

2 Digital Rights Management: Technological Aspects

2.1 Definition, Aspects, and Overview

*Niels Rump*⁴

Abstract: Digital Rights Management is a fairly recent technology — it came into use only in the mid 1990s. Nevertheless, it has already lived through a life cycle of ups and downs that many technologies would require decades for.

Digital Rights Management, or DRM, has been called “the saviour” of intellectual property rights as well as “completely useless” in protecting assets; it has been said that it is “accepted and is used” by the participants in the content value chain while others say DRM is “not used at all”.⁵

This paper takes a closer look at the role of DRM in distributing content through networks such as the Internet and indicates what types of technology are available, in what environments they exist and how well today’s DRM systems fulfil what is expected of them by various members of the content value chain.

I Introduction

Before embarking on the discussion about “Digital Rights Management”, the term itself needs defining. Unfortunately there are many definitions, depending of the viewpoint of the person providing the definition. One such definition is given in whatis.com⁶:

Definition 1.

“Digital rights management (DRM) is a type of server software developed to enable secure distribution — and perhaps more importantly, to disable illegal distribution — of paid content over the Web. [...]”

While this definition is definitely true, and it represents a fairly dominant view on what DRM is and provides, it does not give the full picture as it omits looking at the environment in which DRM Systems are to be used. Figure 1 shows this environment by providing the steps that most content goes through when being traded⁷: production, digitisation, identification, ascription of descriptions, distribution, use (by a consumer), monitoring of use, and collection of money. Any of these steps may be omitted in certain circumstances. For example, if content is distributed “for free” the step of collecting money will not need to be executed.

Digital Rights Management plays a role in *every step* depicted in the diagram and listed above. Hence, a more generic definition can be given as follows⁸:

⁴ Rightscom Ltd.

⁵ See: *Günnewig* within this book on page 528.

⁶ See: whatis.com (2002).

⁷ The term “trade” includes commercial trade for money using a variety of business models as well as peer-to-peer distribution where usually no money changes hands and other non-revenue generating trades such as “promotion”.

⁸ See: *Iannella* (2001).

Definition 2.

“DRM covers the description, identification, trading, protecting, monitoring and tracking of all forms of usages over both tangible and intangible assets. [...]”

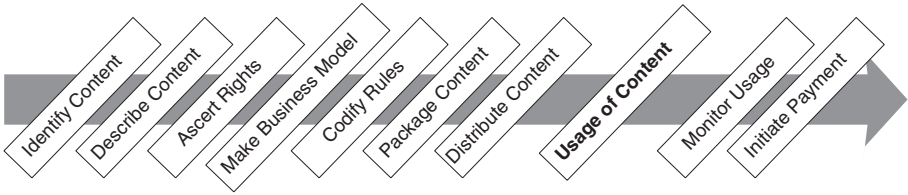


Fig. 1. Different Steps of Trading Content

In short, DRM includes *everything* that someone does with content in order to trade it. These DRM functions can be split into two groups as depicted in Figure 2:



Fig. 2. The two Parts of DRM

Firstly, DRM is about *managing digital rights* (depicted as the “Management” box in Figure 2). Rights holders need to identify their content (how else does a content or rights owner know what right he really owns?), they need to collect metadata⁹ to the content (how else should potential customers of such content be able find what they want to obtain?), they need to assert what rights they have in the content (only when knowing this can he actually attempt to distribute content), and they need to develop business models for distributing their assets¹⁰.

Secondly, DRM is about *digitally managing of rights*, or enforcing exploitation rules as determined by the rights holder (or any of the rights holder’s business partners, such as distributors, wholesalers, e-sellers, etc.). This second group of DRM functions is what Definition 1 speaks about; it is also this definition, with most people have in mind, when discussing DRM. Most of the “DRM technologies” (as briefly introduced in Section III of this article) fall into this second group of DRM functions.

