Norsk Regnesentral
NORWEGIAN COMPUTING CENTER

Report

State of the art in Digital Rights Management

A MARIAGE project report

Report no 1018

Authors Truls Fretland, Lothar Fritsch, Arne Kristian Groven

Date 06-June-2008

ISBN 978-82-539-0528-0

Norsk Regnesentral
NORWEGIAN COMPUTING CENTER

About the authors

Truls Fretland is a research scientist at Norsk Regnesentral. He recieved his masters degree in industrial mathematics from the Norwegian University of Science and Technology (NTNU) in Trondheim in 2004. The topic of his diploma work was cryptography. After finishing university he worked three years as an assistant professor in mathematics at the university college in Sør-Trøndelag (HiST). In autumn 2007 he started at NR where he works in the area of computer security.

Lothar Fritsch is a research scientist with Norsk Regnesentral. Lothars work focuses on the analysis of security and privacy requirements in upcoming application areas. Particularly he has experience on the deployment of privacy functionality into new systems with respect to requirements engineering and verification. He used to work as a researcher at the T-Mobile Chair for Mobile Commerce & Multilateral Security at Frankfurt's Johann Wolfgang Goethe – University in Germany from 2002-2007. Before this, he was employed as a product manager in IT security by fun communications GmbH, Karlsruhe, Germany where he was responsible for IT security product definitions in the areas of PKI, signature law application and secure e-payment, and additionally working on ITSEC security certification. He has received his diploma degree from the University of Saarland in Saarbrücken where he graduated with a specialization in computer security and cryptography.

Arne-Kristian Groven is a senior research scientist at Norsk Regnesentral. He is educated at the Department of informatics, Univerity of Oslo, where he also worked for one year. He has been working at the Halden Reactor Project, Institute for Energy Technology (IFE), analysing safety critial systems before joining Norsk Regnesentral in 1996. He is currently working in various security and trust projects.

Norsk Regnesentral

Norsk Regnesentral (Norwegian Computing Center, NR) is a private, independent, non-profit foundation established in 1952. NR carries out contract research and development projects in the areas of information and communication technology and applied statistical modeling. The clients are a broad range of industrial, commercial and public service organizations in the national as well as the international market. Our scientific and technical capabilities are further developed in co-operation with The Research Council of Norway and key customers. The results of our projects may take the form of reports, software, prototypes, and short courses. A proof of the confidence and appreciation our clients have for us is given by the fact that most of our new contracts are signed with previous customers.

Norsk Regnesentral
Norwegian Computing Center
Postboks 114, Blindern
NO-0314 Oslo, Norway

Besøksadresse
Office address
Gaustadalléen 23
NO-0373 Oslo, Norway

Telefon · telephone
(+47) 22 85 25 00
Telefaks · telefax
(+47) 22 69 76 60

Internett · internet
www.nr.no
E-post · e-mail
nr@nr.no

Title	**State of the art in digital rights management**
Authors	**Truls Fretland, Lothar Fritsch, Arne-Kristian Groven**
Date	19-May-2008
Year	2008
ISBN	978-82-539-0528-0
Publication number	1018

Abstract

Digital Rights Management has been widely discussed from many prespectives. By far most publicity gained the term with the media industry's wish to enforce copyright and licence policies for digital media consumptions using DRM technology. The resulting discussion gave rise to a debate about corporate power, fair use, and the future of modern computer concepts such as Trusted Computing. In the shadow of this public debate about the future of digital media usage, it is not always easy to tell apart science fiction, the frontier of research, and the properties of existing DRM systems that are in use.

This report summarizes contemporary DRM systems, their principles, their assumptions and their effectiveness. It is intended as a survey on the state of the art of today's DRM products.

Keywords	DRM, intellectual property, digital rights management, content security, archival.
Target group	General public, journalists, web developers
Availability	Public
Project number	320375
Research field	Multimedia data formats, long-time availability of personal digital media, information security & privacy, digital rights management
Number of pages	34

Preface

"Making Rich Media Accessible for Generations": The driving vision behind MARIAGE is the prospect of advancing technology in the area of rich media in order to overcome current system limitations in search, navigation, retrieval and use over time. Aimed at signifying the difference between current and a new generation of multimedia systems, MARIAGE intends to enable the benefits of rights managed, intelligent metadata handling and semantic driven, search, navigation, retrieval and usefor an extended period of time (20+ years). The main theme of MARIAGE is the ability to publish and access rich media material over a long period of time.

The MARIAGE project is funded by the Norwegian Science Council.

Contents

1 Introduction

This report summarizes contemporary DRM systems, their principles, their assumptions and their classification. It is intended as a survey on the state of the art of today's DRM products.

Intellectual property rights (IPR) has a substantial impact on a trusted, long-term storage of rich media documents. The IPR issues in rich media are more complex and significant than for traditional media and if not properly addressed can impede or even prevent long-term storage and access activities. Simply copying digital media onto another medium, encapsulating content, or migrating content to new platforms, all involve activities which can infringe. Some of the additional complexity in IPR issues relates to the fact that digital documents are also easily copied and re-distributed. Rights holders are therefore particularly concerned with controlling access and potential infringements of IPR. Therefore engendering trust among customers is essential in long time preservation of rich media.

In Section 2 we give an overview of the terminology and how these words relate to each other. Section 3 is the main part, containing a brief overview of current DRM systems, namely the proprietary systems from Microsoft and Apple, and an open standard from the MPEG group. Several other DRM systems is also mentioned. In Section 4 we discuss problems beyond technology that need to be solved for DRM system to succeed. We conclude by giving some guidelines for use of DRM in the context of long time preservation.

2 Taxonomy of Digital Rights Management

Many views on DRM exist, but terms, technology, copyright laws and the limitations of DRM are a broad topic with much potential for confusion and myth-building. This section of the report on DRM defines and explains the basic terms and concepts and the context of DRM.

2.1 Stakeholders in Digital Rights Management

The number of parties interested in or affected by DRM is high. In a stakeholder analysis for the music industry alone, the INDICARE project identified eight different stakeholders [INDI2004]. As this list focuses on the revenue stream, more stakeholders can be added, for example archives, libraries, broadcast media combined with Internet, streaming media companies, and others. The stakeholders identified by INDICARE are shown in Illustration 1.

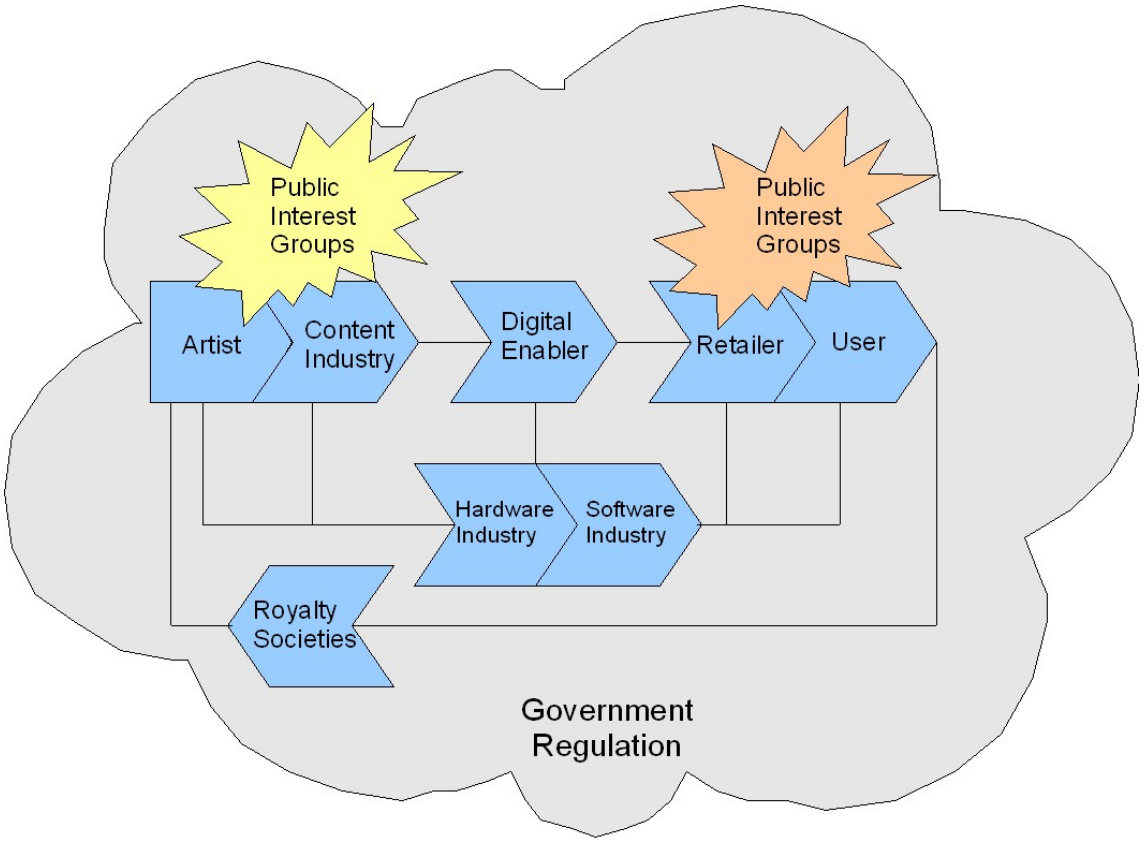

Illustration 1: Stakeholders in DRM: The example of the digital music industry.

