Networked Audiovisual Systems and Home Platforms (NAVSHP) strategic objective

NAVSHP (FP6) DRM Requirements Report

Target release version: V1_.0

Dissemination level: PP

I Document

Title	**NAVSHP (FP6) DRM Requirements Report**
Type	Report
Ref	NAVSHP DRM
Target version	V1_0
Current issue	v0.11
Status	Final
File	NAVSHP DRM CG_ADT_20050218
Author(s)	Miguel Dias, ADETTI/MEDIANET - Miguel.Dias@adetti.iscte.pt (Editor) Carlos Serrão, ADETTI /MEDIANET - Carlos.serrao@adetti.iscte.pt Jean Marc Bouqueau - UCL/MEDIANET, boucqueau@tele.ucl.ac.be Yves Maetz, THOMSON/MEDIANET - yves.maetz@thomson.net Olivier Bomsel, Ecole de Mines/MEDIANET - bomsel@cerna.ensmp.fr Anne-Gaëlle Geffroy, Ecole de Mines/MEDIANET - ageffroy@ensmp.fr Zvi Lifshitz, OPTIBASE/TIRAMISU/ENTHRONE Alexandre Cotarmanac'h, FRANCE TELECOM/DANAE - Alexandre.cotarmanach@francetelecom.com Info Wolf , T-SYSTEMS/DANAE - wolfi@t-systems.com Silvia Llorente, UPF/VISNET - Silvia.llorente@upf.edu Jonas Lundberg, Linköpings Universitet / ELIN - jonlu@ida.liu.se Leonardo Chiariglione, CEDEO - Leonardo@chiariglione.org Jean-Pierre Evain, EBU - evain@ebu.ch Julian Seseña, ROSE/AVISTA - jsesena@rose.es Sven Wischnowsky - T-Systems International GmbH - sven.wischnowsky@t-systems.com
Reviewer(s)	Leonardo Chiariglione, CEDEO - Leonardo@chiariglione.org; Julian Seseña, ROSE/AVISTA - jsesena@rose.es
Approver(s)	
Approval date	
Release date	17-01-2005

II Distribution of the release version

Dissemination level	PP
Distribution list (for	

RE documents)	

III History

Date	Version	Comment
07/06/2004		Decision was taken in the Concertation Group 1 - CG1, DRM, to produce this report Zvi from TIRAMISU contributed with DRM requirements deliverable
24/10/2004	0.1	Outline of report ready Miguel Dias, Carlos Serrão from MEDIANET contributed with the DRM requirements deliverable (for the MEDIANET Use Cases)
29/11/2004	0.11	Draft version ready, after contributions from Zvi from TIRAMISU, Leonardo from CEDEO, Miguel Dias and Carlos Serrão from MEDIANET, Alexandre and Wolf from DANAE, Silvia from VISNET and Julian from AVISTA
29/11/2004	0.11	Added the Executive Summary.
06/01/2005	0.11	Chapter 1 and 2 re-written and Glossary added by Miguel Dias, taking into account contributions by Anne-Gaëlle and Olivier Bomsel from MEDIANET. Chapter 3 re-written by Miguel Dias, taking into account comments by Leonardo Chiariglione and Yves and Jean-Marc from MEDIANET.
12/01/2005	0.11	Chapter 2 re-written by Jonas Lundberg from the FP5 ELIN project.
13/01/2005	0.11	Chapter 4 re-written by Sven Wischnowsky from T-Systems
16/01/2005	0.11	Chapter 5, Conclusions, by Leonardo Chiariglione integrated. References to “fair use” removed.
25/01/2005	0.11	Definition of “social use” included by Jean-Pierre Evain from EBU.

IV Executive Summary

Delegates from six FP6 Projects (IP MEDIANET, IP ENTHRONE, STREP TIRAMISU, STREP DANAE, SSA AVISTA, NoE VISNET), enlarged by participations from the EUROPEAN BROADCASTING UNION and the FP5 Project ELIN, chaired by Miguel Dias, have been joining efforts in the framework of Coordination Group 1 - CG1, DRM, chaired by Leonardo Chiariglione, to release a DRM Requirements Report that expresses the views on DRM of the Networked Audiovisual Systems and Home Platforms (NAVSHP) strategic objective, of the Information Society Technologies priority in the FP6. This report is the result of such efforts that expresses the common view of these FP5 and FP6 Projects and Institutions, on the requirements for the future DRM technologies, systems and toolkits in the European Audio-Visual sector. Initially designed to express the common view of NAVSHP in DRM, the authors are planning to submit this report to the consideration of other FP6 Priorities, so that it may reach the status of a DRM Requirements Report for the complete FP6 programme. Comments on this document are solicited.