II Environment for DRM Systems

Different elements of DRM systems are used in different stages of content trading as depicted in Figure 1. This already shows that these technical elements are not operating in isolation. In fact, the technologies used are dependent on the business models in operation and these, as well as the technologies themselves, depend on the legal system that prevails. For example, it would be imprudent to use high-security technology to protect content with comparatively low value or to use technology that offers little

⁹ The physical ascription of metadata falls into the second group of DRM functions.

¹⁰ The expression of such permitted forms of exploitation using a “Rights Expression Language” falls, again, into the second group of DRM functions.

protection when the content to be protected is of very high value. Similarly, protecting content with cryptographic technologies that are illegal in key markets will not enable a business to flourish and is bound to fail.

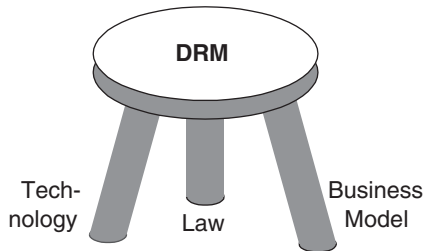


Fig. 3. Three Crucial Elements of DRM — the “three Legged Stool”

The three columns for DRM systems (technology, business models, and the legal underpinnings) can be compared to a three-legged stool which can stand upright only when all three legs are of the same length. As soon as one leg is too short (or, in fact, too long) the stool will fall over. Unfortunately, unlike a three-legged stool which, when all legs are the same length is fairly stable, the same does not apply to DRM systems. They are subject to influences by several external factors and it is those factors, that can lead to DRM systems not being used even when the technology is working properly. These influences, as described in some detail below, ultimately determine the success of DRM.

II.1 Economic Aspects

Economic aspects, such as the market situation, play a major role for rights holders and content distributors in determining which business models for distributing content and which technology (DRM and others) to use for supporting their business models. They of course also determine whether consumers are willing to obtain¹¹ content in new formats through new content delivery services — which usually also means the purchase of new equipment (e.g. an ebook reader, an internet-ready home stereo system or a digital television set).

The uncertain commercial climate following the burst of the “dot.com bubble” was certainly detrimental to the uptake of such content delivery services.

II.2 Social Aspects

The question of how socially acceptable it is to use DRM systems is the second critical issue which influences the promotion and use of DRM-governed content.

Why should a customer start using software with DRM components that, by their nature, limit the customer’s freedom in interacting with the content? Only when the majority of customers can be convinced that DRM is an appropriate mechanism for enjoying content, will they start to regularly use it.¹²

¹¹ Similar to footnote 7 on “trade” above (see page 3), the notion of obtaining content includes buying content for money as well as obtaining it “for free”. See: *Fetscherin* within this book on page 301.

¹² See: *Günnewig* within this book on page 528.

Providing “added value” to such DRM-protected content seems to be a possibility for achieving this goal. Unfortunately for the DRM providers and rights holders in the context of the music industry, the proliferation of unprotected ISO/MPEG Audio Layer III (mp3) content¹³ has already created a mind set that music can be freely copied and shared which puts a further burden on providing added value that has to be offered.¹⁴

Other social aspects also influence the uptake of DRM systems. For example the discussions on the tension between the right to protect ones intellectual property (as laid down in most countries’ copyright laws) and concerns over the erosion of “fair use” issues (as championed by the academic and library communities as well as, increasingly, by pressure groups for the handicapped) have dominated the discussion about DRM Systems. While many DRM systems can technically handle both aspects, their *use* has so far been geared towards the protection, leading to even more resistance to the concept and usage of DRM. Thus the aforementioned discussions can be expected to continue for the foreseeable future.

These objections against the use of DRM with content need to be overcome by an informed and open discussion and a sensible use of technology in sensible business models in order to create a social environment that is accepting of DRM.

II.3 International Aspects

The above issues cannot, however, be examined on a purely national basis and have to be investigated in an international context because for a variety of reasons:

1. The production and dissemination of content is in many cases too expensive for the content to only be disseminated in one territory. Hence, the rights situation in several countries will have to be taken into account.
2. The laws protecting intellectual property are significantly varied from country to country, despite recent efforts towards international harmonisation.
3. And last, but certainly not least, any content made available on the internet, even if intended to be distributed into one country only, is automatically available to internet users all over the world.¹⁵

Only when all these aspects are taken into account, can a working DRM system with all its components become successful, not only in protecting content, but also in supporting content distribution through viable business models.