In the music case, the stakeholders have interests and functions found in INDICARE as presented below in Table 1. Some of the claims might not hold for all real-world stakeholders, though. However, what is clearly illustrated in this analysis is the fact that the stakeholders' interests are conflicting, and thus hard to model into a single policy for DRM that will satisfy all stakeholders' expectations. However, few of the stakeholders might have the economic power and political impact to implement their view on DRM, while other stakeholders might not have the ability to excercise such power. This observation is the source of various strong conflicts along the lines of DRM in public discourse, politics and lobbyism.

Stakeholder	Description	Interests in DRM
Artist	Creators of content such as artists, singers, songwriters, composers.	(1) Wish to protect their Intellectual Property. (2) Are for fair use, free speech, and artistic freedom to innovate and create new content. (3) Well-known artists are probably negatively affected by internet piracy, whereas less popular artists might profit. (4) Are not in favor of government control. (5) Do not wish to enforce current copyright law.
User	Users of digital content such as consumers (individual), schools, libraries.	*Consumers*: (1) Do not like to be restricted in their usage, advocate fair use, free speech, privacy, and do not like new regulations and laws.? Do not like to be treated as criminals. *Schools / Libraries*: (1) Privacy and fair use concern them. (2) Both do not wish to enforce current copyright law and are against excessive technological and legal control.
Content Industry	Recording Industry Association of America (RIAA), Content Owners (Disney), Music labels (Sony, BMG).	(1) Wish to protect Intellectual Property. (2) Desire government regulation, DRM per federal mandate(s) and private efforts. (3) Anti fair use, believe it gives hackers an excuse to circumvent DRM. (4) Affected negatively by internet piracy. Fight with technological (DRM) and legal solutions (lawsuits). (5) Wish to enforce current copyright law.
Government	Government departments and bodies which establish and maintain the legal & regulatory environment for other stakeholders.	(1) Have to balance various requirements such as piracy, privacy, fair use, copyright on a political, regulatory level. (2) Represent to a certain extent all stakeholders. Are not heavily affected by Internet piracy (possibly loss of tax revenue). (3) Enforcement of copyright related laws is the result of the power exercised by the various stakeholders.
Digital enablers	Companies which support the distribution of digital music to users. Companies from the telecommunications industry, DRM providers, ISPs.	(1) Have to balance various interests both of content providers (copyright protection) and those of users (fair use, privacy). (2) Not directly affected by internet piracy. (3) Try to find market-driven solutions, instead of government regulations, by taking into account the concerns of both the content industry and users. (4) Some have been sued by content providers.
Hardware industry	Hardware companies producing end-devices for users of digital content (e.g. PC, PDA, CD-player, or mobile devices). Companies like Sony, Philips, Nokia, IBM, Ericsson, or HP.	(1) Try to balance privacy, fair use with copyright protection. (2) Not directly affected by internet piracy. On the contrary, legal or illegal demand for content increases demand for end-devices. (3) Want market-driven solutions, instead of government regulations. (4) Do not wish to enforce current copyright law.

Stakeholder	Description	Interests in DRM
Software industry	Software for the production, distribution and consumption of digital content. Companies like Microsoft, Linux, Apple, Real Networks.	(1) Have to balance copyright protection and privacy, fair use. (2) Some effort on Trusted Computing under way (Microsoft) with Next Generation Secure Computing Base (NGSCB). But others try to remain „open“ (Linux). (3) Some negatively affected by internet piracy, others not. (4) Have also a perspective as artists (creator of content) as well as content industry. (5) Try finding market-driven solutions, instead of government regulations.
Public Interest Groups	Public Interest Groups support mainly artists and users of content. Organizations such as Net Coalition, Electronic Frontier Foundation (EFF), Electronic Privacy Information Centre (EPIC).	(1) Wish to preserve privacy, free speech, fair use, and artist freedom. (2) Are not negatively affected by internet piracy. (3) Are against government regulations and combat technology solutions restricting users and threatening user rights. (4) Do not wish to enforce current copyright law.
Retailer	Distributors of digital music such as „traditional“ retailers, e-retailers, web sites, portals. Example. B&N, Amazon.com, Music Net.	(1) Have to balance interests of both, content providers (copyright protection) and of users (fair use, privacy). (2) Are negatively affected by internet piracy. (3) Try to find market-driven solutions, instead of government regulations.
Royalty Society	Act mainly in the name of artists and content providers for the collection of royalties.	(1) Wish to protect Intellectual Property. (2) Are negatively affected by internet piracy (e.g., loss of royalties due to illegal streaming of music).

Table 1: Music sector DRM stakeholder analysis from [INDI2004].

2.2 Media Business Models and Digital Rights Management

DRM is used to secure either one of two stakeholder interests in a business context. It either helps in controlling the use of copyrighted material, or is used to secure certain media business models against the dangers of third-party digital reproduction. DRM is deployed to add security to the two interests in the media business. When structuring different ways of deploying business models that use DRM, they are usually classified by either the degree of control over media use they implement, or by the technological efforts that have to be implemented on various points of the media infrastructrue to be able to implement the model. In Table 2, the gradient from to control (bottom) to total control (top) is elaborated. The table follows [Sobe2003] in its analysis of control levels and related technological complexity.

Business models are not unified within the media industry. Value chains exist for broadcast production, music exploitation, art, literature, patents and many other kinds of media objects. Aside from the original creator-consumer value chain, rights for possession, use or exploitation of media can be granted, recalled, temporarily licenced or licenced with constraints (e.g. geographical regions). A single piece of media content (for example a musical piece) can have many complex rights attached to it – ownership, playing licence, recording licence, broadcast licence, internet licence, library licence, and so on. It is near to impossible to find a unified

«business model». A value chain analysis is, however, a valuable tool for the analysis of the complexity of the introduction of DRM for a particular part of the media market, as the value chain will reveal the other stakeholders that have to cooperate to implement DRM with high control levels.

Often, DRM is said to enable new digital media business. This refers to media consumption models such as pay-per-view, video-on-demand, or pay-per-use for software. Here, some form of DRM is required to keep users from using media without payment. Few of these models have been implemented outside of the pay TV world.

A major problem for the deployment of DRM is the fact that the base platform for secure DRM must be deployed to the majority of users or consumers before the protection becomes effective. Media players must somehow support the DRM scheme, otherwise users might simply circumvent the DRM systems. Rolling out new media technology to all its users at the same time is a problem of the magnitude of the introduction of new TV standards – where every new technology makes the target market smaller at first. The existing deployments of DRM hence all focus on particular communities that have a high penetration rate of the DRM technology (these will be discussed below in section 3).

Copyright control level		Business model	Technology base requirements	Control over systems
High	**8**	Total control beyond copyright. Producers and publishers enforce any media usage policy with technical means.	Technological and legal enforcement on all parts of the media infrastructure and on all possible recording and recoding equipment and distribution channels.	**High**
	7	Access, copy & redistribution control with producers and infrastructure.	Technological equipment on all components, legal framework for its mandatory deployment.	
	6	Access, copy & distribution control over media with infrastructure support (e.g. DVDs)	Requires special equipment and cooperation of the user to use it.	
	5	Strict access control, but no copy & redistribution control (e.g. Pay TV)	Requires special equipment to access media.	
	4	Control over access, copy and redistribution of digital content (e.g. Ebooks)	Requires reader software or players compatible to the system.	
	3	Acess control, but no copy or redistribution control over materials.	No technical requirements on user side.	
	2	Tax and royalty system	No technical requirements on user side.	
	1	Noncommercial use levy	No technical requirements on user side.	
Low	**0**	Anti-Copyright: No copyright exists. Creators are compensated with «tips», government subsidies, or their own ressources.	Unclear. No enforcement necessary, but creators might insist on being recognized as creators. Could involve watermarking.	**Low**

Table 2: Basic setup for DRM business models based on [Sobe2003].

Summarizing this section, a DRM system is often related to a business model for media use. The specification of the DRM system's properties, the extent it has to be installed on all system components ranging from producers to end users, and its restrictiveness to the user's wishes to use a system all depend on the business concept that is to be secured with DRM.

2.3 Roles and Terms in Digital Rights Management

This section defines concepts, roles and terminology that will be used for the remainder of this report. We introduce the scenario whithin we see DRM, the main actors and their interactions.

