobile phones next year compatible with the DRM technology. Which standards and functions that are to be supported have not yet been determined. There are still many questions left to be answered.

[1] IDC group report p.3

1.3 Purpose

In order to make the decisions necessary for the new phones; having the right knowledge to base them upon is vital.

The purpose of this thesis is therefore to investigate and summarise the DRM market of today. What DRM applications that exist and for what cause they have been developed.

Focus on how well DRM is suited for Internet versus the mobile Internet in mobile phones. Whether to use DRM for mobile Internet or for Internet is not a matter of a choice to be taken. This is only to investigate how appropriate it is constructed for the different platforms.

Another attempt will be to investigate what level of protection that is needed for mobile Internet or what level of protection the content providers would be satisfied with.

This will help people understand what already exists out there and how it is used, and consequently, how Sony Ericsson might use it in some way.

2 The question at issue

2.1 Hypothesis

*"**If** Mobile phone developers can develop tools to protect content **then** this will benefit providers and owners of the content!"*

2.2 Questions

1. What are the differences between mobile Internet DRM and Internet DRM?
2. How do the applications look today for DRM?
3. Is an open DRM solution sufficient for the requirements of the mobile Internet? (What level of protection is needed?)
4. How are the future aspects of the DRM development?

2.3 Limitations

We will not make our own DRM application or establish which application that is working the best today or which would suit Sony Ericsson the best.

We will not speculate in what application/ technology that would be seen as a future standard in the DRM topic.

We will not concentrate on the technologies that are used for mobile Internet or Internet.

The result of this thesis is not supposed to be an answer whether to use DRM for mobile Internet or for Internet, since it is not a choice to make for the producers. DRM is a technique that is used on both platforms.

3 Methods

3.1 Research

We have chosen to make a qualitative research since we think that these scientific methods of working will suite our thesis. The qualitative approach can be said to involve five steps[2]:

1. Deducing a hypothesis
2. Expressing the hypothesis
3. Testing the hypothesis
4. Examining the outcome
5. Eventual modification of the theory and return to the first step

The qualitative research method often start with a very vague idea of the theory and examine the practical world to understand and further develop the theory.

The focus will not only be on our hypothesis but also on the questions and these components together will be the foundation of the research. We have used the questions to make the hypothesis clearer.

Our hypothesis will be tested through observations, case studies and interviews. The observations and case studies will be made through exploring existing DRM application and concepts. The application case study will be of great help when to test our hypothesis and will also be a good ground for our analysis.
The literature will be of help mainly when to understand the background of the problem but also when to study the vendors interested in DRM.

3.1.1 Literature

DRM is a relatively new topic and there is little information concerning it. There are few books that are supporting the subject. Most of the books that are available concerning this topic are the ones regarding the techniques that DRM is built on. Since the newest information and technologies are found easily on the Internet and in reports, the short supply of books has not been worrying.

[2] Reliability and confirmability of Qualitative research. P.2-3

The literature we have used is as follows:

- Report from International Data Corporation (IDC) group
- Internal reports from Ericsson
- Specifications of different techniques
- Internet
- Articles
- Books

We have been in contact with Ericsson employees who have expertise and knowledge about DRM and different technologies concerning DRM. We have had various meetings with these persons during the process.

These persons are:

- Christer Sandahl, Technical Section Manager, System Management for Open Execution Managment, our supervisor at SonyEricsson.
- Stefan Andersson, Security Expert

3.1.2 Interviews

The interviews that are performed will not be in focus when testing the hypothesis. The interviews have instead an important role for this research giving information on understanding what the mobile operators think of DRM.

The target group for our interview is Sony Ericsson customers, in this case it is the mobile operators. The mobile operators that we have selected have been the ones that have a 3G-network licence. These operators are in particular interest since they will provide this fast network, and the DRM issue will be in focus when this network is taken in use. They are also the companies we expect to have knowledge about DRM.

The interviews will be in the “Standardised Open - Ended Interviews” form, since we think this interview technique will be a suitable choice when trying to achieve a structured interview. The interviewer can answer in its own words and the goal is to let them answer according to their own categories and interests in order to hear their point of view of the phenomenon[3].

The questionnaire is attached in enclosure 1. The companies that we have contacted for our research are:

- Tele2 – Ulf Baldhagen, Content Manager, email interview.
- Telia – Did not respond.
- Europolitan – Mårten Ulfsbäck, Mobile Internet Applications Manager, phone interview.
- Hi3G – Did not have time for an interview.
- Orange – Did not have time for an interview.

[3] Interviews in qualitative research, Nedstam p. 1-5

The interviews were made over phone and e-mail, depending on the interviewee's request. The companies we interviewed were restricted to those with a 3G license.

4 History and development of DRM

4.1 History and development of DRM

The first time DRM was introduced in the late 1980s. Some of the companies in the business existing today, were founded then and in the early 1990s. However most of today's DRM companies came during the last five years.

The companies developing DRM come with many different technology backgrounds. Some originate from the security business. Two are well-known multinational companies (Microsoft, IBM). Many are spin-offs (i.e. ContentGuard, from Xerox). Others come from the media area such as the entertainment, online industry, software licensing, pay TV, or publishing technologies (i.e. Adobe).
Intertrust (1990) is one of the few pure DRM technology companies[4].

Unlike the vendors, the DRM technologies are relatively new. You could say that DRM is a "fine balancing act between the needs of the content owner on the one hand and the content consumer or user on the other"[4]. If the DRM functions as it is supposed to, the users will never even see that it is operating in the background. Only when access rights have been violated will it appear and become noticeable to the user[5].

The rapid development in technology in recent years has made it very easy for people to copy, alter or distribute files. Now illegal file sharing is growing uncontrollable. This business makes the industry lose billions every year. Illegally distributed files, such as MP3s (Moving Picture Experts Group audio layer 3), are spread everywhere. From all this, the need for DRM has sprung up.

DRM is, for the monetary reasons mentioned above, a priority for most content providers today. Included here, are major companies from the movie and record industry, as well as book publishers and on-line banks. You can say that every company that produces anything digitally or needs secure authentication and transfers is affected.

As it is with all new markets, the DRM market also has factors driving it. IDC has recognised four market factors, ordered below:

1. Intellectual Property Protection
   With the Internet and the sharing of digital information just keep on expanding, content-owners look for new ways to prevent all kinds of misuse. At the same time they are looking at new ways of doing business. Today, many providers

[4] IDC group report p.8

hesitate to publish their works due to insufficient ways to ensure their proper use. Until there is a safe method many companies will hesitate to enter new markets/businesses and consequently miss new developments and revenue opportunities.

2. Competing Standards
   In emerging markets, there is usually not a general standard in the beginning, and the same is recognisable to the DRM market. The establishment of such a standard is important though for a continued prosperous development of any new market. The goal with such a standard is to integrate, interoperate, and eliminate obstacles for adoption and widespread use.

3. New Revenue Opportunities
   As mentioned above, DRM will create new revenue opportunities. It is a technology that lets content-owners publicise digital content in a package containing specified rights for that specific content. Since the fear of illegal use diminishes, DRM makes them able to control their content in ways that used to be impossible. It is now not only secure but also merchantable.

4. Protection of Privacy and Confidentiality
   The digital development has led to a higher demand for more and better privacy. In the United States for example, federal legislation mandating access protection and audit trails for electronically distributed information contribute to a higher DRM demand, since DRM can provide all the necessary security for maintaining sufficient privacy[5].

   Since there is no general standard set every company can (and they do) make its own solutions. There are however so far a few standards introduced, which all await a possible general adoption. They will be explained further in chapter 10.2.

4.2 Obstacles to DRM development

There are a few obstacles that all could slow down or even stop the DRM market growth.

- Too many players. There are twenty plus companies, all with a different non-standard solution. With all these possibilities, customers have a hard time choosing the right DRM for their needs.

- Partial solutions. Most companies offer an independent technology, requiring integration into applications or other systems to be fully useful. On top of this, many can only handle a limited number of content types.

[5] IDC group report p.11

- Lack of expertise. With technology being so new many companies lack the expertise needed to fully deliver sufficient electronic distribution solutions. This could lead to more trials than actual applications.

- Not enough clear legal precedent. A number of open court battles will affect the law regarding copyright ownership and digital distribution, of which some could have major impact for the future.

- Consumer reaction to content prising. Consumers may hesitate to pay for any content whatsoever or they might not want to pay as much as asked. It could also be hard to convince people to pay for content that was recently free. All this could lead to a delay of the consumer adoption to DRM.

- Competing standards. As mentioned above, the lack of a generally accepted DRM standard will delay adoption.