¹³ One should better say: “technically unprotected mp3 files” as the content in these files is, in most cases and jurisdictions, still *legally* protected.

¹⁴ See: Rump, Herre, Brandenburg, Koller, Allamanche (1999).

¹⁵ Some DRM systems are able to limit the accessibility to the content to certain countries. That, however, requires that the DRM system runs on devices that provide support for that particular DRM system and which operate in these countries. This may lead to problems, in countries where copyrights laws do not sufficiently protect the viability of such systems — or even make them illegal.

III Components of DRM Systems

As described in Section I of this article, DRM Systems have to fulfil a variety of tasks. For each of these a variety of tools exists as described below.¹⁶

1. *Secure containers* make the content inaccessible to those users that are not authorised to access the content. These containers mainly rely on cryptographic algorithms such as DES¹⁷ or AES¹⁸. An early example is the Multimedia Protection Protocol (MMP) developed by Fraunhofer IIS¹⁹. Other examples include SDC's Digital Multimedia Object, InterTrust's DigiBox and DigiFile, and Microsoft's file format for ebooks `.lit`.
2. *Rights expressions* are used to express to whom access to the content wrapped in secure containers is permitted. Such rights expressions are formed either using simple rights expression flags or complex Rights Expression Languages such as ISO/MPEG's Right Expression Language²⁰ in conjunction with its Rights Data Dictionary²¹.

Fraunhofer's MMP is an example of a system using only simple rights expressions (MMP only allows music playback on one authorised machine) while the other examples given above all allow complex rights expressions. To what extent complex expressions will be practical in "small footprint devices" such as mobile phones and PDAs²² remains to be seen.

3. Content *identification and description* systems are used to uniquely identify the content (e.g. International Standard Book number²³) and to associate descriptive metadata with the content (e.g. SMPTE's²⁴ Metadata Dictionary²⁵).

Often content identification systems are combined with content description systems. For example, for each International Standard Work Code (ISWC) a minimal set of metadata (including items such as title, author, composer, etc.) will be created. Similarly, minimal metadata exists for the International Standard Book Number (ISBN) which has been in use for several decades. However no ISBN metadata data is *electronically* available, which forces online booksellers such as Amazon.com to capture their own metadata. This data is, however, of less value than the original data because of data re-entry problems (when data is re-keyed into systems where typos can create serious problems).

Such data — from the original source or not — can then be used, for example, by retailers for their stock control systems. The combination of ISBNs and book-related metadata has become very popular with consumers to, for instance, find, order and buy books.

Such identification systems also exist for other media types (e.g. International Standard Recording Codes (ISRC) for sound recordings, International Standard

¹⁶ A more in-depth discussion of some of these components can be found in subsequent articles within this book.

¹⁷ Data Encryption Standard.

¹⁸ Advanced Encryption Standard, also known as Rijndael.

¹⁹ See: Rump (1996).

²⁰ See: MPEG-21 REL (2003).

²¹ See: MPEG-21 RDD (2003).

²² Personal Digital Assistants.

²³ See: ISBN (1992).

²⁴ Society of Motion Picture and Television Engineers.

²⁵ See: SMPTE (2001).

Audio-visual Numbers (ISAN) for audio-visual material and Digital Object Identifiers (DOI) which is a generic content identification system²⁶).

4. Also important is the *identification of people* and organisations that intend to interact with the content. Not only does a rights owner need to associate a claim of ownership with the content but also the consumer will need to be uniquely identified. Such user identification systems are a prerequisite for DRM systems to be able to limit access to content to those users that have a right to gain access. One crucial aspect of the identification of *consumers* using unique identification schemes concerns Privacy regulations²⁷: When a DRM system uses a unique identification system for the consumers of content, it becomes fairly easy to generate a user profile that is potentially far more detailed than the ones credit card companies can assemble today. This is often seen as critical because the consumer has less control over such profiles when created by a service company located somewhere in the DRM value chain (from the rights owner via several intermediaries and service providers to the end user, see Figure 4) than if done by the credit card company that the user has a direct contract with.