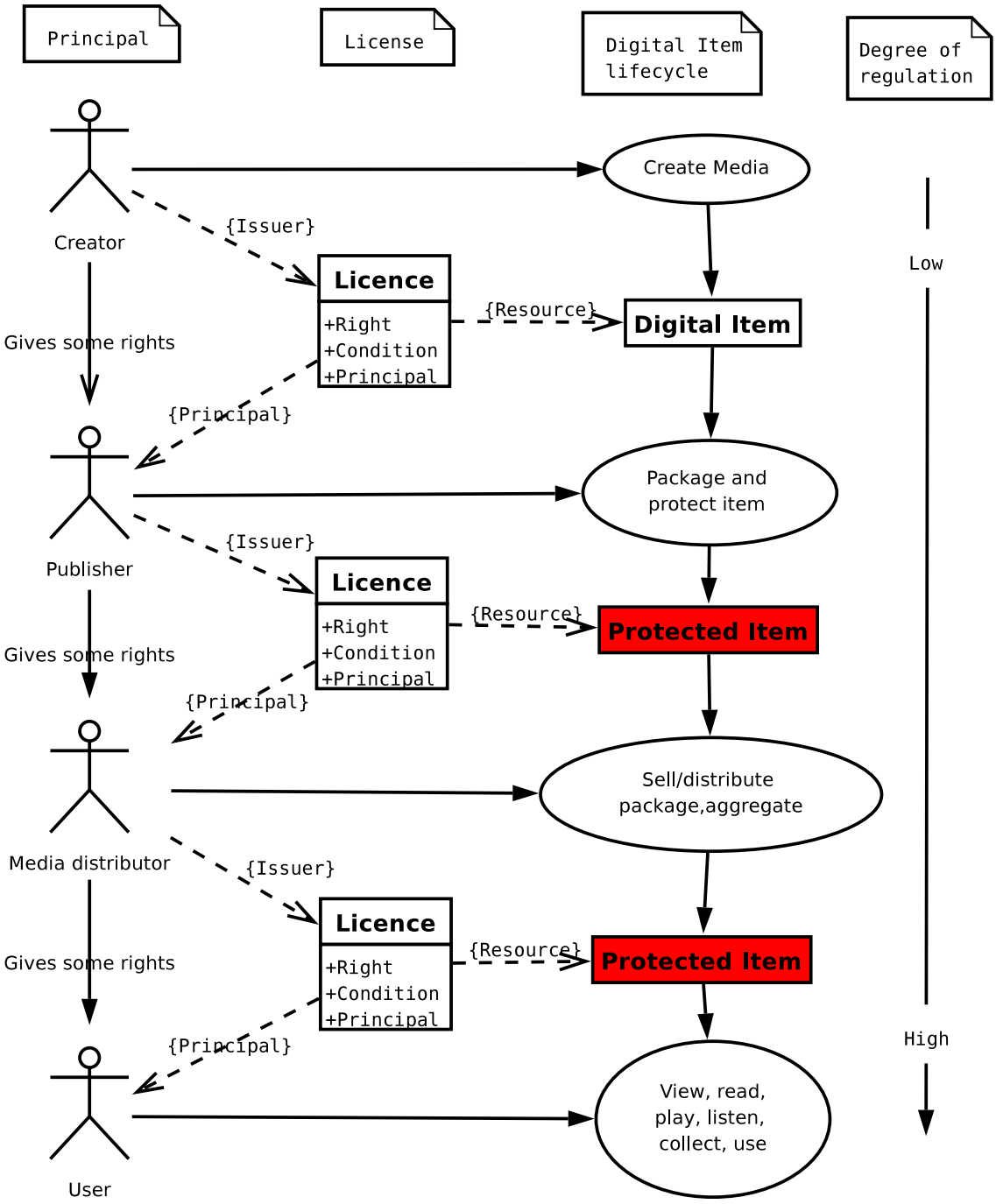

Illustration 2: Lifecycle of digital media object

Illustration 2 shows the lifecycle of a digital media object, encapsulated in the Digital Item, and the actors involved in the cycle (the illustration resembles UML-style, but is not formal). The creator of the media has all rights, issues rights of the media to one or more publishers. Depending on the rights given, the publisher further issues a license to one or more media distributors. Each actor in the illustration may use the media according to the license that is issued with the media. E.g. the user may play the protected media 3 times, but may not issue license to others.
The license is the statement that give a principal rights to use one or more Digital Items. The language for expressing rights in MPEG-21 is named Rights Expression Language (REL) and is based upon eXtensible Rights Markup Language (XrML). In XrML [Cont2002] the license contains the identity of the issuer and a grant. A grant specifies that a principal has some rights over a resource under certain conditions. E.g "Alice is given the right to play the song Wonderland one time before december 2007". The grant consist of four parts, namely:

1. The *principal* ('Alice') to whom the grant is issued.
2. The *right* that the grant specifies ('play')
3. The *resource* that is the media object to which a principal is granted a right ('the song Wonderland')
4. The *condition* under which rights can be exercised (' one time before december 2007')

Table 3 gives an overview of the roles and the terms that are used in this paper, common names used in other papers, together with a definition of the term.

Principals / roles	**Names used in other papers**		**Definition**
Creator	Content producer, artist	P r i n c i p a l	Owner of the copyright in a work. He/she holds the exclusive right to use or authorize others to use the work on agreed terms
Publisher	Rights holder, Copyright holder, content provider		Acts in the name of the creator. Compiles and packs creations to provide the media distributors with media.
Media Distributor	reseller		Distributes the media to the end user. Apply to a Rights Holder for a license to exploit the creation.
User	consumer, customer		Person who wants to make use of the digital media
Terms			
Digital media	Intellectual property, entity, creation, content, resource, digital assets		The objects that are made by the creator subject to a set of rights.
Digital Item*	Object, digital object, media object		Digital media together with metadata.
License*			Grant given by an issuer
Grant*			Contains right(s), resource(s), condition(s) and principal(s)
Right*			Specifies an action or activity that a principal may perform using a resource
Resource*			Identifies the object with associated rights to be used in a license
Conditions*			Specifies the terms, conditions and obligations under which rights can be exercised, e.g. a time interval within which a right can be exercised, a limit to the number of times a right can be exercised and a fee that must be paid.

Table 3: Roles and terms in DRM (* : terminology used in MPEG-21 REL)

2.4 Typology of DRM systems

This section will present a basic DRM threat model, followed by a taxonomy of DRM system types that is made along the efforts of a DRM system to stop a copyrighted object from being used. This typology will be later used to classify the DRM systems analyzed in the main part of this report.

2.4.1 Threats to copyrighted objects

Being an information security system, DRM requires a threat analysis before any technological measure for protection can be deployed. For technical security, many of these threats can be reduced to threats to confidentiality, integrity, availability and non-repudiation. However, in the face of the numerous applications and business interests in DRM, threats also have to be viewed in the context of DRM. A threat model for DRM was sketched in [ClNe2000], which is presented in brief in this section. Threats to DRM systems are posed by performing certain actions on the copyrighted objects that are not covered by the license granted. Threat agents are entities that have access to the object. Threat targets are the computer system components and networks that store and transport the copyrighted objects.

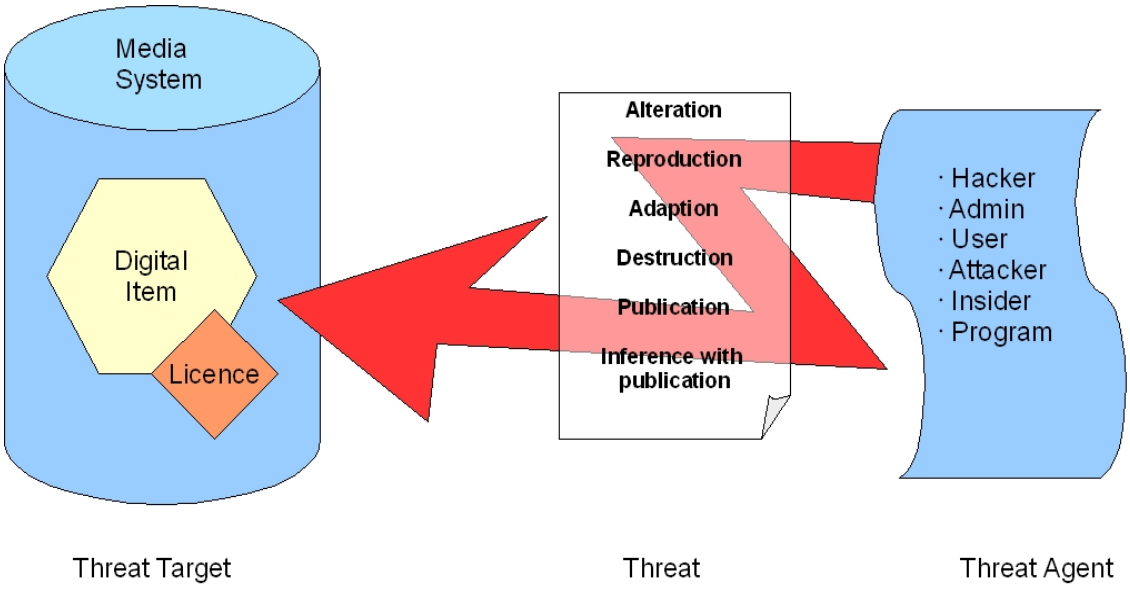

Illustration 3: Threat model for DRM.

The basic threats to copyrighted objects and the systems they are handled with are shown in Illustration 3. While these threats relate to the copyrighted object, most practical attacks on DRM systems are carried out by exploitation of weaknesses in the overall system security concepts. How, after all, is a piece of digital media, or a key that can decrypt such a piece, protected from a program accessing it on a hard disk or a memory card? Here, security models and their practical implementation come into play. The quality – and price – of the underlying information security measures are decisive about the threat impact.

2.4.2 Types of DRM systems

In [ClNe2000], DRM systems are classified into passive and active system types. Passive DRM systems are systems used on objects while they are under the control of the creator or legal user, or systems used to track illicit use. Active DRM systems are systems that act to stop a user from committing a license violation. Actions in active DRM systems range from notification of either

the user or the rights owner up to object destruction and denial of service. Generally, active DRM is thought to stop a computer system from using the copyrighted object until a license is obtained.