5 DRM – Digital Rights Management

5.1 Components of DRM

The summary from all the different DRM descriptions is that a DRM system is supposed to enable secure exchange of copyright-protected digital media. DRM provides the ability for the content owner to distribute their content securely to authorised recipients, which gives them the control over the whole distribution chain. Here is one example as is seen in picture 5.1 of how DRM can be described, by Frank Hartung and Friedhelm Ramme[6]:

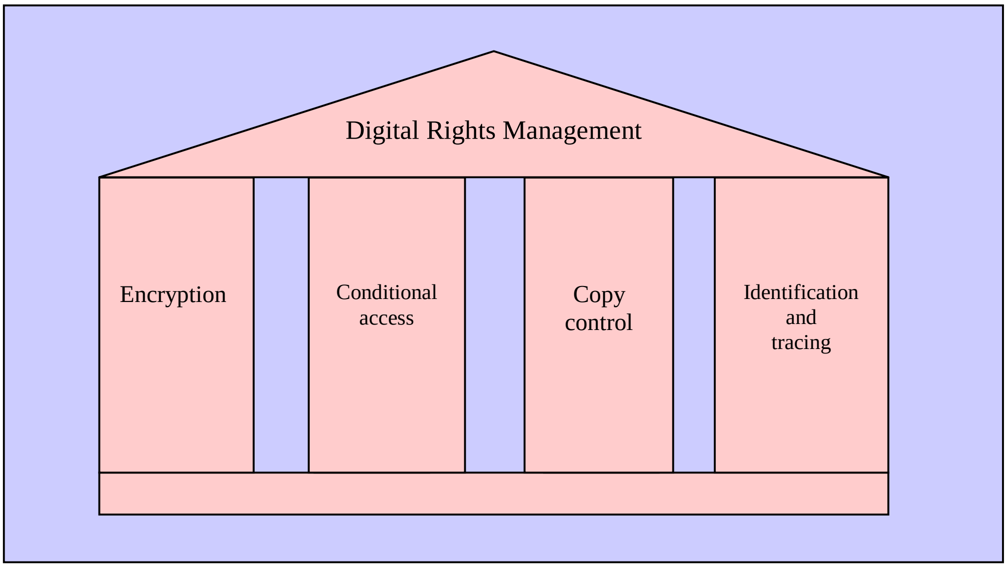

Figure 5.1: DRM can be seen as a foundation of four pillars.

[6] DRM and Watermarking of Multimedia Content for M-commerce Applications p. 79-80

- The first pillar is encryption: The content is being encrypted to shut out uncontrolled access. The decryption key management belongs to this pillar too.[7] The key management shall be separated from content protection and they shall be stored separately, to modify independently, and to assign different sets of rights to the same content, or vice versa.[8]

- The second pillar is conditional access: By adding flexible usage rules, the access to the protected media is controlled. The strength of the modern DRM system is that the usage rules can be adapted to the business model, so that access can be restricted to certain users, for a limited time or for a limited number of accesses.

- The third pillar is copy control: Depending on the usage rules, no/one/several/unlimited copies of the multimedia data are allowed, with or without the right to make further copies. DRM systems enforce these copy restrictions. For some usage rules, copy control is difficult to achieve and requires sophisticated technology like watermarking (see Enclosure 2).

- The fourth pillar is identification and tracing: Authorised users of multimedia often have access, if not to the digital data version, then to the analogue version of the data. Then they are capable of making copies from the analogue output. Analogue copies are very hard to prevent and some applications have the feature to trace back copies that have been made either from the digital source or the analogue. This is made with watermarking and is called fingerprinting.[9]

A DRM system is similar to other systems, which means that the system is never stronger then its weakest component. This is why all the steps and components in a DRM system must be integrated with each other. This also means that content must be encoded through the whole distribution chain. From the content provider to the analogue loudspeaker and perhaps even after that.
Every technical accessory concerning content playback needs to get a certificate, to ensure DRM security. This will be a difficult process both from a technical and a legal point of view. Especially when all the vendors are developing different products based on different standards[10].

[7] DRM and Watermarking of Multimedia Content for M-commerce Applications p. 79-80
[8] DRM requirements for PSS Release 5
[9] DRM and Watermarking of Multimedia Content for M-commerce Applications p. 79-80
[10] dagensIT.se p.2

5.2 DRM concepts

5.2.1 A general DRM concept

The DRM market today is growing stronger and there are several different models of how to construct a DRM solution. The different solutions are often thought of as being used for different media contents. The solution that we show (figure 5.2) here is a mix of a few of them, as an attempt to make it as general as possible. DRM has a lack of standards but the general concept is traceable through all the different applications, and that is what we have tried to catch[11].

1 The content author/provider creates content. Content can be music, software, books or any other types of media.

2 The publisher takes the content and seals it. First the publisher takes the content and with the DRM Right Description Languages, then puts on the usage rules. The publisher then makes the content watermarked to ensure copy protection. When the content is watermarked it is being protected with the help of cryptographic methods (see Enclosure 2), either with a private or a public key. When the content is made cryptographic the source code can no longer be seen. The Rights Description Languages will be described later in this chapter[12].

3 The publisher configures access control (license templates). The DRM systems of today have the strengths of making specific usage rules for certain users and for a limited time, or a limited number of accesses.

4 The publisher puts the protected content on a server and makes it available on the Internet, for example through a portal.

5 The publisher also puts the license templates on a license server, different templates for different uses.

6 The consumer asks for the protected media and sets up the license template, which specifies how the consumer is allowed to use the protected content. When the template is set, the consumer is asked to pay the amount for the license. The protected content is easy to download but the license costs.

7 The consumer downloads the protected content, for example to his/her mobile phone. The download process is made over a secure channel like SSL/WTLS (Secure Socket Layer/Wireless Transport Security Layer) to a mobile phone. The consumer can use the media according to what the license template allows. The consumer must require the license from the license server before the content can be used. The license is also downloaded in a cryptographic form and the user needs a key to decrypt it. The downloading process is also done over a secure channel here.

[11] http://www.intertrust.com/main/products/#
[12] http://www-4.ibm.com/software/is/emms/

8 The protected content can be played/viewed with a special player/viewer. The player keeps the content in a protected form. The player can only play the content with the help of the license template, which is known as the private key. The key decrypts the content inside the player. If the license template does not meet up with the requirements, then the player/viewer will not play the content. The player/viewer is able to play the content without extracting the watermark. This is because the content must remain protected, even after being played.

Protected content can be shared with other users. In order for them to use the content they first have to purchase their own license template to decrypt it.

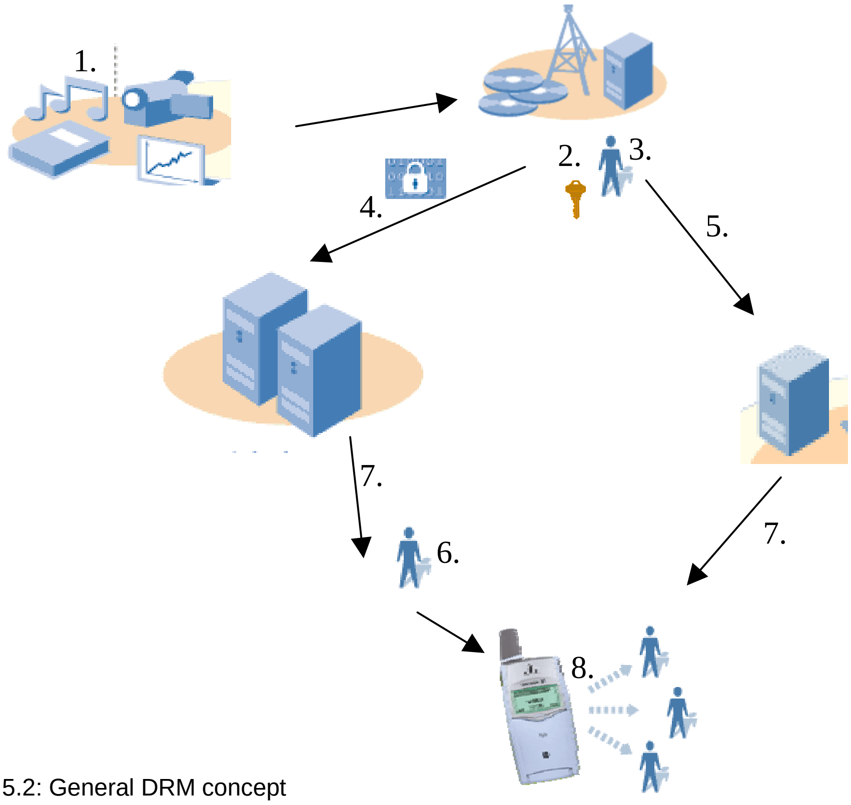

Figure 5.2: General DRM concept

5.2.2 An alternative DRM concept

The alternative DRM concept can be called an open variant of the "general DRM concept". The general DRM concept is sometimes also known as the "Full DRM". For simplicity we refer the alternative DRM concept now as the Open DRM.

Open DRM's (figure 5.3) main differences comparing to the other concept are that it lowers the degree of security. Open DRM does not use cryptography or watermarking but still use Rights Definitions Languages. Open DRM is a model constructed for trusted networks[13].

[13] Report from Vodafone (secret)

The workflow:

The content providers pass its information to the publishers. The content can be any kind of digital media (music, e-books, phone signals etc.). The publishers take the digital content and add rights to the content. The rights are being made with help of Rights Descriptions Languages for DRM. The rights rules that are being made are for example: save, forward, play two times. There is no cryptography or watermarking added to the content. It is only the rights that specify how the content usage rules are. These rights are described in a file attached to the content.