V Glossary of Terms

Authorized domain: Authorized domain is a set of content rendering devices (belonging to the same household, in the case of a home network).

Broadcasting: Broadcasting designates a unidirectional distribution channel, supporting the diffusion of streamed digital content (e.g. digital broadcasting on fixed and mobile devices, ADSL distribution through one-way dedicated channels, 3G streaming on mobile phones, etc).

Contract law: Contract Law designates a contractual agreement between parties (e.g. content owners and end-users or subscribers), enforced by DRM systems, that can sometimes override copyright law and especially limitations to copyright law as fair uses. Under contract law content owners can decide themselves what is fair use or not, and fix the width of their rights.

Content (is the same as Content Item): Content is a Digital Asset (containing structured data elements and metadata) that can be protected and whose access can be mediated by a DRM system.

Consumer: A Consumer is an end-user that consumes a digital content (or media) item.

Copyright law: Copyright law is Public law (DMCA, EUCD…) defining copyrights and mentioning in broad terms the exception granted to “fair use”. Each country has its own copyright law and, in the case of Europe, each country handles a specific roadmap for the national transcription of the EUCD [AD.9]. The economic role of Copyright law, “is to provide incentives in intellectual creation by giving the owner a temporary monopoly on exploitation” [AD.9].

Downloading: Downloading refers to a bidirectional distribution channel, where a digital content item (normally a file) is retrieved from a remote server or service provider, requiring a reliable service to the network provider, which has no real time requirements, and that usually is offered on a best effort basis.

DMCA: Digital Millennium Copyright Act (2000)

DRM: Digital Rights Management (see DRM definition in Chapter 2. SOCIAL AND BUSINESS APPROACH TO DRM).

End-user: It’s the same as the last User in the Content life-cycle or, to abbreviate, User.

Encryption: It’s a technology that enables the protection of content and requires key management.

EUCD: European Union Copyright Directive (2001).

Key: A key is a technological component of an encryption/decryption system. In more detail, a Key encapsulates data used by a cryptographic method. It is a piece of information that controls the operation of a cryptography algorithm. In encryption, a key specifies the particular transformation of plain text into ciphered text, or vice versa (during decryption.) A key can be contained in a license and a license can contain more than one key (for example, one license may give access to a set of content items encrypted with different keys).

Key management. In cryptography science, key management includes all of the provisions made in a cryptographic system design, in cryptographic protocols regarding that design, in

user procedures, and so forth, which are related to generation, exchange, storage, safeguarding, use, vetting, and replacement of keys.

License: Licence is the logic container that carries the rights to use a content item. It contains data representing the granted Rights expressed by a Rights Expressions Language, from an existing Rights Holder to a User (whom, after receiving the granted rights, becomes a new Rights Holder).

Personal backup: Personal backup copies of the content, refer to private copies of the content in the context of fair use (such as for time shifting or uses for educational purposes).

Pirated content: Pirated Content is the same as Commercial Copyright Circumvention.

Rights: Rights are the ability of an end-user to execute a pre-defined set of utility functions on a content item[1]. These utility functions are the permissions (e.g. right to view/hear, copy, modify, record, excerpt, translate in an other language, keep for a certain period, distribute, etc.), constraints (e.g. play/view/hear n times, play/view/hear n hours, only in Europe) and obligations (e.g. payment, tracking information) which apply to the content and provide liberality of use granted to the end-user.

Rights Expression: Rights Expression [AD.7] is the statement of Functions that can be performed on a Content Item and the circumstances in which they can be performed.

Rights holder: Rights holder indicates the user that is entitled to the given rights. A user becomes a rights holder after obtaining a license carrying the necessary rights.

Scrambling: Scrambling is the process of transforming clear-text content into something that is not understandable by the end-user without the appropriate unscrambling data (typically this unscrambling data, such as a key, is protected with encryption systems). A Scrambling process may or may not require a key.

Signalling (standard): Signalling standard is a standard that signals that a given content item code-stream is protected. It is embedded in the content item code-stream.

Social use: In this report, "social use" of content means content usage with limitations and exceptions defined by national laws and practices.