Passive DRM systems	
	Media protection while under control of creator, publisher, distributor
	Digital item protection while in transit to other systems
	Digital item protection while in control of a licensee or recipient
	Tracing of illegal copies
Active DRM systems	
	Notification of the rights under the licence
	Identification of licensee, identity management
	Enforcement mechanisms on client-side, including: ● prevention ● action-logfiles(«spyware behaviour») ● recording of efforts to breach the licence ● reporting to copyright-owner or other entity
	Deletion or destruction / access denial of digital items

Table 4: DRM typology according to [ClNe2000].

2.4.3 Connection typology

Further features of DRM systems are their need for a playback device or other node of the technical system to be connected to the DRM infrastructure. Some systems are stand-alone, others need to be connected to a DRM system to be able to play digital items. Other systems work offline and independent of connections to DRM servers when the items are being used. In Illustration 4, we show a pay TV example as connected online system. As a representative of independent offline systems, we show the DVD zoning protection.

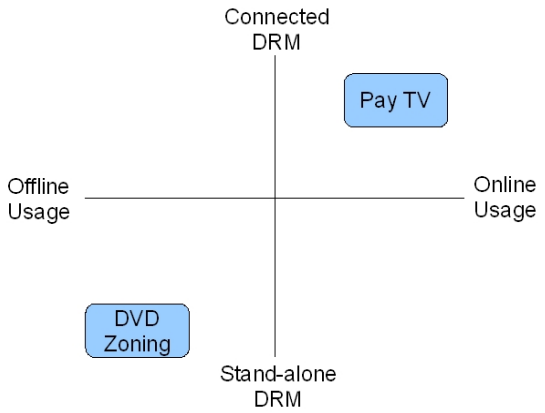

Illustration 4: Connection typology for DRM systems.

The typology will be used to classify the DRM systems in the rest of this report.

3 Current DRM technology

This section provides an overview of contemporary DRM systems that are in use with the media industry and with technology vendors. The focus is on relevant, practically applied systems rather than research prototypes. For this overview, the Microsoft DRM system has been chosen as an important representative of DRM on dektop PC media use. For portable devices and internet distribution, we will take a look at Apple's DRM concept with iTunes and their portable devices iPod and iPhone. For general insight into the interdependence of data formats, media and DRM, we will introduce the DRM scheme that is specified in the MPEG-21 media standard. Finally, some other relevant approaches are summarized, e.g. mobile content protection following the OMA specification as it is implemented e.g. on Nokia mobile phones.

3.1 Broadcasting with encryption: Protected subscriber TV

One of the oldest consumer-oriented DRM concepts is the encryption of television signals on satellite and cable TV systems. In this concept, the technical protection is designed to secure the transport of media against use by non-subscribers of a TV network. Upon delivery to a subscriber, the signal is decrypted with a special TV receiver. Subscribers are authenticated with a smartcard containing keys that reflect their subscription details.

As the media on cable TV is only protected between the TV broadcasting infrastructure and the subscribers' decoder, the subscriber can use any technology to view, record or store media.

Some systems allow the update of keys and subscriptions and the regionalization of content. Usually, these functionality is implemented in the decoder software.

Protected Subscriber TV	
DRM type (Table 4)	Passive DRM
DRM restrictiveness (Table 2)	Level 3
DRM dependency (Illustration 4)	Online / Connected upon delivery

Table 5: Protected subscriber TV classification.

3.2 Microsoft's Windows Media DRM

Windows Media DRM is a software platform aiming at the protected Internet delivery and playback of digital items on personal computers, portable players and networked playback devices (such as TV boxes, DVD players). The system is designed to manage complex license models for digital items in various media. Every aspect of media consumption can be expressed in grants called «business rules» that police the usage of digital items.

Microsoft offers software components and software development libraries for protection of digital items, license management and playback of the digital items. Windows Media DRM uses encryption on the digital items. Users need to buy a license (containing a key and some policy) to be able to play the object. Licenses can expire and therefore might need updates. The user side of Windows Media DRM has a license store where all the user licenses are kept.

Components of Windows media DRM are:

- Windows Media DRM 10 for Portable Devices. Designed to allow devices such as portable audio and video players, set-top boxes, and mobile devices with audio and video capabilities to directly or indirectly acquire and play Windows Media–based digital items.

- Windows Media DRM 10 for Network Devices. Designed to allow devices such as set-top boxes, DVD players, digital media receivers, and digital audio receivers to play back Windows Media–based digital items that reside on another computer on a home network.

- Windows Media Rights Manager 10 Software Development Kit (SDK). Enables content owners to encrypt digital items with a key and deliver licenses to desktop computers and devices for playback of protected digital items.

- Windows Media Format 9.5 SDK, DRM Addendum. Enables independent software vendors (ISVs) to develop applications that can play protected Windows Media–based digital items.

- Windows Media Data Session Toolkit. Used to deliver protected digital items to a computer through physical media in an easy and secure manner.

- Windows Media Device Manager 10 SDK. Enables software vendors or equipment manufacturers to develop applications used to transfer digital items from computers to compatible portable devices.

- Windows Media Portable Device DRM (PDDRM). Enables portable device manufacturers to develop devices that decrypt digital items protected by using Windows Media DRM.

The process of DRM application with Windows Media DRM is specified in seven steps:

1. Packaging. Here, the protected ditigal items are encrypted with their rights and license terms.

2. Distribution. Encrypted digital items can be distributed to resellers, web servers and other repositories.

3. License servicing. A license clearing house is is established. Here, the playback devices will seek licenses to acquire for playback of the digital items.

4. Media acquisition. A user retrieves a protected digital item from a server.

5. License acquisition. Media players will try to retrieve a license, or prompt the user for further information or payment purposes.

6. Retrieval of license. The user receives a license to use the digital item.

7. Playback. With a valid license in the license store, the digital item is decrypted and played or copied to another device.

Illustration 5 shows the steps for managing protected digital items in Windows Media DRM.

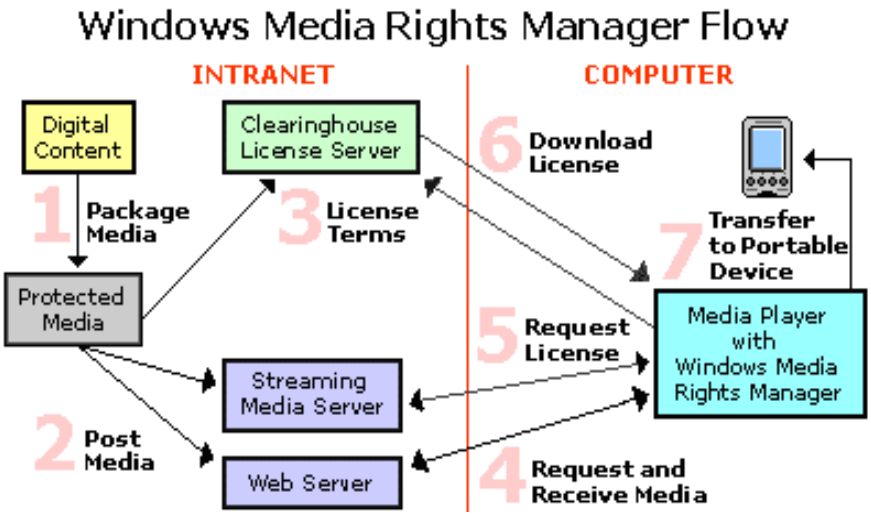

Illustration 5: Windows Media Rights Management (from http://www.microsoft.com/windows/windowsmedia/howto/articles/drmarchitecture.aspx)

Microsoft controls software vendors that include Windows Media DRM into their playback devices and players. Windows Media DRM contains mechanisms to exclude certain players or DRM components from playback. According to Microsoft, they will be used to exclude insecure players from the DRM platform. It establishes a mechanism to control the player software used with Windows media DRM. Software developers must be certified by Microsoft before they can distribute players with the DRM system.

The licenses contain a set of «business rules» that are set up during the packaging phase. These rules determine the possible usage of the digital item. Business rules can allow pay-per-view, free preview, playback at certain times of the day, and expiration of a license. Many other possible rules can be configured with the licenses.

Microsoft Windows Media DRM	
DRM type (Table 4)	Active DRM
DRM restrictiveness (Table 2)	Level 3 or higher, typically 4
DRM dependency (Illustration 4)	Online / Connected upon delivery Connection required if licences expire

Table 6:Microsoft Windows Media DRM classification.

3.3 Advanced Access Content System (AACS)

The Advanced Access Content System (AACS) is developed by AACS Licensing Administrator (AACS LA), a consortium that includes Sony, Disney, Intel, Matsushita (Panasonic), Toshiba, Warner Bros., IBM and Microsoft. It has been operating under an "interim agreement" since 2005 because the final specification has not yet been finalised. AACS is a new standard for content distribution and digital rights management, intended to restrict access to and copying of the next generation of optical discs and DVDs.