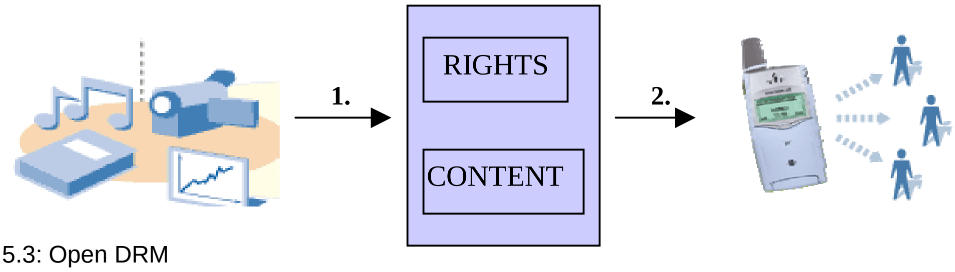

Figure 5.3: Open DRM

The transfer (2) between the publisher and the consumer (mobile phone) is made over a secure channel, like Secure Socket Layer (SSL) or a similar transfer mode Transport Layer Security (TLS). The content within a trusted network is secured using Wireless Transport Security Layer (WTLS).

A trusted network is an area where the network traffic is going over secure networks protected by SSL, TLS. The content is delivered secured by WTLS. Trusted networks are suitable to create around mobile phones.

In the absence of encryption, this concept is a target for attacks. To ensure as high security as possible the client (mobile phone) must verify its identity and that the target devise is within a trusted network. Then the client is approved to download content from e.g. the ring tone portal. When forwarding content between clients, the network must perform a client authentication test before delivery to the recipient.

5.2.4 Differences between general DRM and alternative DRM

The main difference between the general DRM (Full DRM) concept and the alternative DRM (Open DRM) concept is the level of security. The security level in the Open DRM is lower, since encryption and watermarking are not attached to the digital content. Another difference is that in Open DRM there are no licence templates. Open DRM relies on the Rights Definitions languages. The player senses the rights and is controlled after them. The user can only use the content how it is specified in the Rights.

This is working within a trusted network as a mobile phone. In a mobile phone it is harder to modify the hardware and to “hack” the Rights.

An obvious method is to attack the Open DRM, where a personal computer (PC) is connected within the network by a terminal. The PC can emulate a legitimate mobile phone to receive content. Then within the PC environment the Rights can be hacked and modified. The modified content can then be distributed over the Internet without limitation. In the Full DRM concept this is harder to achieve because the content is always encrypted and can never be seen in its source code.

The different concepts are supposed to be used in different areas, according to the value associated to the content[14].

The Open DRM is considered appropriated for low-value content, like:

- News, weather
- Privileged information (football results)
- Ring tones, screensavers

The Full DRM is considered appropriated for high-value content, like:

- Music
- CD, DVD
- Books

	Full DRM	**Open DRM**
Security	High	Low
Media type	Music, CD, Books	Weather reports, Ring tones, Screen savers
Watermarking	Yes	No
Trusted Network	Not required	Required
Rights Description Languages	No	Yes
Platform	Internet, Mobile Internet	Mobile Internet
Cryptography/ License	Yes	No

Figure 5.4: Comparison between Full and Open DRM.

Low-value contents are thought to be of no interest for the hackers to attack, that is why the use of lower security is applicable here. With high-value content the need of higher protection against attacks is needed.

[15] Vodafone's report (secret)

5.2.3 Rights Descriptions Languages

There are several proposals for rights description languages, mainly derived from eXtensible Markup Language (XML). These languages produce conditional access based on usage rules. At present two languages are more outstanding than the other ones. These are eXtensible Rights Markup Language (XrML) and Open Digital Rights Language (ODRL) and will be described here[15]

5.2.3.1 XrML- eXtensible Rights Markup Language

XrML is a language in XML, which describes definitions of rights, fees and conditions for using digital content owned by ContentGuard. XrML is licensed on a royalty-free basis.

It is a language that manages digital content in trusted systems. Trusted systems are systems that can hold digital contents and which can be trusted to honour the rights, conditions, and fees specified for digital contents. XrML also wants to develop an approach and language that can be used not only in the publishing industries but in other industries as well[16].

5.2.3.2 ODRL- Open Digital Rights Language

ODRL is the standard vocabulary for the expression of terms and conditions over assets. It does not enforce or order any polices for DRM, but provides the mechanisms to express such polices.

ODRL does not depend on any media types and can be used both within a trusted or not trusted system[17].

5.3 Mobile Internet DRM vs. Internet DRM

5.3.1 Internet DRM

Personal Computers (PC) are working as the device for Internet DRM. PCs are working as the platform for Internet for almost everyone here in Europe. This is the most common way of thinking of Internet. Internet DRM means that the PC will need a compatible program installed, which will support, and is able to playback the DRM protected content. These are the different applications, which are discussed in chapter 6.

5.3.2 Mobile Internet DRM

Mobile phones are working as the device for mobile Internet. The new high-rate networks that support General Packet Radio Service (GPRS) and Universal Mobile Telecommunications System (UMTS) make it possible for the consumers to access a

[15] Overview over Rights Description Languages for DRM, p.1-3
[16] XrML specification p.5-8
[17] ODRL specification p.1-4

hole new kind of wireless data services which require a high data flow through the networks. This opens up a new platform for DRM and a new market for the content providers and mobile operators and the use of mobile e-commerce (m-commerce) grows.

Mobile networks are often thought, from a DRM point of view, of being a more attractive distribution channel for multimedia content providers.[18]

5.3.3 How they differ from each other

Mobile Internet and Internet are two different kind of platforms that can be used for DRM applications. DRM applications are needed for content protection. The platforms have different techniques for enabling content downloading from the Internet, which will be the main usage area for DRM. As it looks today the downloading capacity speed and access to Internet, from the two platforms are very different.

Both mobile Internet and Internet have different properties that make them more or less suitable to be the most appropriate platform for DRM.

It is not a choice to make, to have the mobile Internet or the Internet as the platform for DRM but a matter of adapting it in various ways for DRM.

5.3.3.1 Authentication of User

An important issue in a DRM system is that the identity of the person (that for example downloads a music file) is known, so the person can be charged for the content.

A major difference between the Internet and mobile phone is that the identity of a mobile phone is always known. The mobile phone identity information provides more reliable information about the user. The operator often knows the individual user that owns a mobile phone[19]. The user's mobile phone has an identity number, in the Global System for Mobile Communication (GSM) it is called the International Mobile Equipment Identity (IMEI) number. This can be used in DRM systems for authentication, billing and marking of data[20]. The people that use pre-paid cash card is not that well or at all identified as the other users of mobile phones are (in Sweden it is not required to reveal any information about yourself when you by a pre-paid cash card).

In Internet the identity of the user is also known in the way that the user has an Internet Protocol (IP) number, that is unique for each PC, unlike the mobile phone's

[18] DRM and Watermarking of Multimedia Content for M-commerce Applications p. 83
[19] Overview study of Digital Right Management p.14
[20] DRM and Watermarking of Multimedia Content for M-commerce Applications p.83

IMEI the IP number is easy to hide and manipulate with. Every connection from the phone with the world around takes place on a settled operator's network.[19]

5.3.3.2 Platform environment

The closed environment in the mobile phone makes it more secure for rights management and protection. The mobile phones are less vulnerable to attacks against DRM systems than an open environment, like a computer, is, since the hardware is hard to hack[17]. A mobile phone has the software embedded in the hardware and this makes the phone hard to manipulate with. In the PC the software is easy to access and manipulate with.

5.3.3.3 Billing opportunities

In the mobile phone system there is always an operator controlling the billing. This works if the mobile phone is on a subscription, not if it has a pre-paid card.

This can be used in media distribution regarding charging for services and content, which the user requires[18].

When you use a pre-paid card you are relatively unknown to the operator and most importantly you do not have a monthly bill, so when trying to download you might not have sufficient funds.

5.3.3.4 Security

In the mobile phone the installation of a program is restricted to the developers of the mobile phone. The users are not, as it looks today, allowed to install any programs. A PC works oppositely, and allows any software to be installed on.[21]
Mobile developers are starting to enable users to download programs to the mobile phone by themselves. The mobile developers have become united to agree on different standards that the mobile phones will support.[22] This will increase the access that the users have to the mobile phone and may impact the security.

5.3.3.5 Resource allocation

DRM systems require additional resource usage like memory, processor capacity and signalling to function. To put up a session between a client (for example mobile phone, PC) and a server (for example a music portal), a great number of messages must be exchanged (e.g. for cryptographic key management) and additional complexity in the terminal for the decryption and deciphering. This amount of information that is exchanged may have an impact on the mobile phone since the memory resources are limited inside of it[23].

[21] dagensIT.se p.2
[22] http://www.aftonbladet.se/vss/ekonomi/story/0,2789,105809,00.html
[23] Overview of Digital Rights Management, p.14

6 DRM Applications

6.1 General information

With no general DRM standard adopted, many companies have developed and marketed their own solutions. Currently there are twenty plus different applications available on the market. From the market's perspective this is a good situation, the competition gets fierce and the development proceeds. Even though this situation also gains customers, it has a negative impact as well. If a customer wants to use the service of many companies, the customer has to download/install just as many applications. This is an inconvenience that could lead to people hesitating to buy what they really want; they might feel locked to one application.

In the long run though, it will be the DRM users – publishers, content providers and consumers – who will decide the issue by choosing the user-friendly systems that work across a wide range of platforms. It is all about demand and supply.