Streaming: Streaming refers to a bidirectional distribution channel, where a digital content item can be retrieved from a remote server or service provider, requiring a service to the network provider that bears some strict Quality Of Service (QoS) requirements (namely, real time requirements) and that can be offered as a non-reliable service (that is, some data items can be lost during transmission and never received by the consumer). The reliability offered by this service, depends on the network technology used by the network provider.

Subscriber: A Subscriber is a Consumer that has subscribed to a given media delivery service.

Super-distribution: Super-distribution [AD.7] is a mechanism that:

1. allows a User to distribute Content to recipient Devices through potentially insecure delivery systems and

---

[1] These rights vary substantially from country to country, although the most important issues tend to be equivalent.

2. enables the Users of the recipient Devices to obtain a Rights Expression for the said Content.

User privacy: User privacy is the right that prevents the disclosure of the real identity of an end-user, when he/she purchases and/or consumes a given content item.

Virtual Identity: Virtual identity establishes a relation with the Rights Holder real identity, such that the disclosure of such relation can only be done by a DRM system to appropriate authorized systems, in specific and clearly announced cases.

VI Applicable Documents

[AD.1] Zvi Lifshitz, “TIRAMISU DRM Requirements”, Deliverable TIR-W8-DRM-R2.2.doc, IST TIRAMISU, Brussles, May 2004.

[AD.2] Zvi Lifshitz, “TIRAMISU DRM Requirements and Beyond - NAVSHP DRM Coordination Group”, Internal Document TIRAMISU DRM Requirements and Beyond, IST TIRAMISU, Palma de Mallorca, October 24, 2004.

[AD.3] Carlos Serrão, Miguel Dias, “MEDIANET Requirements contribution to NAVSHP DRM CG”, Internal Report C_Contribution to NAVSHP DRM CG_ADT_041011, IST MEDIANET, September 2004.

[AD.4] Carlos Serrão, Miguel Dias, “MEDIANET DRM Requirements”, Internal report MEDIANET-DRM-Requirements, IST MEDIANET, Palma de Mallorca, October 24, 2004.

[AD.5] I. Wolf, A. Cotarmanac’h, “DRM in DANAE”, Internal report Danae_DRM_concertation_palma241004, IST DANAE, Palma de Mallorca, October 24, 2004.

[AD.6] Silvia Llorente, “VISNET NOE - VISNET-DRM”, Internal report, IST VISNET, Palma de Mallorca, October 24, 2004.

[AD.7] The Digital Media Project, “DMP terminology”, Internal report - dmp0147, Osaka, July 2004.

[AD.8] Eric Dhiel et al, “Medianet: A framework to unify different distribution channels”, Internal Report - Medianet position paper, IST MEDIANET, October 1st, 2004.

[AD.9] Olivier Bomsel, Anne Gaëlle Geffroy, “Economic Analysis of DRMs”, Deliverable DB.5.14_Economic analysis of DRMs_V1_0, IST MEDIANET, December 2004.

[AD.10] High Level Group on Digital Rights Management, ”Final Report”, Internal Report 040709 HLG DRM FINAL REPORT, March-July 2004

[AD.11] BEUC, The European Consumers’ Organisation, “Digital Rights Management, Internal Report -DRM views”, Internal Report, BEUC, September, 2004

[AD.12] MAETZ Yves, LELIEVRE Sylvain, TANG-TALPIN Yan-Mei, BOUCQUEAU Jean-Marc, “Requirements on Security Framework”, Deliverable DB52_RequirementsOnSecurityFramework_V0-5_Final_041217, IST MEDIANET, January 2005.

[AD.13] EUROPEAN BROADCASTING UNION, “EBU Memorandum on Digital Rights Management”, EBU Legal and Public Affairs Department, Internal Report DAJ/HR/mp, May 2003.