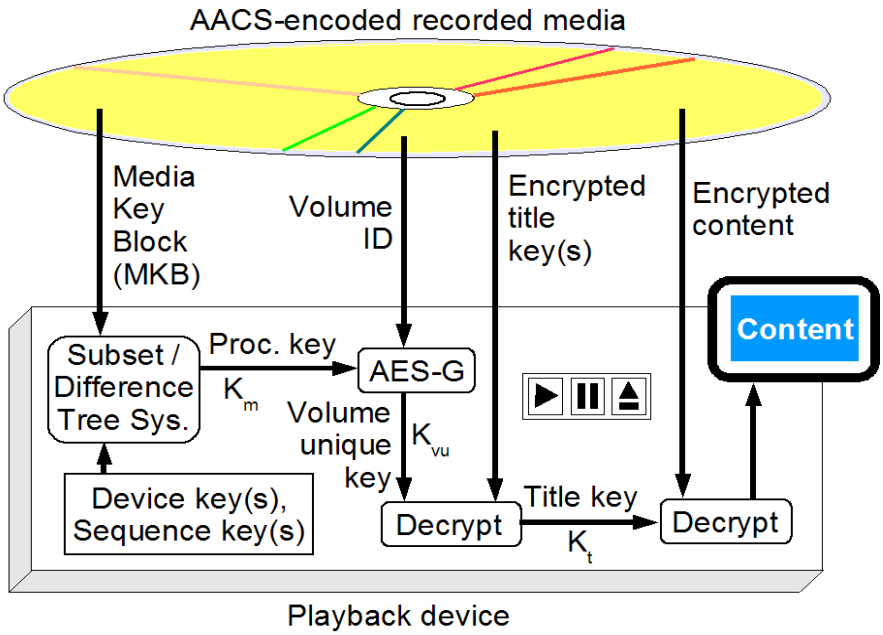

Illustration 6: AACS decryption process. The source is http://en.wikipedia.org/wiki/Image:AACS_dataflow.png

Cryptography is used in AACS to control the use of digital media. It encrypts content under one or more title keys using AES, the Advanced Encryption Standard. Title keys are derived from a combination of a media key (encoded in a Media Key Block) and the Volume ID of the media, e.g., a physical serial number embedded on a pre-recorded disc.

The approach provisions each individual player with a unique set of decryption keys which are used in a broadcast encryption scheme. This approach allows licensors to "revoke" individual players, or more specifically, the decryption keys associated with the player. So if a given player's keys are compromised and published, the AACS LA can simply revoke those keys in future content, making the keys/player useless for decrypting new titles.

The technique used here is called the Subset Difference technique which is a big and largely secret collection of *never changing* Processing and Device Keys derived from one Master Device Key (or a few). Device Keys can in essense be used to derive a desired Processing Key and because only a few Device Keys are given (hidden in the Player) only a part of all Processing Keys are "reachable" by any given player.

Illustration 7 can be used to explain the Subset Difference technique, showing a specific software player, illustrated as a truck, together with all the Processing Keys, illustrated by a «parking spots» (P) in the tree, i.e. the leafs in the tree. The truck is unable to back and is constrained by the its unability to make sharp turns, only 90 degrees at its best. Therefore the

green «P»s (Processing Keys) are reachable while the red ones are not for this specific truck, i.e. player.

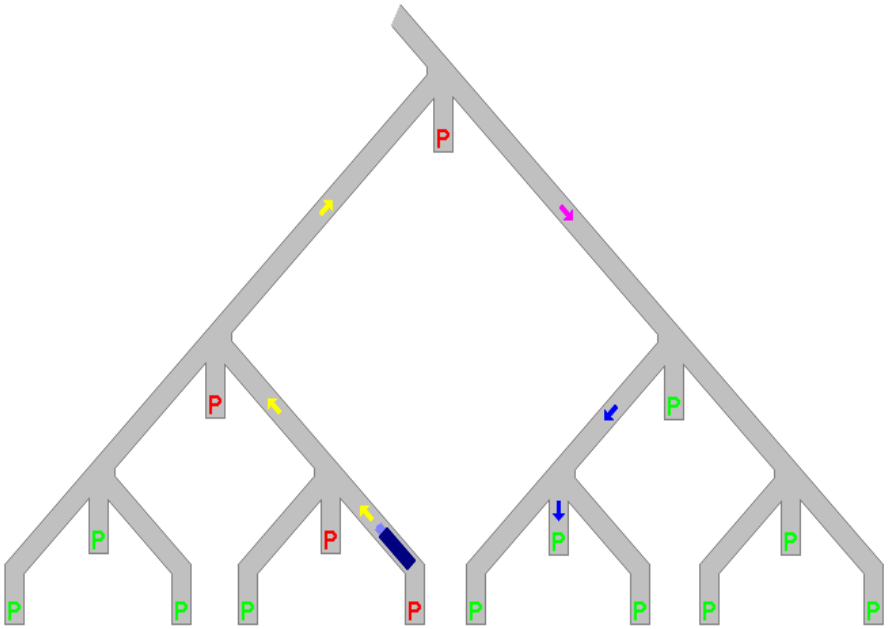

Illustration 7: A software player, illustrated as a truck, can reach the green Processing Keys, but not the red ones.

Instructions are given in the Media Key Block (MKB) file on the AACS-encoded media you want to play, telling the player which Processing Key (parking spot) it should try to reach. If this parking spot is reached, The Processing Key decrypts the C-value in the MKB file, giving the Media Key as a result. If not, the player has been revoked. In AACS, driving up this three does not take place. Instead, a Device Key given (to you) indicates where to go down, towards the leafs. By using AES-G3, either a left or right sub-Device Keys can be calculated, or (possibly) a given Processing Key.

AACS also has tracing of traitors called «Sequence keys». If an attacker tries to keep a compromised key secret, by only publishing decrypted title keys, it can still be traced. AACS allows different versions of short sections of a movie to be encrypted with different keys. A certain player will only be able to decrypt one version of each section. By embedding a digital watermark in the different versions and analyzing what sections of the movie the attacker publishes, the compromised keys will eventually be identified and revoked.

A feature called «Managed copy» is not included in the interim standard, but it is expected to be a part of the final AACS specification. Here consumers can make legal copies of films and other digital content protected by AACS. This requires the device to obtain authorization by contacting a remote server on the Internet. Possible «Managed copy» scenarios include:

- Create a full-resolution copy for storage on a media server
- Create an exact duplicate onto a recordable disc for backup
- Create a scaled-down version for watching on a portable device

Sources:

Wikipedia summary on AACS:
http://en.wikipedia.org/wiki/Advanced_Access_Content_System (accessed 8-May.2008)

Understanding AACS (including Subset-Difference) , Doom9's forum:
http://forum.doom9.org/showthread.php?t=122363

AACS LA LLC: Advanced Access Content System (AACS): Introduction and Common Cryptographic Elements, v0.91, 17-Feb-2006

Advanced Access Content System (ACCS)	
DRM type (Table 4)	Active DRM
DRM restrictiveness (Table 2)	Level 8
DRM dependency (Illustration 4)	Offline, but possibly connected upon «managed copy» or download of new content. Device binding of online content possible. Risk of blocking out older hardware on newer media.

3.4 Apple iTunes “Fair Play”

Reliable technical documentation on Fairplay is sparse. Most of the information in this section is based on Wikipedia pages as referenced at the end of this section.

FairPlay is a digital rights management (DRM) technology created by Apple Inc., based on technology created by the company Veridisc. FairPlay is built into the QuickTime multimedia software and used by the iPhone, iPod, iTunes, and iTunes Store. Apple's approach protects solely music purchased from the Apple iTunes music store. The iTunes desktop software for Macintosh and Windows personal computers is the central entity in the scenario. For each user, iTunes manages the collection of music files and their distribution to players and other computers.

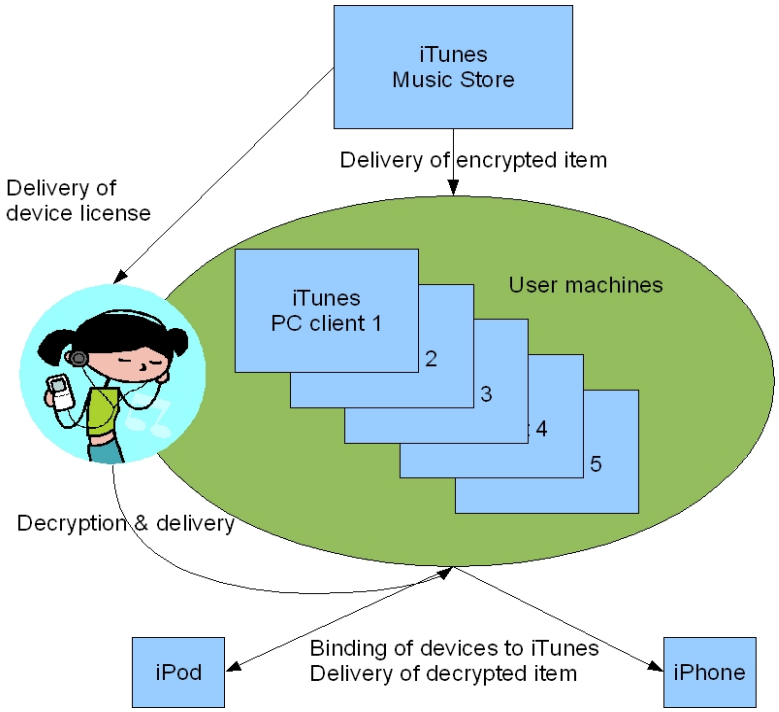

Illustration 8: Apple iTunes & Fairplay DRM use case.