Not all of these application vendors have or plan a solution for the mobile market, e.g. for mobile phones. The major DRM companies (disregarding platform) we have identified are listed here:

- **Microsoft**. So far Windows Media Players, which are secure, have been installed on over 350 million PCs and portable devices. This means of course that Microsoft is and will continue to be a leader in the DRM market for all uses, both application and embedded use.
  Microsoft's DRM solution is however specified towards their own Windows operating system (OS) and their rich media format, which leaves the market for other OS or cross-OS solutions wide open. (IDC)
  Microsoft develops its rights management system based on ContentGuard and XrML.[24] (Ericsson report)

- **Intertrust**. So far Intertrust is not a market-leading company, but they sure have potential. Their patents are impressive totalling 18 issued ones. Intertrust's strategy is to be a neutral third-party provider of core DRM technology. In return they integrate it into their software and hardware. Intertrust has attracted over 50 parners, but has so far not generated any revenue.
  Nokia recently (Feb. 2001) bought 5% of Intertrust for $20 million, bringing DRM into Nokia's portable Music Player device.[25]

- **ContentGuard**. Originally a spin-off from Xerox, they now have alliances with and investments from Microsoft, Xerox and Adobe. ContentGuard and Microsoft have an ongoing exchange program in the fields of research and technology. ContentGuard also collaborates with Adobe Acrobat/PDF.[26]

[24] Windows Media Technologies 7
[25] http://www.intertrust.com
[26] http://www.contentguard.com

- **NEC**. NEC has created a Mobile Digital Rights Management system called VS-7810. It is compatible with mobile terminals from cellular handsets to PDAs and game machines. Examples of deliverable contents are different kinds of games, publications (e.g. books and outlines), and music services such as “jukeboxes” (billed per song) and buying songs (play them as much as you want).[27]

- **IBM**. IBM’s solution is called Electronic Media Management System (EMMS). It provides a modular, end-to-end DRM based content distribution solution. It allows content owners and other stakeholders in the value chain to conduct e-commerce and deliver digital media over a variety of digital transmission systems and devices. Currently it does not support video or streaming media. IBM works with five major label companies (Sony, Warner, EMI, Universal, and BMG).[28]

- **Sony**. Sony has developed a solution (openMG) for copyright protection technology that contains DRM. This technology is based on three key areas. (1) The download of music from multiple electronic music distribution platforms; (2) the playback of music files and the recording of music from audio CDs to the PC (OpenMG Jukebox Software); and (3) allows for the secure transfer of content to and from the PC and portable devices. OpenMG is constructed for a PC environment. [29] Sony has also developed a solution for mobile devices, OpenMG Light. OpenMG Light is built upon the same technology as OpenMG.[30]

7 Analysis and Result

7.1 Survey

In this part all the solutions along with their properties are evaluated. The major properties for the different 28 solutions (Reciprocal turned out to be out of business) that we have looked closer at are:

Cryptography
Watermarking
Exists/used today
Kind of content
Mobile Internet
Own created licenses
Standards
Client
Other information

First we want to make clear the information we have collected was found on the different companies homepages. This information might sometimes not be fully accurate, since the companies write and announce what they feel like and what they

[27] http://www.nec.co.jp
[28] http://www-4.ibm.com/software/is/emms/
[29] http://www9.station.sony.com/sca/press/feb_25_99_pf.html
[30] http://www.sony.co.jp/en/SonyInfo/News/Press/200105/01-0516E/

want their customers to know. We want you as a reader to have this in mind when you read this.

The different patterns that we could find from the table (enclosure 2) are:

SDMI – MPEG

From the table we can see a relation between the SDMI group and the audio/music media. Out of the seven companies identified to be supporting SDMI, six clearly have music/audio as their main (or only) media type.
MPEG is more differentiated with its four companies supporting a variety of media types. A focus towards the movie/TV media can however be seen, even though MPEG did invent the MP3.
There is also one company, InterTrust, that supports and collaborates with both groups. They have a number of applications for all kinds of purposes, e.g. music and movies.

	SDMI	MPEG
Companies	7	4
Main media type	Music	Video
Mobile Internet	4/7	2/4

Figure 7.1: Comparing SDMI and MPEG

Four out of the seven mobile solutions belong to SDMI, and two to MPEG.
Only three of the 21 Internet solutions support SDMI, and two MPEG. We can clearly see a pattern here. With a new technology (DRM) and market (Mobile Internet) emerging, companies do not want to risk developing a product not compatible with anything else, and consequently being left alone. Collaborating with other companies with a mutual standard does therefore give relief. The risk of their products turning out obsolete is decreasing. It is easier to develop solutions for the Internet and PC, since this market is more known and open. Everyone can develop and sell software for a PC, but this is much harder when it comes to mobile phones, since their software is embedded.

	#	SDMI	MPEG	No standard
Mobile Internet	7	4/7	2/7	2/7
Internet	21	3/21	2/21	**16/21**

Figure 7.2: Comparing Mobile Internet and Internet.

Cryptography – License – Client

From the table we can see a clear pattern associated with cryptography methods and license handling. Encrypted content needs a key to be decrypted, this key is in DRM context called a license (ticket). The license must be in contact with the encrypted content for it to become decrypted.

We assume the vendors of DRM that use cryptography with licenses should have some kind of license control on the user side. If you have a license to decrypt the content, then the content will be free unless you decrypt it in a controlled way. For example in a trusted and from the company's point of view controlled client/viewer. From the 28 solutions, 20 are using cryptography and they all use licenses.
We looked into which of these 20 companies that have developed its own client/viewer for the user side, the result is showed in figure 7.3.

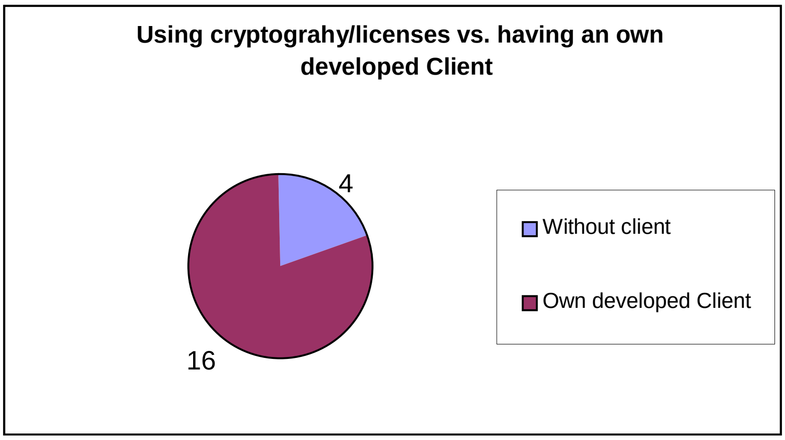

Figure 7.3: Own developed client or not.

The result was that 4 out of 20 have not developed an own client/viewer to be installed on the user side of the DRM system.
If the company that develops a DRM system do not consider a secure encrypted method on the client side, the content will be made free when it has been decrypted. This is not wanted in a secured DRM system. These companies without own developed client can of course solve this in another way. Some of the four companies were using existing viewers like Acrobat Reader and Internet Explorer, how they have control over the licenses and the decryption is unknown.

Exists today – Used today

An interesting approach to our survey was to try to determine if all the applications/techniques developed actually are used as well today. Out of 28 solutions, 25 looked to be in use, either as an own application used for example by a book publisher, or built in another application as a complement technique. This was expected because if a company develops a product it often has sponsors and interested parties behind them supporting them financially during the development phase. The DRM market has showed to be a very complicated and nestled network of companies working jointly developing standards but still remaining competitors.

Driving force

We thought it to be interesting to see which of these 27 solutions that actually have produced an own application and who are concentrating on techniques and infrastructure systems for DRM. The result is showed in figure 7.4.

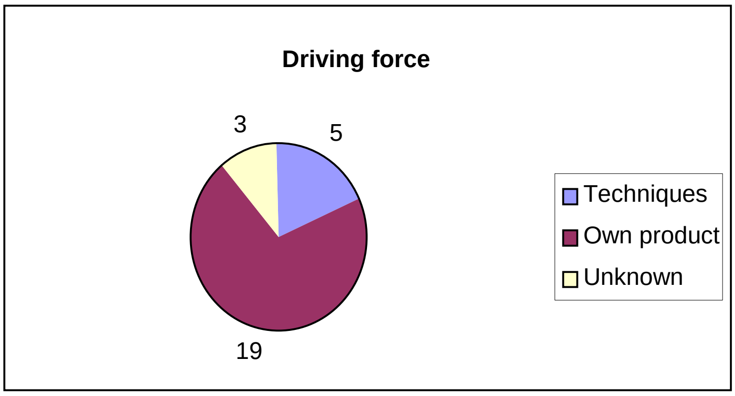

Figure 7.4: Driving force.

The unknown part from figure 7.4, is the solutions we have problem deciding where they should belong. These were solutions that supported MPEG, and we think it is hard to make clear what they really produce. The greater part is producing an application for DRM. The solutions that we think more of being techniques seem to be able to function together with other techniques and in that way a company could take the parts it likes from all the techniques and put together a solution that would fit the best. An example is that in NTT DoCoMo's mobile phones, there is a DRM system implemented that is built on both IBM's EMMS system and Sony's OpenMG Light[31].

Mobile Internet – Internet

Out of 27 DRM solutions only six is applicable to mobile Internet. This distinction can grow even larger though we have concentrated on finding solutions for mobile phones. Many of the companies that have a DRM solution for mobile Internet also have a solution for Internet. Then we have concentrated on the solution for mobile Internet.