[AD.14] EUROPEAN BROADCASTING UNION, “EBU Requirements - Content Protection and Copy Management (CPCM) for Free-to-Air”, Internal Report, EBU, Geneva, 5 October 2004

VII Table of Contents

1 Introduction

Delegates from six FP6 Projects (IP MEDIANET, IP ENTHRONE, STREP TIRAMISU, STREP DANAE, SSA AVISTA, NoE VISNET), enlarged by participations from the EUROPEAN BROADCASTING UNION and the FP5 Project ELIN, chaired by Miguel Dias, have been joining efforts in the framework of Coordination Group 1 - CG1, DRM, chaired by Leonardo Chiariglione, to release a DRM Requirements Report that expresses the views on DRM of the Networked Audiovisual Systems and Home Platforms (NAVSHP) strategic objective, of the Information Society Technologies priority in the FP6. This report is the result of such efforts that expresses the common view of these FP5 and FP6 Projects and Institutions, on the requirements for the future DRM technologies, systems and toolkits in the European Audio-Visual sector. Initially designed to express the common view of NAVSHP in DRM, the authors are planning to submit this report to the consideration of other FP6 Priorities, so that it may reach the status of a DRM Requirements Report for the complete FP6 programme.. Comments on this document are solicited.

1.1 Methodology of work

Three meetings of CG1, organised in Barcelona (7th June), Palma de Mallorca (24th October) and Nice (2nd December) and various collaborative sessions over the Internet, have originated the production of this report, after reviewing different DRM requirements that were brought to the meetings as contributions from the mentioned projects.

From a software engineering perspective, requirements (in this context, software requirements) represent the expression of the final functionalities of the targeted software system.

At the stage of the completion of this document, the identified FP6 NAVSHP projects are engaged in DRM software engineering tasks, including specification and development of given DRM functionalities. These have been defined during a previous requirements capture stage, which has spread during the year of 2004, with a duration that has varied from project to project. It is worth noticing that deriving requirements before developing a system is a common practice, which is also valid in standardization activities.

It's the aim of this document to capture and identify the DRM requirements that are shared across the mentioned FP6 NAVSHP projects. Some of the requirements are mandatory, whereas others are optional, depending in the use case implementation, the business context and the regulatory and legal environment. The authors believe that, to some extent, these DRM requirements can be addressed in the future interoperable DRM systems and platforms.

Each of the identified DRM requirements has been uniquely identified with a numeric code. This approach is generally useful at a later stage to trace back each of the requirements in order to identify if they are or not considered in a given implementation.

Defining requirements is a hard process. In order to be able to achieve better requirements identification, each requirement must include the attributes listed below:

a) Identifier - each requirement shall include an identifier, to facilitate tracing through subsequent phases.

b) Title - each requirement shall include a simple and concise identifier that captures the essence of the requirement.

c) Need - essential requirements shall be marked as such. Essential or absolute requirements are non-negotiable; others may be less vitally important and subject to negotiation and are thus optional. In this context, the terms "must", "required" or

"shall" refer to an absolute requirement, the term "may" indicates that an item is truly optional, and the terms "should" or "recommended" mean that there may exist valid reasons in particular circumstances to ignore the particular requirement.

d) Priority - for incremental delivery, each requirement should include a measure of priority so that the developer can decide the production schedule.

e) Stability - some requirements may be known to be stable over the expected life of the software/application; others may be more dependent on feedback from the design phase, or may be subject to change during the application life cycle. Such unstable requirements should be flagged.

f) Clarity in the description - a requirement is clear if it has one, and only one, interpretation. Clarity implies lack of ambiguity. If a term used in a particular context has multiple meanings, the term should be qualified or replaced with a more specific term.

g) Verifiability - each requirement shall be verifiable. This means that it must be possible to:

    - Check that the requirement has been incorporated in the design;
    - Prove that the software will implement the requirement;
    - Test that the software does implement the requirement.

Although all of these attributes can be used to identify the requirements, for the sake of simplicity of the document, we have only used a subset of them, namely, Identifier, Need, Title and Clarity of the Description. More specifically, regarding the "Need" parameter, the authors have realised that, the precise definition of this parameter for a given DRM requirement, depend on the specific business model context and legislation, which varies from country to country. A requirement that is optional for some business case in a specific country, might be compulsory in another context or even contradict a legal directive regarding IPR law in another national context. This document identifies the need for DRM technologies, systems and toolkits to achieve a certain goal. Therefore instead of "shall/should/must/may", requirements should be expressed as: "there is a need to give the DRM system the ability to…", or, to simplify: "there is a need to…". In specific cases were the requirement is clearly mandatory, the expression of such requirement is: "It shall be possible to give the DRM system the ability to…".

This document is organized in the following way:

- Chapter 2 details the Social and Business issues around the concept of DRM.
- Chapter 3 presents the NAVSHP DRM requirements, organised in the following way:
    - Business and Market Requirements
    - Technological Requirements
    - Social Requirements
    - Legal Requirements according to the EU
- Chapter 4 addresses the specific DRM issues related to the distribution channels for multimedia content.
- Chapter 5 extracts some conclusions.