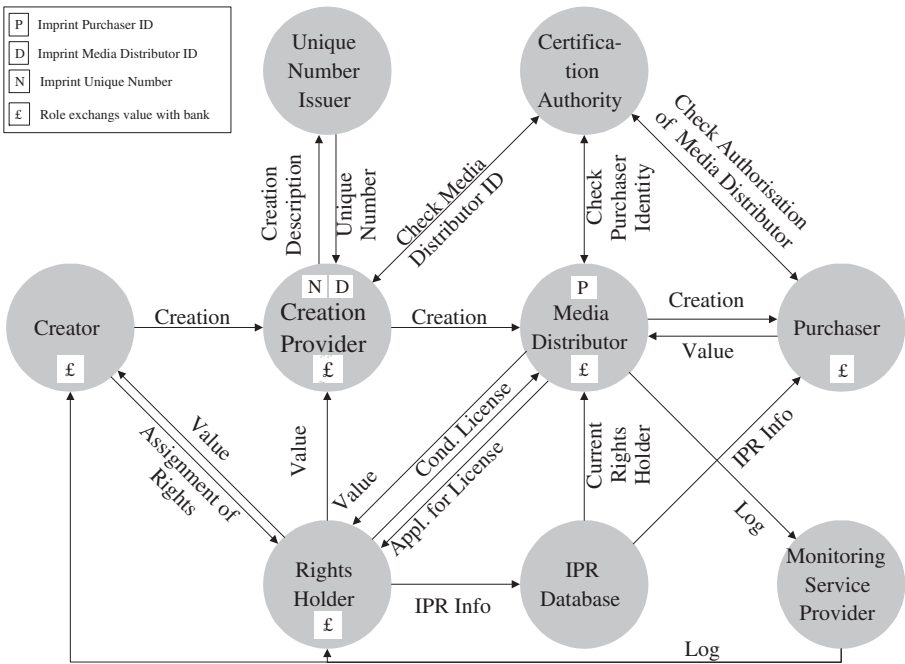


Fig. 4. A Model for a Content Value Chain: The Imprimatur Business Model²⁸

5. Closely related to the identification of people are algorithms to *authenticate* the person or organisation that wants to interact with any content. This function will involve cryptographic algorithms and may need an agency that issues electronic “passports” or certificates. This agency acts akin to the passport office of a country

²⁶ See: DOI (2003); *Paskin* within this book on page 26.

²⁷ See: Bygrave (2001); *Bygrave* within this book on page 418.

²⁸ See: Imprimatur (1997).

and is usually referred to as a “Trusted Third Party” or TTP as it is paramount that all members of the content value chain (see Figure 4) trust this party.

Only when the TTP is trusted by *all* parties in the content value chain, will the DRM systems and components that the TTP certifies be useable. It only takes one crucial partner to deny this trust for the whole chain to break and the DRM system to become useless in that particular value chain.

Other authentication needs can also be fulfilled by such algorithms with possible support from a TTP; two examples of such authentication are:

- Devices may need to authenticate themselves to the services they communicate with (and vice versa) so that both sides can be “sure” that they are communicating with a trusted member of the content value chain.
- Even within a DRM system, different components (e.g. the subsystem that deals with processing the rights expressions and the tools that “open” the secure container) need to establish a secure and authenticated channel amongst themselves.

A TTP may also perform a further task. When it is detected that a user or a component does not behave as expected (in other words: when the user or device cannot be trusted any longer)²⁹ it may be necessary that the certificate associated with that user or component is revoked. This revocation function is a crucial and hotly debated issue as device manufacturers do not like the idea that their devices may suddenly become unusable just because the TTP deemed it necessary to revoke some certificates.