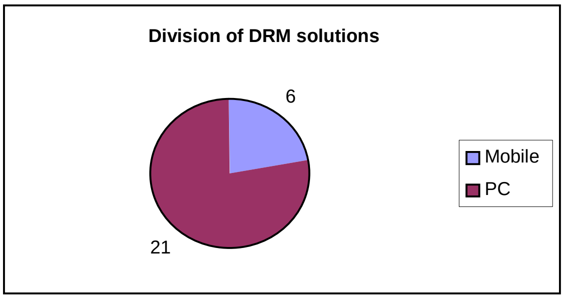

Figure 7.5: Division of DRM solutions.

[31] www.sony.co.jp/en/SonyInfo/News/Press/200105/01-0516E/

An answer to why it is such a great difference can be explained by numerous reasons. First the mobile phone market is a narrow market and a hard market to catch on. It requires a close co-operation between the DRM company and the mobile phone developer, since it is the mobile phone developer that decides which software that are implemented in the mobile phone and what content type that are allowed to playback in the mobile phone. A DRM company must ask the mobile phone developer if they want to support/attach their DRM solution in their mobile phone.

When producing a DRM solution for Internet (PC) you don't have to consider that, you only need to consider what operating system the client software must support. An attempt to lift up the market for mobile Internet is that many operators (Vodafone, Telefonica) and system producer (Ericsson, Nokia, and Sony) has gone together for developing a platform for mobile services[32]. This united platform will for example support Java, and have a Java Virtual Machine (JVM) installed. This will probably open up the market for the companies that develop Java applets. Perhaps this also will open up the market for DRM solutions for mobile devices, but the memory space will be limited inside the part of the phone that will be "locked up".

The mobile phone developers' highest wish is to have one playback device for all content. This will be hard to achieve since there are a lot of actors and so far no standard has been announced. All mobile developers are agreed that they do not wish the DRM market to be that fragmented as the Internet DRM market is.

In some aspects we consider it to be easier to develop a DRM solution for mobile phones. This is because mobile phone software is embedded and not reachable. Then the protected content will not be reachable and can not be manipulated. The level of security can be discussed, and perhaps it is not that important to have the highest security since it is harder to attack a mobile phone than a PC.

We assume the future with 3G network, will increase the growth of mobile DRM solutions, since the demand for DRM in mobile phones will increase when high value (music) content will be available to download from mobile Internet. It can also take another turn, the DRM solutions will be restricted to the ones that the market leader of mobile phone developing and operator have chosen.

[32] Öppen platform ska lyfta mobilt internet, Computer Sweden

Full solution

We could discern three solutions out of 27, which all have every security property (cryptography, watermarking, license, and a support standard such as SDMI and an own developed client). These are in figure 7.6.

Solution	Media	Protection	Platform
Liquid Audio, SP3	Music	Full	Internet, PC
Inter Trust, RightsPhone	Music	Full	Mobile Internet, mobile phone
IBM, EMMS	Music	Full	Mobile Internet, mobile phone

Figure 7.6: Solutions that support all protection properties.

These could be seen as an optimal DRM system, but there is no guarantee that these would be any better than the other ones just because they consist of every protection mechanism.
With a high protection level the threshold for copying digital content is raised, in an attempt to make it harder for people to copy digital content.

If we had made the selection without watermarking and standard, nearly every company on the list would have been selected. So how come so few actually make, as we put it in the table, a full protection? Is it enough with just cryptography, a license and a client? It is hard to say. It is always better with a more extensive the solution and a more secure environment. However, when regarding other factors, such as costs, available space/memory in the phone, maybe it is just not worth implementing too much in the phones. It is always a fine balance between developing a good product (and its development costs) and generating enough revenue.

Different content also has different protection requirements. If a phone is only able to handle cheap screen savers it is of course not necessary with an extensive DRM solution. On the other hand, the new phones with music abilities require sufficient protection.

7.2 What security level is required in a DRM system for mobile phones?

Protection can be looked at in two different kinds, first the protection that is *in* the object (cryptography and watermarking). That is an attempt to lock the protection to the content. The other one is protection *around* the object (DRM distribution chain, controlled access to content with playback protected). The difference is that if the protection in the object gets broken then only that object gets free. If the shield surrounding the object breaks, for example the DVD standard that got broken then every object of that kind can get free.
We have earlier discussed two different kinds of DRM concepts differentiated according to their security level (Full and Open DRM). The open DRM solution is more concentrated on protection surrounding the object, there is no protection

embedded in the object, and the pressure gets higher on the surrounding protection. The Full DRM supports both protections, in and around the object.

In chapter 5.3 we discussed how the mobile phone is suited for DRM. We consider the mobile phone to be a good platform as we described it there. We think the mobile phone can be the platform for achieving the raised threshold for copying digital content that is required by a DRM system. The DRM market is new and untested in mobile phones, it is only in Japan the DRM techniques has been implemented in a phone. The mobile phone environment makes it more appropriate to have a lower security DRM system (Open DRM, chapter 5.2.2) implemented. Whether this solution would be possible to use for anything else but low value content is today not known. Low value content is considered not to be desirable enough to make any great effort to hack it.

The open DRM solution is more attractive for the hackers and an easier goal then the full DRM. Open DRM's main property is that it requires a trusted network, which can be achieved within a mobile phone network. It is also an attractive point for the hackers to attack, for example to camouflage a PC to behave as a mobile phone and through that way get let inside the trusted network.

A good thing would be to start out in a low scale of the open DRM and to allow it to only handle low value content, to check how the market responds. If the hackers start to attack the solution then it would be unthinkable to let the Open DRM solution support music as well, since it is likely to be hacked. If this would happen the music producers would not approve with that particular solution and consequently put their music content on other portals supporting a higher DRM solution.

We can not give a direct answer to which security level that is needed in the mobile phone. We think the Open DRM solution is not suited at all for the Internet on the PC platform, since its open platform would make the solution too vulnerable.
What we can say is to start out low and then if it is needed make the DRM solution more secure or Full.

7.3 Future aspects

The DRM business is only a couple of years old. Predictions are therefore not based on much material, and sometimes even not on enough material. This means there are no revenue track records to analyse. Consequently, it is hard to predict the future and make accurate predictions.

However, with all existing facts, some forecasts have of course been made. IDC for example predicts the following figures for the world-wide DRM market from 2000 to 2005.

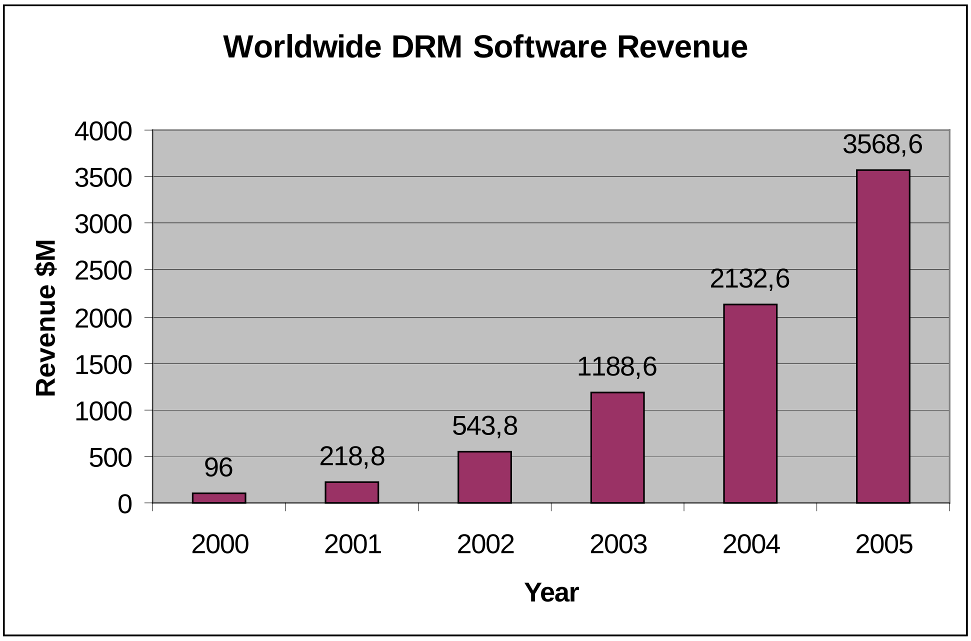

Figure 7.7 IDC's predictions for the DRM market. The CAGR (Compound Annual Growth Rate) is 106,1%.

These figures do not include the revenue for Microsoft DRM, since it is free. This estimation assumes a couple of things. For example:

- Royalty and transaction revenue accelerates as adoption spreads and usage increases in out years.

- The integration of DRM technologies with other content infrastructure will ease adoption and assist market growth.[33]

The IDC predictions above focus on the money involved. Other ways of looking at it are how many companies/solutions and what content that will be out there. How many will actually use DRM based solutions and services and to what extent? The different ways of looking at this are numerous.

The DRM market is growing, it might not necessarily end up exactly as IDC predicts it, but we do believe it will grow substantially. In most fields this would have resulted in more players on the market; the bigger the market/opportunities the more players pop up. However, it is different with mobile phones. There are a few reasons for this. In order to develop a mobile DRM solution you need to collaborate with a phone manufacturer, e.g. Sony Ericsson, since the DRM technology is embedded in the phone. In order to attract customers, they want to make their phones compatible with

[33] IDC group report p. 17

other manufacturers' phones, and since there are not many players out there, the market is limited, with little space for smaller DRM developers.

As with many new technologies/standards it might not be the best technical solution that will "win". A more important aspect is the amount of available content. For example, not many people will buy a good technical solution with little interesting content, when there is a sufficient one with more fun and more wanted content.