2 Social and Business Requirements of DRM

2.1 DRM Definition

A precise definition of DRM, Digital Rights Management, from the technical and economical point of views can be extracted from [AD.9]:

"DRM systems are means of assigning access to digital contents. In other words, DRMs are, first of all, technological tools designed for excluding consumers from information goods, which, otherwise, would be public goods. In that function, they supplement intellectual property rights whose economic role is to provide incentives in intellectual creation by giving the owner a temporary monopoly on exploitation. This is why DRMs frequently refer to "rights models" as to define the range of accesses they grant. By doing so, DRMs should also be considered as versioning tools, providing to each kind of content, a pre-defined set of utilities: right to view (hear), modify, record, excerpt, translate in another language, keep for a certain period, distribute, etc. In principle, these utilities do not concern the information format of the version (quality, density, compression, languages…) but only the liberality of use granted to the consumer".

2.2 The Goal of DRM Systems

The goal of the DRM systems, considered in this document, is to enable business involving multimedia content to function, by enforcing licensing agreements for social use and offering business opportunities to the content rights owner and content provider. Different businesses will depend on restricting and ensuring what content uses are possible. By social use, we envisage cases such as time shifting, private backup copying or uses for educational purposes. A good set of DRM tools could motivate content owners, producers and distributors, to take advantage of the enormous digital potential available. An important issue is that DRM systems, which are in fact technical private measures protecting copyright, may enforce license contracts that can sometimes override copyright law and especially limitations to copyright law as social uses. Copyright law and technical private measures protecting copyright such as DRMs can have different goals, the first seeking public interest and the second private ones. These issues are not technical, but will affect the value of a DRM toolkit for daily use, since the technology must support both law, business, and the social use which business aims at, and which law can restrict or guarantee. Also DRM systems could be used by law enforcement agencies, to track down copyright circumventors.

A DRM system provides a set of functionalities related to content and to a set of different actors, which intervene across the multimedia content value chain. This value chain incorporates functions regarding content production and protection, content registration, content distribution and control of content usage at the end-user side. In that end of the value chain, a major DRM function is the control of which end-user (subscriber) has content access[2], when he/she has such access, for how long and for what type of content. Additionally, DRM determines what the end-user can do with the content: if it can be stored, copied, exchanged or distributed to others.

We do not yet know the requirements of the DRM toolkit, which will change, as businesses, law and desired uses change. On the one hand, this calls for a broad approach, enabling a flexible toolkit of technologies, which can adapt to the changing requirements, and differences in requirements between stakeholders. On the other hand, it also calls for a

[2] In TV usage scenarios, the control of content access does not mean the control of who is in front of the TV-set, but the control of the subscriber of that TV service.

narrow approach, of identifying key requirements which should be built in the first iteration, which will be useful for key stakeholders, involved in current media business.

It is not the task of technology developers to state what should and should not be required; this has to be invented by relevant stakeholders. For instance, law professionals could evaluate whether any user rights are already guaranteed by law, and provide recommendations to policy makers, advising whether the current state of affairs should be changed or maintained. This potentially changing state of affairs will affect the DRM toolkit, by requiring all to implement certain aspects, or by giving them complete freedom of choice.

Business stakeholders may depend on having supporting DRM tools, supporting key aspects of their business, such as for instance allowing or disallowing Peer-to-Peer (P2P) sharing of their content. One way of approaching the second problem, of finding key DRM tools, would be to include the state-of-the-art, so that current businesses could move over to the new toolkit. Considering business, interoperability with previous DRM tools, would mean to support the same business models. Then, converting old DRM systems to a new interoperable toolkit would not affect business. However, merely converting old DRM systems into one interoperable solution would not provide so much benefit, for individual business. To do better, it is vital to involve key businesses. However, due to constantly changing business circumstances, it would be unwise to implement only what seems to be required right now. Nevertheless, the core set of requirements could be expanded incrementally, by also including new promising DRM tools.