6. Another set of technologies closely related to the identification of content are technologies to persistently associate identifiers and other information with the content³⁰. These most prominent technologies in this domain are *Watermarking* and *Fingerprinting*. In most cases, watermarking and fingerprinting is used to help to prove that a copyright violation has taken place. Hence these technologies are often referred to as forensic DRM technologies.

But both technologies also have non-forensic applications: Watermarking has, albeit with not too much success, been used to convey business rules to client devices. Examples include the Content Scrambling System (CSS) for Video DVDs and the SDMI³¹ Phase I watermark.

Fingerprinting has additional uses such as well. One example are services that automatically provide metadata to users from “listening” to the music. One use case often given is a user sitting in a pub or restaurant and, upon hearing a song he likes, activates his fingerprinting device (e.g. his mobile phone) which will recognise the song, and transmit some information to a service provider. When arriving at home, the user will find the same song as a DRM-governed audio file in his email inbox — sent by an automated system using the fingerprints to identify which song the user liked.

7. A mechanism to *report events* such as the purchase of a piece of content is also important in order to allow event-based payments to be processed. These event-based payments (e.g. “pay-per-view”) are one of the examples of new business models that DRM systems can enable.

²⁹ Reasons for such a loss in trust may be because a component type (or even an individual component) thought to be “secure” has been hacked.

³⁰ See: MPEG-21 PAT (2003).

³¹ Secure Digital Music Initiative.

Such event reports can also be of interest for organisations that are active in the collection of royalties, such as Collecting Societies (e.g. GEMA³² and GVL³³ in Germany).

8. *Payment systems* which are enabled through such event reporting systems need also to be integrated into the system. This involves either linking to a credit card or bank account, or to anonymous payment systems (often called “electronic cash”³⁴). However, both systems have problems associated with them: credit cards are, in many countries only available for adults, and electronic cash systems have not been able to attract enough users to make it worthwhile for a rights holder to accept this “currency”.

The final element³⁵ is the “glue” between the components listed above. Only through this glue, can participants in the content value chain trust the system to do what they expect it to do. Several DRM systems use *obfuscation techniques* to make the hardware and software that provide the DRM functionality resilient against reverse engineering and, more importantly, malicious attacks. Other systems use hardware support for providing the glue between different components. One example for such a system are products based on the Trusted Computing Platform Alliance’s (TCPA) specification³⁶. This specification is cited as an example for technology that has the ability to further the security and user–friendliness of DRM systems. On the other hand, the TCPA is often criticised for violating the privacy of users, as systems based on the TCPA have the potential to monitor *all* interaction between a user and his system³⁷.

IV Evaluation Criteria for DRM Systems

As indicated above, the various members of the content value chain (see Figure 4) will have different priorities as to what is important to them in a content distribution system. However, all have different interests and priorities in each of the following eight criteria: (1) how user–friendly is the system, (2) how trustworthy, (3) secure and (4) extensible is the system, (5) how can it be implemented, (6) what resources are needed for implementation and adoption, (7) how open is the system and, finally, does it (8) interoperate with other systems?

In the following subsections, these criteria are looked at in some detail. It is important to note, though, that they refer to the *entire content distribution system*, not the DRM subsystem, or even the DRM systems’ components.

IV.1 User Friendliness

User Friendliness is one of the most important criteria. The content distribution system and the DRM components that are a part of it have to be *very easy to use* for those participants in the value chain to access or manage content and rights. This is

³² Gesellschaft für musikalische Aufführungs– und mechanische Vervielfältigungsrechte.

³³ Gesellschaft zur Verwertung von Leistungsschutzrechten mbH.

³⁴ See: Asokan, Janson, Steiner, Waidner (1996).

³⁵ Of course, there are more than just nine elements that can make up DRM systems. Nevertheless the list presented here covers the most prominent and important components.

³⁶ See: TCPA (2002).

³⁷ See: Andersen (2003).

paramount especially for the consumer; why should a consumer switch to using a new system when it is cumbersome to use?

But the same argument is also true for other participants in the value chain. When there is an existing content distribution channel that offers all participants reliable revenue opportunities, why should those companies change to a new distribution method when this new method does not offer any benefits over the old one?