One thing that is almost certain though is that the lack of one common standard, or a few standards, will hinder growth in the short term. If a solution cannot be found or agreed upon, this could last longer. It is therefore vital for everyone to find and introduce such a standard as soon as possible.

All this applies to the Mobile DRM market, and not at all to the Internet, where we believe more solutions/companies will keep the market fragmented, since the PC is an open environment.

7.3.1 NTT DoCoMo I-mode

I-mode is the name of Japanese giant NTT DoCoMo's 3G mobile solution. It is a mobile phone with colour screen, bigger display, and more features than regular GSM phones.

Subscribing to I-mode gives you access to more than 40000 Internet sites, e-mail, online ticketing, and restaurant services. All these things are available at competitive prices, through the billing being based on the volume of data transmitted, and not on the time spent connected. With connection speeds being much faster it is no longer that expensive to download for example music[34]. All file-transactions are protected with a DRM-solution, jointly developed by IBM Japan and Sony.[35]
Downloadable content does not include MP3's or any other file-format that is not supported by NTT. Only music from DoCoMo's websites is available. Their new music distribution service is called M-stage.
The phones are not compatible with any file formats whatsoever, that are not "approved" by them.
One downside could be that you can only use files/services provided by DoCoMo. They control the entire chain, from making the phones to listening to the music. There are no other players involved.

This service is currently only available in Japan, but with the new 3G-networks being built in Europe, which should be up and running during 2002, similar services and opportunities will be coming soon.

Sony Ericsson's phone T68 has a program, enabling I-mode functions in the phone. It transforms I-mode to WAP-pages, and shows them in colour. It depends on the operator. They need to install the program in their WAP-gateways. Nokia and other

[34] NTT DoCoMo to Launch PHS Music Distribution Service, www.nttdocomo.com
[35] http://www.sony.co.jp/en/SonyInfo/News/Press/200105/01-0516E

Ericsson phones can also use this service, but it is only the T68 that has the colour screen.[36]

7.2.1 Interviews with mobile operators about DRM

Here we present and discuss information that we have collected, processed, and analysed from our mobile operator survey.

Since we did not receive sufficient information for a table, we summarise the answers in the text instead.

Answers:

Out of the five companies (Telia, Tele2, Orange, HI3G, and Europolitan) we contacted, only two companies (Europolitan and Tele2) answered.

Europolitan (E) had knowledge about DRM and they have been working with it for "an unspecified time". We asked E to explain what DRM is and they answered "it is very hard to explain, it exists as many different explanations as it exists applications and companies working with DRM", and they added that all content in the future will be wirelessly transported and secured. At present it exists content that go through the Internet, however due to its low value, the transfer security is low. E says this is one kind of DRM. All this depends on how you describe DRM. They think it is hard to see DRM as a sole product, it is more like a wishful general term, and they expect the protective shield to be much stronger in the future.

Europolitan did not answer the question about how they would like to implement DRM; they did not comment which security level they will support or which applications they could to see as an alternative for the mobile market.

Neither company specified any billing techniques, but they will probably use different alternatives. It might also be possible to choose billing technique depending on who you are. E charge 30-50% of the content providers' revenue (in Japan only 7%). E defends this by saying they have a customer service and support 24 hours a day.

Both companies predict the future services to evolve more e-mail services for the mobile phone, e.g. being notified when you have new mail. Other services they are planning are more business-adjusted services, for example access to the company's Intranet and new mobile games, such as a football game where you can pick your players.

Both companies will probably develop own portals, from which users can download content, however they will not handle any content production. Since the download will go through their network, other Internet portals must support their standards or come to an agreement with the mobile operators. At present it is not possible to download a music file, but it will be in the future though. Tele2 however, thinks it will take years before that will be available, with the compressing techniques existing

[36] http://www.mobil.nu/nyheter/visa.asp?id=4340&sid=1

today. Tele2 eventually predicts it to take about 3 minutes on an average transfer speed of 300 kbps (Kilobyte per second).

Both companies expect the usage of new services and faster networks to grow. Europolitan points to increased usage through the phones now supporting Java and that it will open up the market. Tele2 emphasises first of all the phones, and secondly the services to change the mobile market from 2G to 3G. Fun services directed towards young people and communities will be the main drive, according to Tele2.

Tele2 see I-mode as a “fun”, modern concept, but there is not much that is comparable to the Swedish market. The Japanese market differs a lot, however they do think there are elements that can be used here. Europolitan think the difference between Sweden and Japan is that Sweden is much more PC-oriented than Japan. In Japan the Internet is mainly used on mobile phones, while we in Sweden use the PC to surf the Net.
Japan prefers to download pictures and other not so serious services. E think the Swedish market demands “serious” products and services and they wait for such. At the same time Japan is ahead with better technology and terminals, and simpler usability.

On the last question, what a 3G license means for the company, Europolitan responded that they never considered not getting one, and Tele2 said it means huge investments and is strategically important. They will bring the experiences they get from Sweden to other Tele2 companies in Europe.

Summary

From these interviews, we would first of all like to mention their lack of DRM knowledge. We think DRM is a necessary ingredient for the future. If the mobile operators do not have knowledge or interest in it, the work put in by the mobile producers into building robust DRM applications for their mobile phones will not be for any use.

To create a robust mobile DRM solution, operators and developers must work together for it to be secured and for the content to be controlled during the entire distribution chain.

Another thing different from our predictions is that Tele2 do not think it will be possible to download music for years. We believe that already next year it will be possible to download music to mobile phones. As mentioned above, if they do not co-operate it will not be possible.

We think it is good that both Europolitan and Tele2 develop new products and services continuously. This is good for the users and increases users’ interest for mobile Internet.

9 Discussion and Conclusion

When this project started, we did not have any knowledge of DRM. Along with the process we have learned more and more, and realised the complexity and size of the DRM business, which consists of companies from many different fields, e.g. content providers, software developers, mobile phone manufacturers, and operators. With DRM being so new, there hardly exists any printed material, so we have mostly used Internet sources. Another aspect making this hard, is the definition of DRM; there are as many explanations of DRM as there are companies involved.

When comparing the mobile Internet with the Internet we found the sooner to be more secure and more suitable for DRM. It is not about choosing between the two; they are used for different purposes. DRM is a technique that is to be used on both platforms.

We have looked into the existing DRM applications, and found that they are all different regarding content, protection mechanisms, target groups, platforms and clients etc. The applications are generally well made, and a good foundation for the future, even though they are not widely used today. Mobile DRM applications are barely used today; hence it is hard to know how they function.

An Open DRM solution is sufficient for a mobile phone, it would meet the DRM requirements. However, we do not recommend it due to the high risk of attacks/hackers on high-value content. It is enough for low-value content though.

We believe the DRM market and its value will increase exponentially over the next few years. The “winner” will be the company providing most content. How technically advanced a solution is, does not matter as much, and consequently not the priority.
The number of players on the mobile Internet DRM market will be less than on the Internet DRM market, due to the complexity of getting applications into the phone. The latter will consist of many more players, and remain fragmented, since it is an open market.

Through answering the questions together with researching the theory, we have concluded that our hypothesis is true. A DRM solution has clearly showed to be able to handle content securely, leading to the content providers getting paid. Consequently if the mobile phone developers embed a DRM solution then the same outcome as mentioned above will occur.

When conducting future studies we can recommend things we did not have time to do, but nevertheless are very interesting. Find the best solutions and implement them in mobile phones to see how they would behave in a real environment, and eventually find the most suitable one. Look closer into the protection techniques and see how a trusted network functions, to find out how secure it really is. These are our examples of future studies or theses building on our research.

9 References

Literature

Katzenbeisse S, Petitcolas F AP, “Information hiding, techniques for steganography and digital watermarking” ISBN: 1-58053-035-4

Web sites

Sony – http://www.sony.com, http://www.openMG.com,
Mindport – http://www.sentriq.com
NEC – http://www.nec-cx.com/products/vs-7810/
Realnetworks – http://www.realnetworks.com
InterTrust – http://www.intertrust.com
Verance – http://www.verance.com
PublishOne – http://www.publishone.com
Sealed Media – http://www.sealedmedia.com
LiquidAudio – http://www.liquidaudio.com
MediaDna – http://www.mediadna.com
Encryption Software – http://www.encrsoft.com
Perimele – http://www.perimele.com
Preview System – http://www.previewsystems.com
RightsMarket – http://www.rightsmarket.com
Envivio – http://www.envivio.com
J. River INC – http://www.musicex.com
Adobe – http://www.adobe.com
Macrovision – http://www.macrovision.com
Alchemedia – http://www.alchemedia.com
Atabok – http://www.atabok.com
Authentica – http://www.authencia.com
DigitalOwl – http://www.digitalowl.com
NetActive – http://www.netactive.com
ContentGuard – http://www.contentguard.com
Reciprocal – http://www.reciprocal.com
IBM - http://www.ibm.com/products/emms
MPEG – http://www.mpeg.org
SDMI – http://www.sdmi.com
XrML – http://www.xrml.org
ODRL – http://www.odrl.com
3GPP – http://www.3gpp.org
NTT DoCoMo http://www.nttdocomo.com
(All web sites have been visited frequently during the process, 2001-10-01 – 2001-12-18)

National Institute of Standards and Technology –
http://csrc.nist.gov/encryption/aes/aesfact.html (2001-10-18)

Reports

Hartung, Frank, Björk Niklas, Ericsson,“Overview study of Digital Right Management (DRM)” 2001-05-17

Duhl Joshua, IDC Group, “The DRM Landscape: Technologies, Vendors, and Markets” June 2001

Hartung Frank, Ericsson, “Overview over Rights Description Languages for DRM” 2001-01-05

Vodafone Group R&D, Secret report.