Social use relates to both business and law. It involves what rights users are guaranteed by law, and what they view as their “should-be” rights. This is important to know both for policy makers and for business stakeholders. The user view, firstly, reveals important aspects that might be transformed into rights, by policy makers. Secondly, it reveals important aspects that future business most likely will consider, when they decide on their market strategy. It is not easy to predict what business stakeholders will want to do with their contents, but discovering what is considered attractive social uses of media, is another way of extending the core set of requirements, to include when considering DRM tools. Social uses could for instance be sharing contents with friends, time shifting, and media shifting. Sharing with friends could be done through for instance file sharing, by giving away storage media containing contents, or by sharing the currently played file with friends with in a range of one room, through a wireless network. Time shifting, would be to use the media at whatever time the user would like. Media shifting would be to transfer, rather than making a copy of the file. Then there is also the possibility of the users wanting to trade their copy away, maybe in exchange of some other file, or cash. A study should be made to discover what users think about current DRM tools, existing on the market, what people in general do with unprotected media, and whether DRM tools could provide new opportunities of social use. One particular issue is that DRM is also about managing rights for non-digital media, which might still need digital management. For instance, some business might want to allow the buyer of a vinyl record to get access to a digital counterpart as well, or to give that buyer some other benefit that can be managed using a DRM toolkit.

Law has already been mentioned here, but one particular and sensitive aspect is the possibility of tracking violations of DRM, through different schemes. This possibility has both positive and negative aspects. The most salient positive aspect is that it could make it easier to track down copyright circumventors, but the apparent negative aspect, is that users might be concerned for their privacy. That concern for privacy could give the entire DRM project a bad reputation, which might not be in the interest of businesses depending on DRM for their living. It should also be considered by law policy makers, evaluating whether it is in the interest of the state or country to allow. Until these aspects are examined, it would be useful to consider what DRM technology can and cannot do regarding tracking violations. Without that knowledge, it would be hard for anyone to make informed decisions. Again, it might be wise to include any currently available DRM tools for this purpose, to stay in touch with the state-of-the-art, and to include any promising tools, seen from the viewpoint of different

stakeholders. One example of a law, is the US “fair use” law. Making the toolkit support that law, would enable the toolkit to be used for the US market, although it is less relevant for other markets. It is however more important to ensure that the toolkit supports European laws, and future laws that are currently considered in the EC.

One way of reaching different sets of stakeholders would be that the many projects funded by the European commission would address these issues in their work, regarding their different project areas. That could provide a rather quick and broad coverage to discover what is needed for an early DRM toolkit.

In sum, contractual licenses enforcing is a combination of social conventions, legal measures and technology. This document is mainly about technology, but it also addresses all these three aspects, since social conventions and the ability to enforce the contractual law are also affected by the technology in use.

Therefore we can refer to three Social and Business objectives the DRM technology has to deal with:

1. Provision of efficient access control.
2. Ease of access to and use of content
3. Provision of tools for assistance in contractual law enforcing regarding usage rights, in specific legal contexts.

Key requirements, for achieving these objectives, are elaborated below in this section. They will be expanded and described in detail in Chapter 3, NAVSHP (FP6) DRM REQUIREMENTS, which provides and exhaustive list of requirements that are needed by DRM systems and toolkits. These requirements are now seen as central, and should be evaluated as discussed above. Some requirements may be in conflict with each other, which should be noted when considering what is required for particular businesses, for different stakeholders. It is now vital to discover which requirement set to implement in a first version of a DRM system or toolkit, and how to make the system extensible, to be able to meet new requirements, and expand the possible uses of the DRM system, in subsequent versions of the system.

2.2.1 Efficient use control

To achieve efficient use control, DRM systems may enable the copyright owner to:

- Prevent illegal use of the protected media.
- Associate legal use of media with payment mechanisms.
- Eliminate the proliferation of unprotected copyrighted media.
- Associate access criteria (defined by the right owner of the content) to the protected content.

2.2.2 Ease of access to and use of content

To achieve ease of use, and to make DRM systems attractive to users, a toolkit will most likely need to:

- Try to preserve users rights for digital content use, especially the rights enjoyed with traditional analogue content.
- Ensure access to protected media is as easy and simple as to unprotected content.
- Respect user privacy.

- Avoid adding extra encumbrance to the cost of the media creation, distribution and consumption.
- Allow free choice of services and devices independently of the media item and the license.
- Assist in assuring users, content creators, distributors and rights owners, that remuneration is distributed fairly.
- Provide new opportunities for access, such as restoring digital media to a user, in case of theft or corrupted media files.
- Provide access depending on owning rights to different uses of content, rather than on owning a particular copy of the content in a particular medium.