IV.2 Trust

The second criteria is the question of how far members of the value chain can trust the system to behave in the manner they expect. Rights holders especially will need to have enough trust in the system that it will not let their content “leak” out of the protective domain,³⁸ and that payment will be made in accordance with the business model defined for the content. At the other extreme of the value chain, the end user needs to be able to sure that access to the content in accordance with the rules agreed will be honoured.

Similar trust issues exist for the remaining participants in the value chain (e.g. payment system providers and fulfilment centres) and if they are not met, the system will not be supported by that member of the value chain. Depending on the importance of that member this may render the particular DRM unusable.

IV.3 Security

Security is the criterion that is most often listed as the top priority for DRM systems. Indeed it is important that a DRM system is secure, because it handles valuable goods — from the content itself to the money that consumers are willing to pay for it.

Recent investigations have shown that all DRM systems investigated can be broken into. Hence, none of the systems provide 100% protection against deliberate attacks.³⁹ DRM technology providers have long since acknowledged this fact and state that their systems can only be made impregnable at a fairly high cost: making the system significantly less user-friendly.

While it may be doubted that DRM systems can, in fact, be made as robust as it is sometimes claimed, one has to question, if this 100% protection is called for in the first place. As stated in Section II above, it makes no sense to secure content worth €5 using a lock costing €10. Following this argument, a DRM system needs to provide *adequate* security, not 100% security. Adequate from *all* involved parties’ perspectives, that is.

An entirely different aspect of security is the robustness of the DRM system when the content is illicitly removed from the secure container. Technology vendors of digital watermarks (which can, and often are, used in DRM systems) sometimes promise that their watermarks would survive such acts and that it would be possible to trace the content back to the person who illicitly took the content out of the container. Such functionality is often accompanied by a requirement to survive conversion of the content from the digital into the analogue domain.

³⁸ See: *Biddle, England, Peinado, Willman* within this book on page 344.

³⁹ See: Federrath (2002); *Hauser, Wenz* within this book on page 206.

IV.4 Extensibility and Flexibility

On-line distribution is a relatively new method of making content available to the consumer. It can therefore be expected that new business models will be tried — many unsuccessfully — in the next few years. It is therefore important that any DRM technology is flexible enough to deal with new ideas and concepts without costly upgrades. In that context, it needs to be taken into account that such new business models may be significantly more complex than today's relatively straight-forward subscription and "pay-per-view" models, and that they may be unimplementable on today's devices (with consequences with respect to the DRM system's implementability — see below).

Also, as the volume of DRM-protected content traded today is very small, it is important that the systems to handle the trading are able to "grow" with increasing demand. While it is unlikely that the DRM technology itself poses a limitation to such growth, the services built around DRM systems may hinder expansion and may need to be upgraded from time to time.

IV.5 Implementability

Of more interest to device manufacturers is knowing the resources needed to run a DRM system. The algorithms for a DRM system will tend to be chosen dependent on the type of device that the content is to be distributed for (is it a portable device, e.g. an ebook reader, with limited memory and processor power, or is it a desktop device such as a digital television set, or even a personal computer?)⁴⁰. It is the capacity of such devices that may severely limit the technical possibilities — and thereby the business possible models. Issues to look at include:

1. Memory requirements (RAM and ROM);
2. Processor cycles requirements;
3. Special hardware requirements (e.g. tamper resistant components, unique hardware identifier, ...);
4. Special software requirements (e.g. tamper resistant software modules, special operating system functions, ...), etc.

Also connectivity is an issue. If a DRM system needs a permanent connection to a server, the choice of types of devices which can be used for the such a DRM systems is significantly limited. This may not be a problem in some areas — and may even be part of a value-added service — but it will not work in other scenarios. For example a mobile music player that needs a constant connection to a server will not be usable when boarding an aeroplane as such radiating devices are not allowed to be switched on during flights.

IV.6 Openness

The requirement of openness has been discussed for quite a while⁴¹ and centres around the need for independent applications for accessing content (i.e. unprotected as well as DRM-governed content). It has been argued that allowing authors of shareware and open source programs⁴² to participate in the content value chain, will grow the appeal of such technology and systems and will lead to an increased use.