Any protected digital item purchased from the iTunes Store with iTunes is encoded with FairPlay. FairPlay digitally encrypts AAC audio files and prevents users from playing these files on unauthorized computers. The majority of FairPlay-encrypted digital items are purchased through the iTunes Store, using the iTunes jukebox software. The iTunes jukebox software relies on Apple's Quicktime multimedia software for decoding and playback of the encrypted items. Every media player capable of utilizing QuickTime is capable of playing back FairPlay-encrypted files, including RealPlayer, Media Center, and Media Player Classic.

Apple's principal approach defines that every user of digital music can use five different computers to handle the music. These five machines are registered with a user account. Music items are downloaded to iTunes in encrypted form, containing the encoded decryption key for the musical piece. To play the music, iTunes will obtain a license from Apple. Now the music item, including the encrypted key for the music decryption, and the license for the music key, can be used to decrypt the music item. As the iTunes PC software is the only tool that can

upload music to an iPod player (which has a unique ID), iTunes can control where the decrypted music item will be stored at.

Fairplay therefore allows a user to use purchased music on several of his devices or computers, but prevents large-scale music sharing among users. However, iTunes will create audio CDs made of purchased music – which can be encoded back to digital music formats. Fairplay is only implmented on Apple players (iPod, iPhone, iTunes). Hence, all other MP3 players and mobile phones are excluded from buying music on the iTunes music store.

Several authors claim that Apple does not primarily target copy protection, but binding services to Apple hardware with FairPlay, thereby promoting the sales of iPods [Fish2004].

Sources: Wikipedia, http://en.wikipedia.org/wiki/FairPlay , «How fairplay works», http://www.roughlydrafted.com/RD/RDM.Tech.Q1.07/2A351C60-A4E5-4764-A083-FF8610E66A46.html (18-Oct-2007)

Apple iTunes FairPlay	
DRM type (Table 4)	Active DRM
DRM restrictiveness (Table 2)	Level 6
DRM dependency (Illustration 4)	Online / Connected upon purchasing Offline playback Online / Connected upon copying items to new players.

Table 7:Apple iTunes FairPlay classification.

3.5 The MPEG-21 DRM architecture

«MPEG-21 is an open standards-based framework for multimedia delivery and consumption. It aims to enable the use of multimedia resources across a wide range of networks and devices» [BVHB2003] The words «transparent» and «interoperable» are often used to describe MPEG-21, which captures most of its essence: The user of multimedia content should be able to use the content that the user has the rights to use independent of which device, platform, content format and network the user chooses.

3.5.1 Overview

The MPEG-21 standard is more than just a Digital Rights Management system, it is in a sense a media object management system. However, it is possible to use MPEG-21 as a framework for exercising digital rights with specified parts in the standard.

The two main concepts of MPEG-21 are the Digital Item and the User. The Digital Item is the multimedia resource(s) (e.g. a music album, a book) together with metadata. The user is the entity that make use of the Digital Item at the different stages of the value/delivery chain. In our terminology we defined User as the consumer, whereas in MPEG-21 the User could be any of the roles in the value-chain; creator, publisher, media distributor, user and so on.

The intended users for MPEG-21 are those who need a framework and an infrastructure for distributing and consuming multimedia content. Some examples of applications are: Digital libraries, broadcasting, publishing, music/video releases, asset management, trade transactions and e-health.

3.5.2 Components

The MPEG-21 standard currently has 18 parts, and will probably not have more [Ian Burnett -MPEG-21 slideshow]. Part 2, 3, 7, 10, 18 are concering the digital item; i.e. how to declare it (Digital Item Declaration), how to identify (Digital Item Identification), how to access transparently (Digital Item Adaptation), how to process (Digital Item Processing) and how to stream (Digital Item Streaming).

Part 4 of MPEG-21, Intellectual property management protection (IPMP), is MPEG's equivalent of digital rights management, supported by part 5, Rights Expression Language (REL) and part 6, Rights Data Dictionary (RDD).

The main parts of interest will be described in greater detail below.

3.5.2.1 Digital Items

A Digital Item is composed of resources and metadata that is structured in a markup-language called Digital Item Declaration Language (DIDL). The resources are the multimedia content and the metadata contains information about and belonging to the content. The structure of the item displays the relationship between parts of the item. Illustration 9 shows an overview of the Digital Item.

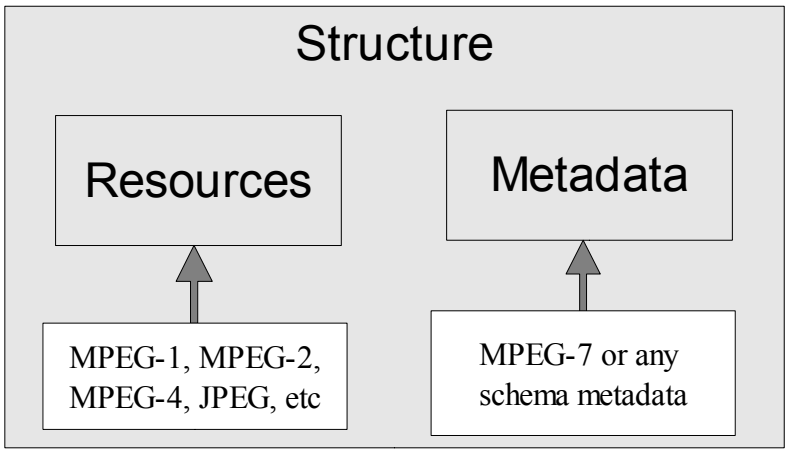

Illustration 9: The structure of a Digital Item

3.5.2.2 IPMP components

«MPEG-21 does not fix a particular DRM-system, but assumes that IPMP functionality is provided by vendor-specific IPMP tools that can be downloaded and made accessible to the terminal as necessary. IPMP tools may implement basic functions such as decryption and watermarking, or may implement complete digital rights management systems in their own right.» [ShSa2006]

The IPMP components protects a part of a Digital Item (DI) by encapsulating it. IPMP defines how to structure the information that is related to protecting the content. It doesn't provide the tools, mechanisms or licenses itself. Hence it is not a complete DRM alone, but a framework for defining a DRM system. It does not cover keys, key management, trust management, encryption algorithms or certification infrastructures. An example of usage of the IPMP components is given [IPMP2005]:

1. A Digital Item is presented in the Digital Item Declaration Language (DIDL).

2. The Digital Item is encapsulated in an IPMP DIDL element. Some of the content in the IPMP DIDL element may be encrypted. The IPMP DIDL element also contains information about what kind of protection that is used.

3. To access the protected content the terminal must obtain and instantiate the IPMP tools that is permitted by the license.

3.5.2.3 Rights Expression Language

The language to express the rights and conditions in a license is known as REL. A license contains: principal, right, resource, condition and is written in xml. REL is based upon Extensible Rights Markup Language (XrML) [Cont2002], and is designed such that it is easy to extend. REL standard extension and REL multimedia extension are two important extensions to the REL core.

REL support different pricing models: Unlimited usage, flat fee sale, pay per view, preview, promotion, subscription, transfer, gifting, personal lending, library loan, rent, multi-tier models, territory restricted, and more.

3.5.2.4 Rights Definition Dictionary

RDD specifies a dictionary of key terms that are required to describe users' rights [BVHB2003]. The terms are consistent and support the Rights Expression Language. Some examples of basic verbs to describe permissions are: «Adapt, delete, diminish, embed, play, print, modify».

3.5.3 Use of MPEG-21 as DRM

Illustration 10 shows the process from artist to consumer and how the content interacts with the license server.

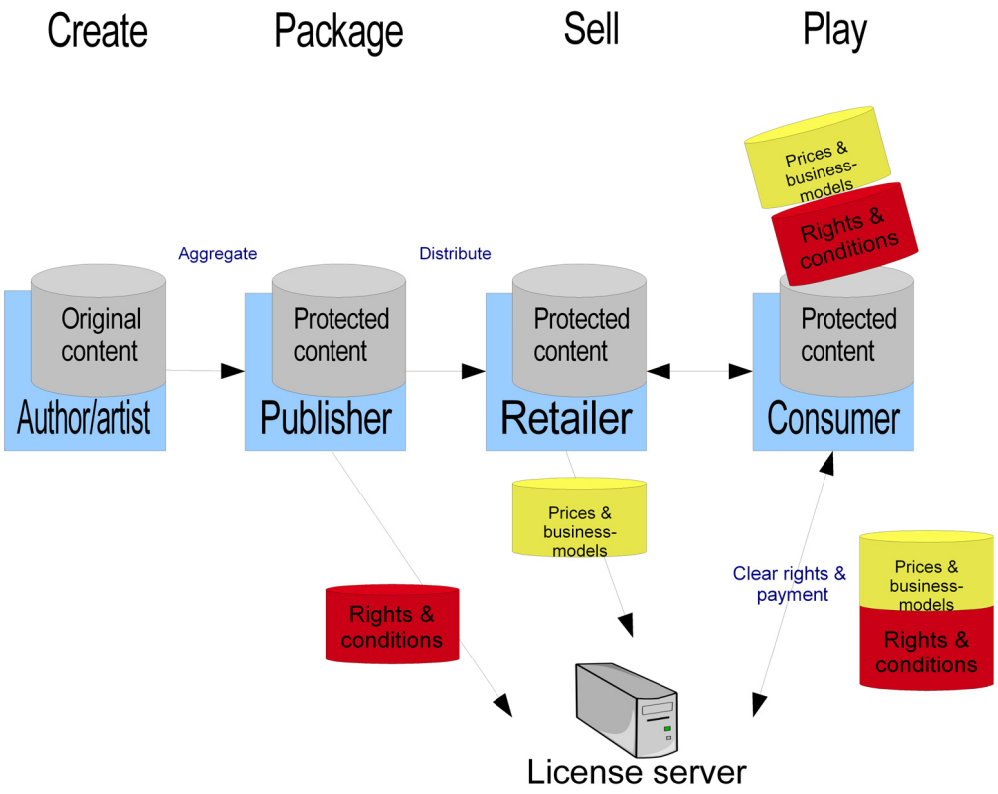

Illustration 10:Example of license-based DRM in MPEG-21 [from Slides of Burnett]

Illustration 11 displays the different questions at the terminal-side, i.e. when the consumer has received the content and wants to interact with it.