Articles/ Specifications

Hartung Frank, Ramme Friedhelm, Ericsson Research, “Digital Rights Management and Watermarking of Multimedia Content for M-commerce Applications” (IFFF Communicaitons Magazine, November 2001)

SDMI(Secure Digital Media Initiative), “SDMI Portable Device Specification, part 1, Version 1.0” Los Angeles 1999-07-08

Koenen Rob, MPEG(Moving pictures Experts Group) – “Intellectual Property Management and Protection in MPEG Standards” January 2001 - Pisa (http://mpeg.telecomitalialab.com/standards/ipmp/index.html, 2001-11-18)

ContentGuard, “XrML: eXtensible rights Markup Language” specification (http://www.xrml.org, 2001-10-17)

Iannella Renato, ODRL(Open Digital Rights Language), “Open Digital Rights Language(ODRL), Version: 0.9, 2001-06-29”

Hanson, Barbara, Alexander Sean, Microsoft, “Windows Media Technologies 7, Version: 4.0”

Fock, Johan DagensIT, number 44, 1 November 2001, “Mobilen står emot piratkopieringar”

Sony, Press Release: “SONY develops copyright protection solutions for digital music content” (http://www9.station.sony.com/sca/press/feb_25_99_pf.html, (2001-10-30))

Sony, Press Release: “OpenMG Light to be provided for NTT DoCoMo’s PHS-Compatible “M-stage music” (http://www.sony.co.jp/en/SonyInfo/News/Press/200105/01-0516E/, (2001-11-01)

Nedstam Josef, Department of Communication Studies, Lund Institute of Technology “Interview in Qualitative Studies”

Karlström Daniel, Department of Communication Systems, Lund University “Reliability and confirmability of qualitative research”

Weintraub Ofer, Hartung Frank, Neff Ralph, LS on Digital Rights Management requirements for PSS Rel-5, TSG-SA WG4 (CODECS) meeting #18 Erlangen, Germany 3-7, September 2001

Research on digital watermarking at Aristotle University of Thessaloniki.
(http://poseidon.csd.auth.gr/signatures/report.html, 2001-10-10)

NTT DoCoMo to Launch PHS Music Distribution Service,
(http://www.nttdocomo.com/new/contents/01/whatnew0105.html, 2001-10-19)

Computer Sweden, Öppen platform ska lyfta mobilt Internet
(http://computersweden.idg.se/includes/print.asp?id=011113-CS9, 2001-11-15)

Paulse Mats, Aftonbladet, Nokia lanserar ny världsstandard
(http://www.aftonbladet.se/vss/ekonomi/story/0,2789,105809,00.html, 2001-11-13)

Hedberg Anna, I-mode I Ericsson T68, Mobil.nu, 2001-11-23
(http://www.mobil.nu/nyheter/visa.asp?id=4340&sid=1)

10 Enclosures

10.1 Enclosure 1

The questions for the interviews with mobile operators:

1. Vilken är din titel?
2. Vad jobbar du med?
3. Hur skulle du vilja beskriva DRM?
4. Vad betyder DRM för dig?
5. Vad betyder DRM för Telia?
6. Jobbar ni med DRM?
7. Hur skulle ni vilja att DRM implementeras?
8. Var skulle ni vilja lägga betalningen?
9. Skulle du vilja peka på någon DRM lösning som du tycker passar för mobila marknaden?
10. Kommer DRM att vara ett givet inslag när de nya tjänsterna lanseras?
11. Hur skulle ni vilja implementera DRM?
12. Skulle ni vilja satsa på en fast månadskostnad av tjänsterna eller betalning per ned laddning/uppkoppling etc?
13. Vilka tjänster planeras för tillfället att implementera för 3G näten eller för GPRS?
14. Kommer ni att satsa på egna 3G portaler med tjänster, eller sköta det på annat sätt?
15. Hur lång tid tar det att ladda ner en låt I dagsläget?
16. Hur lång tid kommer det att ta sen?, den ungefärliga kostnaden?
17. Hur tror ni på de nya tjänsterna, vad uppskattar ni att användandet kommer att bli?
18. Vad tycker du om I-mode?, är det jämförbart med svenska marknaden?
19. Vad betyder en 3G licens för Telia?

10.2 Enclosure 2

Watermarking technique

Watermarking is an old technique, over 700 years ago paper watermarking appeared in the art of handmade papermaking. The need to protect products from being privately copied has always been there, and the need is increasing. From the watermarking technique on paper the step was not big to digital watermarking. Watermarking is a technique to unnoticeably convey information by embedding it into the cover-data. The alternations that the embedded data makes on the cover-data should not degrade the perceived quality. The alternations can vary in strength and the owner can decide how high alternations that are required. The larger alternations, the more degradation of the product, but it makes the shield around the cover-data more robust.
The methods for watermarking all share the same basic principles, first a watermark embedding system and then a watermark recovery system.

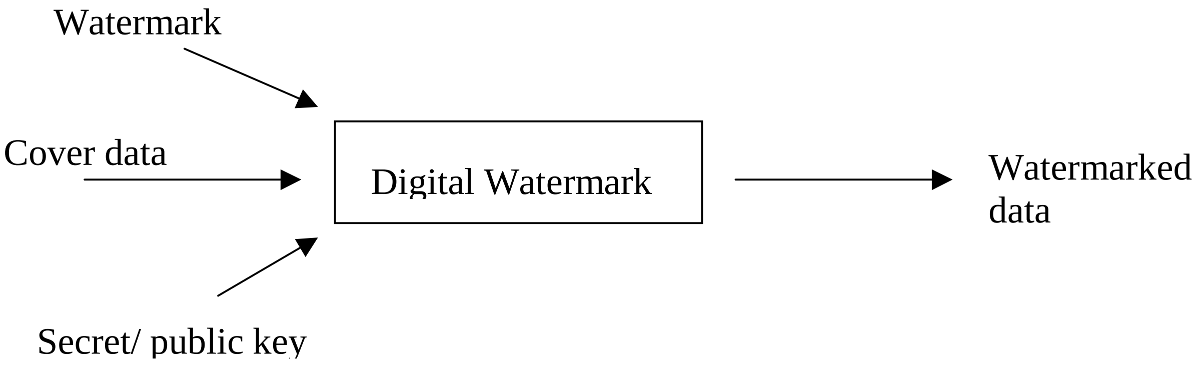

Figure 10.2.1: Generic digital watermarking scheme

By having the watermark, cover data and a secret or public key creating the input to the system, the data is made watermark-protected. The watermark can be of any nature such as a number, text or an image. The key is used to ensure security. This is to prevent unauthorised parties from manipulating the watermark in order to get the source data. The output from the system is the watermarked data. [37]

There are a few properties that are shared by all proposed systems. These are:

Imperceptibility
The modification caused by watermark embedding should not impair the perceived quality of the data.

Redundancy
To keep up the robustness, even though a small number of changes are allowed, the watermark information is usually redundantly distributed over many samples of the

[37] Information Hiding "techniques for steganography and digital watermarking" 97-101

cover data. To ensure that the watermark persists in the data even after manipulation with intentions of removing the watermark.

Keys
Watermarking systems use secure keys to ensure security against attacks trying to erase the watermark and to ensure that the watermark is only accessible by authorised parties [38] [39].

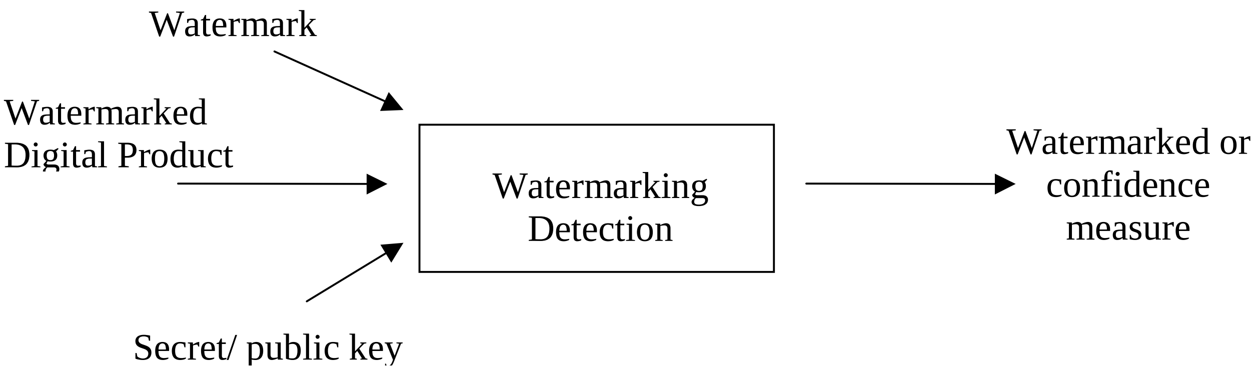
Watermark
Watermarked Digital Product
Watermarking Detection
Watermarked or confidence measure
Secret/ public key

Figure 10.2.2: Generic watermark recovery scheme

Detection is the most crucial part in the watermarking system. The inputs to the system are the watermarked data, the secret/ public key, and depending of the method (what level of security) that are being used, the original data and/ or the original watermark.
The output is the recovered watermark and some kind of confidence measure that indicates how likely it is for the given watermark at the input to be present in the data under inspection.
Watermarking is a general technique and there is a lot of ways of using it. Some applications might be:

Copyright protection
Probably the most common application for watermarking is to protect the copyright. The purpose is to embed information about the source, like the copywriter, the publishing date and so on. This application demands a high level of security since it is used to resolve the rightful ownership and to prevent other parties from claiming the copyright of the source.