⁴⁰ This is because the DRM system is not the only component that needs to run on such devices.

⁴¹ See: Rump, Herre, Brandenburg, Koller, Allamanche (1999).

⁴² Which are, for example, widely used in the mp3 music environment today.

The major drawback of this openness would be that not only honest programmers would gain access to the specification but also those who are eager to provide applications that are written in order to circumvent any DRM system.

A possible way to achieve openness, while still being able to have closed and secure DRM system components, is to either formally standardise or openly declare the interfaces to such closed systems. When, in addition, the closed modules are available for a large number of different platforms and content types, shareware programmers could build their applications based on interfaces to such closed components.

IV.7 Interoperability

Closely related to user-friendliness and openness is the seventh evaluation criteria: To what extent does a DRM system *interoperate* with other systems. For example, when obtaining a DRM-protected ebook, does a consumer need to worry if it will be readable on his ebook reader at home? Or is some conversion needed? And, if so, how cumbersome (and costly) is this process?

Devices, services and content will need to be sufficiently interoperable for DRM protected content to gain widespread use, as it became evident with mp3 compressed music. While several attempts were made to distribute protected music, only a few DRM-enabled playback devices were available and — maybe even more crucial — different published recordings were protected by different DRM systems. This made it impossible to play records from content provider *X* on devices from consumer electronics manufacturer *Y*⁴³. The net result was (and still is) that most electronically distributed music is coded in mp3 *without* any protection. As there are plenty of “mp3 players” available on the market, the distribution of unprotected mp3s is inherently interoperable. Figure 5 illustrates who and what needs to be compatible with what when music is to be commercially distributed to mobile phones.

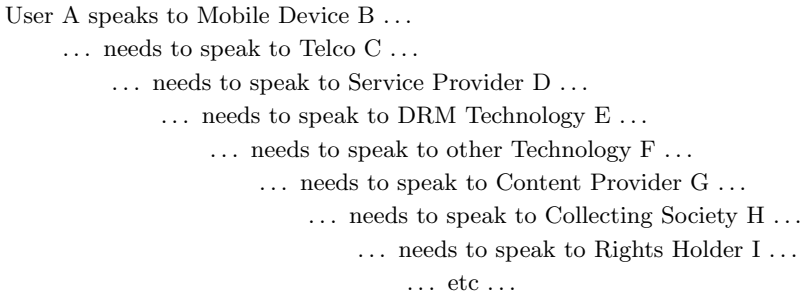


Fig. 5. Interoperability Chain

Developments such as the standardisation of interfaces to DRM systems as conducted by, for example, MPEG⁴⁴ with its MPEG-4 Intellectual Property Management and Protection⁴⁵, may offer the urgently needed interoperability between systems without prescribing the full system. DRM systems with open interfaces and components are, however, something security experts often warn against; and the breakdown of the Content Scrambling System (CSS) for DVD Video has proven that a fully-standardised DRM system does have its weaknesses.⁴⁶

⁴³ See: Rump, Herre, Brandenburg, Koller, Allamanche (1999).

⁴⁴ Ironically the same standards body that also standardised mp3 ...

⁴⁵ See: MPEG-4 IPMP Hooks (2001), MPEG-4 IPMPX (2002).

A completely different aspect of interoperability is the issue of upgrades. Does a DRM system, when upgraded (e.g. when new features are added or a security hole is plugged), provide backward compatibility? If not, how is the upgrade of the *content* a consumer has already obtained — and which, by virtue of the software upgrade, has become outdated — handled? If a user fears that the content he buys today becomes unusable tomorrow, he will certainly be very reluctant to spend any money. The same applies when the process of upgrading the content is cumbersome.