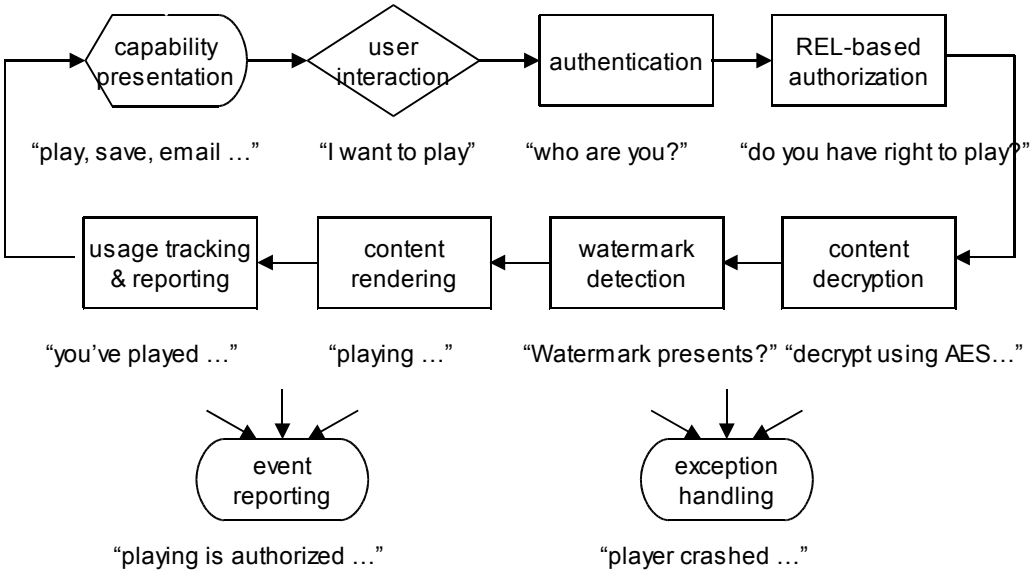

Illustration 11: Terminal-side DRM dataflow [from Slides of Burnett]

Since MPEG-21 can be used in conjunction with different DRM schemes and also offers interoperability between such tools, it is not so useful to classify it in the same manner as the other DRM-systems. However, for the sake of consistency a "classification" of MPEG-21 is given in Table 8.

MPEG-21 DRM	
DRM type (Table 4)	Not specified (flexible)
DRM restrictiveness (Table 2)	Not specified (all levels possible)
DRM dependency (Illustration 4)	Implementation-dependent

Table 8: MPEG-21 DRM classification.

An example extract of the xml-file for a digital item where the audio data is managed by a DRM is given below:

```
<Item>
...
  <Resource mimeType="audio/mp3">
    <ipmpdidl:ProtectedAsset mimeType="audio/mp3"
      <ipmpdidl:Info>
        ...
      </ipmpdidl:Info>
      <ipmpdidl:Contents
ref="http://www.dmu.com/always_red/03_Sawdust_and_Sticks"/>
    </ipmpdidl:ProtectedAsset>
  </Resource>
...
</Item>
```

The example is from the MPEG-21 book by Burnett et.al [BPVK2006].

3.6 Open Mobile Alliance (OMA) DRM

The scope of OMA "Digital Rights Management" [OMA-DRM] is to enable the controlled consumption of digital items on mobile devices (e.g. Mobile phones). This is performed by allowing cpublishers to express usage rights, e.g. the ability to preview digital items, to prevent downloaded items from being illegally forwarded (copied) to other users, and to enable superdistribution of digital items. A complete DRM technology is, however, not in scope of OMA DRM. OMA DRM has the delivery and consumption to users in its focus, it does not aim at a long-term rights management. Neither does OMA DRM 2.0 aim at the implementation of complex license management models.

OMA DRM uses the following DRM components, found in most DRM systems:

- Rights Expression Language
- Content format
- Metadata.

The OMA DRM enables content providers to issue grants for digital items that define how they should be consumed. The DRM system is independent of the item formats and the given operating system or run-time environment. The digital items controlled by the DRM can be a variety of things: games, ring tones, photos, music clips, video clips, streaming media, etc. A publisher can grant appropriate rights to the user for each of these items. The content is distributed with cryptographic protection; hence, the digital item is not usable without the associated rights object on a device. Given this fact, fundamentally, the users are purchasing permissions embodied in rights objects and the rights objects need to be handled in a secure and uncompromising manner.

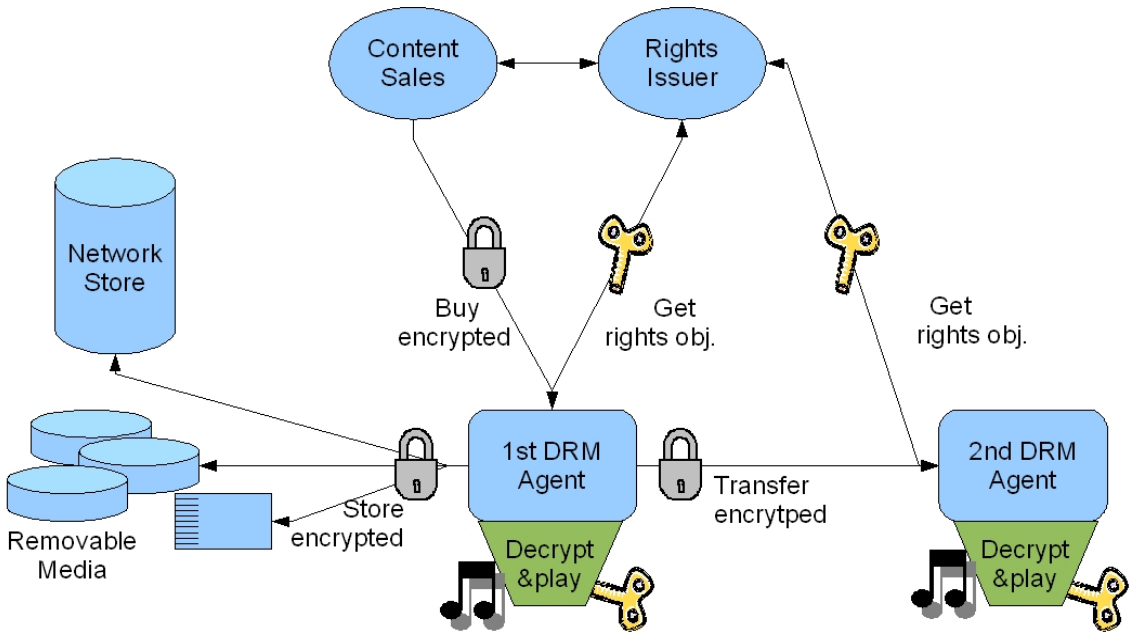

Illustration 12: OMA DRM scenario from the OMA 2.0 architecture specification.

Digital items can be shared among users, but receivers of a copy need to retrieve a new rights object. Rights objects are bound to one particular client, called the DRM Agent. The DRM agent

is a software containing an individual cryptographic key pair. Rights objects are encrypted for a particular DRM Agent. Without the respective and functioning agent, a Rights Object is useless.

The OMA DRM 2.0 Enabler Release defines the protocols, messages and mechanisms necessary to implement the DRM system in the mobile environment. It builds upon the OMA DRM 1.0 Enabler Release with significantly improved security and functionality for a robust, end-to-end DRM system that takes into account the need for secure distribution, authentication of Devices, revocation and other aspectsof the OMA DRM 1.0.

OMA DRM	
DRM type (Table 4)	Active DRM
DRM restrictiveness (Table 2)	Level 4 or 6, possibly higher
DRM dependency (Illustration 4)	Online / Connected upon delivery Playback offline Online / connected upon superdistribution or license expiration

Table 9:OMA DRM classification.