Fingerprinting for traitor tracking
In this application a different watermark is embedded into each distributed copy of the source, because here it is more important to embed information about the legal recipient then about the source. This is useful when to trace and find privately made copies of the source that are illegal. The Internet has seen web crawlers searching for illegally copied images and programs.

[38] http://poseidon.csd.auth.gr/signatures/report.html
[39] Information Hiding “techniques for steganography and digital watermarking” 102

Copy protection
A desirable feature in multimedia systems is copy protection. This is hard to achieve in open systems. In a closed system it is applicable much easier. In closed systems like the DVD system, an indication of the copy status is achieved. The DVD system holds information in the watermark about copy control. The basic concept is that the player rather than the recording device (tape recorder, VCR etc) controls the copy state of the content, by detecting the watermark and comparing this with a physical mark, unable to be copied, on the disc. It checks that the physical mark is correct, i.e. that it matches the watermark, and then the device is authorised to play. A DVD player is not allowed to copy a file that carries a “copy never”[40].

Cryptographic technique

Cryptanalysis is the study of how to compromise (defeat) cryptographic mechanisms, and cryptology (from the Greek *kryptós lógos*, means "hidden word") is the discipline of cryptography and cryptanalysis combined. Cryptography is meant as a method of keeping communications private.

Cryptography is a method of two steps; the first one is encryption. Encryption is the transformation of data into an unreadable form. The unreadable form is only readable with the key that has the appropriate knowledge. The purpose is to keep hidden information hidden even for those that can access the encrypted information, unless they have the key to unlock the encrypted information.

The contrary towards encryption is decryption; it is the transformation of encrypted data back to the natural form. The encryption-decryption process requires some use of secret information as a key. Sometimes the same key is used for both the encryption and the decryption, and sometimes not, more about that later.

Cryptography is more today than just encryption and decryption. Authentication has become to be a subject concerning this. Authentication has started to be as fundamental in our lives as privacy is. Authentication is being used throughout our lives in everyday situations when we for instance sign documents. We are in a world where we need electronic techniques for providing authentication though our decisions are going electronically[41].

Public-key cryptography
The traditional cryptography system functions though both the sender and the receiver of a message use the same secure key. The sender encrypts the message with the secret key and the receiver uses the same secure key to decrypt it back to the original form. This system is called the private-key system. The problem with this method is for both the sender and receiver to share the same secure key, without any outsider knowing about it. The issue increases if the persons are located at different locations and have to trust a courier for transporting the secret key between them.

The public-key cryptography has solved this problem through giving each person a pair of keys, one public and one private one. The public key is published, but the private key is individual and only known to the owner. With this system the need for sharing any secret information together has disappeared. To send a confident message

[40] Information Hiding “techniques for steganography and digital watermarking” 103-105
[41] http://www.crypto.nkfu.edu.tw/infosec/faq/html/1-2.html

now only the public key is required, which is published. The receiver uses its private key to decrypt the message.

Public-key cryptography can be used not only for privacy, like encryption, but also for authentication (digital signatures) and other various techniques.
To make a digital signature the sender makes a computation involving both the private key and the message itself. The output is called a digital signature and is attached to the message. The receiver then has the opportunity to verify the rightful sender of the message, by making a computation involving the message, the purported signature, and the senders' public key. If the result is correct according to a simple, prescribed mathematical relation, the signature is verified to be genuine. Otherwise it has been manipulated.
This can be applied to the DRM systems. The publisher is using public keys to encrypt the digital content and the consumer buys a license, in this case a private key that the consumer then uses to be able to decrypt the digital content[3].

Different techniques
RSA – This is a public-key cryptosystem, which offers both encryption and digital signatures (authentication). RSA is a commonly used cryptosystem and is used in a lot of products, platforms, and industries around the world. It has also been embedded into many operating systems like Microsoft, Apple, Sun and Novell.
At the time of this publication, about 350 companies license RSA technology. The estimated installed base of RSA encryption engines is around 300 million, making it by far the most widely used public-key cryptographic system in the world.

DES – This is called the standard of decryption as the name "Data Encryption Standard" reveals. IBM has developed it. The DEA, often called DES, has been extensively studied since its publication and is the best known and widely used symmetric algorithm in the world. When communicating using DES, both the sender and the receiver must know the secret key. The key is used for both encryption and decryption of the message and for generating a message authentication code (MAC). The MAC is an authentication tag, derived by applying an authentication scheme, with the secret key to a message. The DES system is hard to distribute in a big environment with many users, though it is hard to keep the secret key secret with many users involved.

Triple-DES – This is the improved version of the DES standard. Triple-DES takes the input data (the single-DES key) and encrypts it three times[3].

AES – Is the new standard approved by FIPS (Federal Information Processing Standards). This is the standard that is taking over from DES and also its name (Advanced Encryption Standard) speaks for itself. AES is now in use. On February 28, 2001, NIST announced that a FIPS for the AES is available for public review and comment. This new standard is intended to last for the next 20-30 years. The algorithm that they have selected for this is called Rijndael, and the authors are both from Belgium. AES have three different key sizes, 128-, 192- and 256-bits, in comparison to the DES standard that only had 56-bits size[42].

SDMI

The Secure Digital Music Initiative (SDMI) is a forum that brings together more than 180 companies and organisations representing information technology, consumer electronics, security technology, the recording industry, and Internet service providers.

SDMI's purpose is to develop open technology specifications that protect playing, storing, and distribution of digital music so that a new market for digital music may emerge. The open technology specifications released by SDMI will ultimately be based on three main goals:

1. Provide consumers with convenient access to music both online and in new emerging digital distribution systems.
2. Enable copyright protection for artists' works.
3. Promote the development of new music-related businesses and technologies.

The SDMI specification is built around portable devices (PD) and portable media (PM) that can store and playback protected audio content. Licensed Compliant Modules (LCM) act as interfaces between the applications and the PD/ PM. The content must always be in a protected form even after it has been imported into the SDMI application or LCM, or recorded on a PD. SDMI applications, PDs and LCMs must respect the usage rules that are attached to the digital content.
SDMI is using a screening technology (watermarking) for detecting illegal copies.[43] [44]

MPEG

MPEG (Motion Picture Experts Group) is an ISO/IEC (International Organisation for Standardisation/ International Electrotechnical Commission) working group in charge of the development of standards for coded representation. MPEG is most famous for its file-formats .mpg (mainly video) and .mp3 (audio).
MPEG has a long history in dealing with DRM issues. The MPEG specific term for DRM is IPMP (Intellectual Property Management and Protection). IPMP provides hooks for DRM, but does not specify the algorithm or implementation. A hook is an API or interface that enables to attach a DRM system, without specifying the DRM system and its functionality itself. Even though they ease the deployment of DRM solutions they do not result in an interoperable solution.

The standardisation in IPMP has moved away from the earlier versions MPEG-2 and MPEG-4, towards being more focused on encompassing standardisation in order to reach its most important goal: interoperability.

[42] http://csrc.nist.gov/encryption/aes/aesfact.html
[43] Overview study of digital rights management p. 18
[44] SDMI specification

There are three MPEG standards today, of which one is MPEG's own DRM system, the MPEG-4 IPMP system. These three are MPEG-4, MPEG-7, and MPEG-21.[45] [46]

3GPP

The 3rd Generation Partnership Project (3GPP) is a collaboration agreement established in December 1998.
3GPP shapes the future of mobile communication standards. Currently they have 482 individual member companies, including Ericsson, Nokia, Europolitan, and Vodafone.
The original scope of 3GPP was to produce globally applicable Technical Specifications and Technical Reports for a 3rd Generation Mobile System based on evolved GSM core networks and the radio access technologies that they support. The scope was subsequently amended to include the maintenance and development of the Global System for Mobile communication (GSM) Technical Specifications and Technical Reports.

The DRM demand has led 3GPP to examine the possibilities of a mobile DRM standard. This now has a high priority within the organisation and frequent meetings are held around the world. So far they have proposed requirements for the DRM system standard.[47] They have also declared different levels of DRM protection:

1. No protection where they stand today
2. Legally binding copyright information but no technical mechanisms to enforce them
3. Legally binding copyright information and technical mechanisms to enforce them
4. DRM hooks/ APIs[48]

W3C

The World Web consortium (W3C) consists of 514 different organisations, such as universities and enterprises (i.e. Ericsson). It was founded in 1994 by the creators of the Internet and has had major impact on the Web development[49]. The W3C, which defines broad and widely followed Internet standards, has begun an inquiry into DRM standards. There they included all examples mentioned above.[50]

10.3 Enclosure 3

Application list is attached.

[45] Overview study of digital rights management p. 14
[46] Intellectual Property Management and Protection in MPEG Standards
[47] http://www.3gpp.org
[48] LS on Digital Rights Management requirements for PSS Rel-5
[49] http://www.w3.org/Consortium/Member/List
[50] IDC group report p. 14