IV.8 Cost

Finally, the cost of a DRM system needs to be taken into account. The issues include:

1. The licensing cost for the underlying technology for the
 - a) Content provider's processes
 - b) Payment service provider processes
 - c) Manufacturer of devices that the end user is expected to purchase
2. The integration and implementation cost of the technology so that all affected members of the value chain become “DRM-enabled”
3. The cost to prepare the content elements for digital distribution. While this cost factor is often overlooked, this critical step includes, for example, ensuring that all rights have been cleared for the intended distribution.

As all such cost will, in the end, be paid for by the consumer, it is important that new distribution channels are more efficient, and therefore cheaper, than the old ones. Or, if additional cost is unavoidable, the introduction of new and *attractive* distribution channels may convince consumers to use — and pay for — DRM delivered content, and thereby DRM systems.

In addition, other members of the value chain such as equipment manufacturers will need to be convinced that licensing DRM system components and its integration into their devices is worth their while. In the mp3 case it seems that it would not be worth it: device manufacturers seem to be benefiting more from *not* implementing any DRM systems as mp3 players have become very popular appliances.

V Corporate DRM

Digital Rights Management is mostly associated with managing and protecting assets from publishers of ebooks, electronic magazines, electronic music, compressed and digitised films or videos, etc. However, DRM can be of assistance to *any* company or organisation that intends to protect its internal documents and memos from unauthorised access.

As such documents are content they can be protected from illicit access using the same DRM technology. For example, the annual report to be produced by the Managing Director of a company *A* may, before the report is published, be protected from being “read” by anyone but himself, the MD's secretary and the members of the Board of Directors. Furthermore, only the MD's secretary may “alter” the document and whenever she does this, an audit record will be created. At the time of publication, the access rights will be modified so that all of *A*'s employees and shareholders can “read” the document whilst there will be no “write” privileges any more. Parts of the document may even be made readable to people outside of *A* (such as journalists who

⁴⁶ See: Touretzky (2000).

may want to report on the financial situation of *A* but whom the MD may not want to disclose all details of *A*'s situation⁴⁷).

This corporate DRM example shows that the technology and the evaluation criteria discussed above also apply to the management and protection of “internal” assets of a company or organisation, albeit with a some differences:

1. The user friendliness of the system is of less significance as the company is able to force its employees to use a system even if it is cumbersome. Naturally, a user-friendly system would be beneficial as un-ergonomic components may lead to mistakes in the use of the system which, in turn, may lead to documents unintentionally leaking out.
2. Similarly, interoperability is not that important an issue in such cases because an organisation can simply select and prescribe the tools for internal use.
3. The integration of the DRM components into the existing infrastructure is, on the other hand, of higher importance as larger organisations will usually not have the ability to *replace* its systems. Such companies would need to upgrade and augment their existing system infrastructure.
4. Maybe even more important is the security and trustworthiness that the system provides. As the above example shows, the documents to be protected by the DRM system are likely to be of high value for the organisation and, therefore, it needs to be assured that the documents do not leave the secure container without approval (i.e. without a rights expression allowing this to happen).
5. A less important criterion is cost. Similar to “content companies” a cost-benefit analysis needs to be conducted. However, such an analysis is significantly easier to conduct when no consumer requirements need to be taken into account.

VI Conclusions

This paper provides an overview of the technical issues surrounding DRM and lists a variety of technologies that are needed to address several crucial aspects of digital content distribution.

But does DRM technology actually work? At the moment the answer might well be given with “no”. But a more careful appraisal might indicate that the real response has to be “we have not yet found the right business models and service offerings to make DRM worthwhile”. Clearly, this answer does not mean that DRM Technologies will not find their place in a digital commerce environment. It just means that there is still a lot to do.

VII Acknowledgements

The author wishes to thank the following people for helping in writing this article: Dirk Günnewig, Susanne Guth (who both feature in this book), my colleague Mark Isherwood and — last but not least — my wife Manon.

⁴⁷ This example also shows one crucial issue with DRM systems. They can only be as good as the weakest link (which may be a person using it): If an employee of *A* sells information he obtained from the DRM-protected report to a journalist, there are no technical means for the company can do to stop the journalist to publish the gained information. But, naturally, this “weakest link problem” also exists when no DRM system is used.