3.7 Digimarc Photo Rights Management

This section presents a non-restrictive DRM system complementing the restrictive technologies presented above. Digimarc's[1] digital rights management system focuses on proof-of-ownership and proof-of-authenticity in digital images. The system deploys watermarking technology to leave hidden traces in digital photographs. These traces can either be employed to proof ownership of rights over a photograph, to detect image manipulation e.g. in drivers licenses, or to detect the appearance of copyrighted photography on web pages. Digimarc's products aim at asset management. On the creator's or publisher's side, the products Digimarc ImageBridge and Digimarc MyPictureMarc are used to deploy and manage watermarks and digital items and detect manipulation in them. An Internet search engine called the Digimarc Spider searches web sites for watermarked photos. With this search enginge, Digimarc can provide ownership information to prospective customers as well as digital item usage information to the creators and publishers.

Digimarc Watermarking	
DRM type (Table 4)	Passive DRM
DRM restrictiveness (Table 2)	Level 2
DRM dependency (Illustration 4)	Offline for item usage Online/Connected for rights verification Online/Connected for use survey

Table 10: Digimarc Watermarkin classification.

1Digimarc Corporation, www.digimarc.com, as of 01-Oct-2007.

3.8 Overall analysis of DRM systems' dependency

For the MARIAGE project, the long-term properties of DRM systems are important. Dependency on other systems might make the digital items inaccessible if some external component of a DRM system disappears (e.g., a license broker going out of business). In Illustration 13, we describe dependencies of the DRM systems that were introduced above.

However, to decide about dependency, a distinction between acquisition, use, and distribution of digital items has to be made. In the diagram, we show the analysis for using media with potentially expiring licenses. A system higher up on the «Copnnected DRM» axis has a higher likelyhood of re-connection to the DRM infrastructure than others lower on the vertical axis. Please note that in the case of Windows Media DRM, the system is a rather flexible toolbox that allows the implementation of various scenarios.

MPEG-21 is beyond classification, as it does not contain a particular DRM business model and infrastructrue.

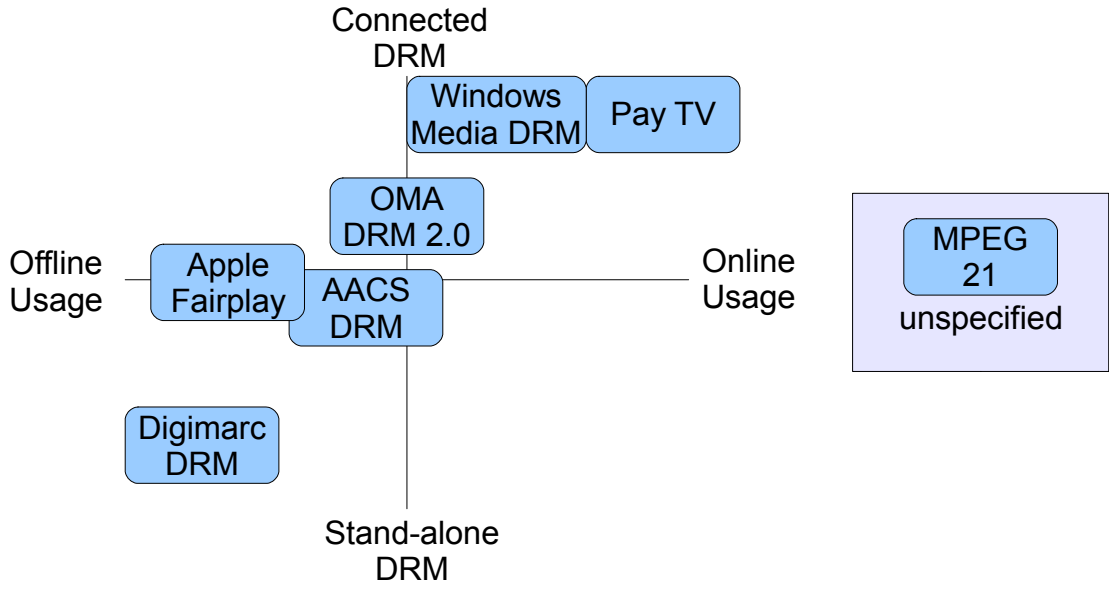

Illustration 13: DRM dependeny.

4 Discussion

From the many possible business models for DRM systems, some are placed inside the legal copyright framework, while some go beyond or violate rights in some countries. For the global deployment of digital media with DRM protection, some severe hindrances exist that need to be considered.

- Differences in national or regional copyright and fair use legislation can render the implementation of certain business models for digital media illegal, e.g. by having a local fair use regime[2].

- Differences in national requirements concerning the archival of cultural goods may have an impact on how DRM projection can be applied to media considered a cultural good[3].

- Changing business models in the media industry need to be considered as well as stakeholders. For example, Swiss collection societies have made a point that they will not tolerate any form of DRM that will weaken artist's renumeration [Schwe2004].

- Upcoming new technology that changes the way people use media can have a vast influence. Portable MP3 players, car stereo units with memory card readers, wearable computers, audiovisual museum guides and ever-innovating mobile phones are likely to be used to play media. But not iTunes music, for the time being, as it can only played on iPods and iPhones.

- National legislation on equal opportunities and accessibility can influence DRM systems, e.g. by requiring media content to be playable on special needs audiovisual devices or by exempting special needs use from regular copyright [Clark2003].

- Consumer and product liability legislation might apply in cases where a DRM system actively sabotages a legal use, e.g. in the case of the Cactus protection system that prevents PC playback of a CD. Protected CDs had to be exchanged against unprotected, playable ones by Bertelsmann[4].

In the design phase of a DRM-related business model and its infrastructure, as a consequence, more issues than network effects and the critical mass of consumers are important. Additionally, legislation may change in the future, and this affect how protected digital media objects that are already deployed are supposed to be used.

2This has happend in Norway in the case of Apple Inc.'s iTunes DRM. It was ruled illegal due to restricting legal rights. See also The Financial Times, «Norway declares Apple's iTunes illegal» of 24-Jan-2007, http://www.ft.com/cms/s/2/1fc40360-abe9-11db-a0ed-0000779e2340.html, as of 26-Oct-2007

3See for example the opinion of Richard Masters, programme manager of the digital objects management programme in the British Library. in Sutherland, J.:"The ideas interview: Richard Masters,"The Guardian, 11-Jul-2006. http://www.guardian.co.uk/ideas/story/0,,1817609,00.html

4 See The Register, «BMG to replace anti-rip Natalie Imbruglia Cds» http://www.theregister.co.uk/2001/11/19/bmg_to_replace_antirip_natalie/, 19-Nov-2001

5 Conclusion

While DRM technology development evolves systems that can secure and restrict media use, the context of DRM deployment to society is not well understood. Besides the technological issues of security management and long-term security of cryptographic methods, many non-technical issues can have a great impact on the deployment, adoption and acceptance of DRM.

Designers and investors in DRM should be aware of this.

6 References

[BVHB2003] Burnett, Ian, Van de Walle, Rik, Hill, Keith, et.al (2003). MPEG-21: Goals and achievements. IEEE Computer Society.

[BPVK2006] Burnett, Ian, Pereira, Fernando, Van de Walle, Rik, Koenen, Rob (2006). The MPEG-21 book. John Wiley & sons.

[ClNe2000] Clarke, Roger and Nees, Stephen (2000) Technological Protections for Digital Copyright Objects, Proceedings of the 8th European Conference on Information Systems (ECIS'2000), July 2000, Vienna, pp. 745-752.

[Clark2003] Clark, J. (2003) Accessibility implications of digital rights management, *http://joeclark.org/access/resources/DRM.html*, accessed 26-Oct-2007.

[Cont2002] XrML 2.0 Technical Overview, version 1.0, March 8, 2002. Contentguard.

[DGLG2003] Jaime Delgado, Isabel Gallego, Silvia Llorente, and Roberto Garc´a, 'IPROnto: An Ontology for Digital Rights Management' in D. Bourcier (ed.), Legal Knowledge and Information Systems. Jurix 2003: The Sixteenth Annual Conference. Amsterdam: IOS Press, 2003, pp. 111-120.

[Fish2004] William W. Fisher, III (2004) iTunes - How Copyright, Contract, and Technology Shape the Business of Digital Media . A Case Study, The Berkmann Center for Internet and society at the Harvard Law School, June 2004.

[INDI2004] Fetscherin, Marc (2004) , Stakeholders in Digital Rights Management: The case of music industry, INDICARE Monitor Vol. 1, No 2, 30 July 2004, Web page visited 2007-10-01, www.indicare.org/tiki-read_article.php?articleId=27

[IPMP2005] Introducing MPEG-21 IPMP components – an overview (2005). http://www.chiariglione.org/mpeg/tutorials/technologies/mp21-ipmp/index.htm

[OMA-DRM] Open Mobile Alliance (2006) DRM V2.0 enabler release, Web page visited 2007-09-28, www.openmobilealliance.org/release_program/drm_v2_0.html

[Schwe2004] Schweri, Y.(2004) Position Paper on Digital Rights Management,International Communications and Art Law, Faculty of Law, Université de Lucerne, Lucerne, Switzerland.

[ShSa2006] Sheppard, N.P., Safavi-Naini, R. (2006) Protecting Privacy with the MPEG-21 IPMP framework. 6th international workshop on Privacy Enhancing Technologies 2006, Cambridge, UK, 28-30 June, 2006, Lecture Notes in Computer Science 4258, 152-171.

[Sobe2003] Sobel, Lionel S. (2003) DRM as an Enabler of Business Models: ISPs as Digital Retailers, Berkeley Technology Law Journal, 18(2), 2003.