2.2.3 Law enforcing assistance

A DRM system could help enforcing the law when regulations were violated. To accomplish this function, DRM systems could:

- Make innocent users aware when the media is pirated.
- Enable tracing the media source and trail.
- Make it difficult for violators to stay anonymous

3 NAVSHP (FP6) DRM REQUIREMENTS

3.1 Business and Market Requirements

3.1.1 Efficient use control

To achieve efficient use control, DRM systems are required to:

Requirement ID	Title
BME-0001	Prevent illegal use of protected content
There is a need to give the DRM system the ability to prevent the illegal or unauthorized use of protected content.	

Requirement ID	Title
BME-0002	Interface with payment systems
There is a need to give the DRM system the ability to provide interfaces to associate it with payment mechanisms.	

Requirement ID	Title
BME-0003	Do not unprotect content without a license
There is a need to give the DRM system the ability to make it computationally hard to access content without a licence.	

Requirement ID	Title
BME-0004	Do not render content that was fraudulently unprotected
There is a need to give a compliant the ability not to render content that has been subjected to copyright circumvention (fraudulently unprotected).	

3.1.2 Motivating obedience

To motivate users to follow regulation, respect licensed usage rights and pay royalties, DRM systems shall have the following requirements:

Requirement ID	Title
BMM-0001	Content usage rights
There is a need to give the DRM system the ability to bind specific access rights to the protected content, and to enforce the devices to respect these rights.	

Requirement ID	Title

BMM-0002	Preserve user rights
There is a need to give the DRM system the ability to preserve the user's rights for digital content use and the references they have with traditional content[3].	

Requirement ID	Title
BMM-0003	User friendly
There is a need to give the DRM system the ability to support seamless operation by the end user, without bothering him/she where not necessary.	

Requirement ID	Title
BMM-0004	Extra costs
There is a need to give the DRM system the ability to minimize extra costs brought by it to the content value chain (production, distribution and consumption). These extra costs should be well below the added value brought by DRM.	

Requirement ID	Title
BMM-0005	Freedom of choice
It shall be possible to give the DRM system the ability for the user to choose any compliant services or compliant devices independently of the content type or license format, enabling a competitive market.	

Requirement ID	Title
BMM-0006	Distribution of remuneration
There is a need to give the DRM system the means to enable the fair distribution of remuneration across all content value chain actors (owners, producers, distributors, retailers, users).	

Requirement ID	Title
BMM-0007	Rights expression
There is a need to give the DRM system the ability to support the expression of various types of usage rights to content, using standard rights expression	

[3] The preservation of users rights as to take into account that they vary substantially from country to country, although the big issues regarding user rights tend to be equivalent.

language, to the extent that this is required for interoperability

Requirement ID	Title
BMM-0008	Separation of content protection from the DRM functions
There is a need to give the DRM system the ability to support the separation of content protection from the rights management and enforcement functions.	

Requirement ID	Title
BMM-0009	Content and Rights
There is a need to give the DRM system the ability to support the separation between content and licensed rights (e.g; the capability to store separately the content and the associated rights, to assign different sets of rights to the same content, etc.).	

Requirement ID	Title
BMM-0010	Protected content identification
There is a need to give the DRM system the ability to identify protected content, such that licenses may be unambiguously associated with it.	

Requirement ID	Title
BMM-0011	Authorized domain support
There is a need to give the DRM system the ability to support content delivery either to a single rendering device (standalone device) with acquisition, storage and rendering capacity or to a set of devices (authorized domain, in the case of a home network) including access devices (or gateways), storage devices, and rendering devices gathered in a community of devices (e.g. belonging to a same household).	

Requirement ID	Title
BMM-0012	Device identification and authentication
There is a need to give the DRM system the possibility for the license issuer to reliably identify and authenticate the device or an authorized domain, for the purpose of either issuing or refusing a license to that device or authorized domain.	

Requirement ID	Title

BMM-0013	Grand access to a particular device
There is a need to give the DRM system the possibility to grant access for a particular content item to a particular device.	

Requirement ID	Title
BMM-0014	License and content delivery times
There is a need to give the DRM system the ability to make possible for licenses and protected content to be delivered at the same time or at different times and to be received in any order.	

Requirement ID	Title
BMM-0015	Content forward locking
There is a need to give the DRM system the ability to forward lock a content item so that when delivered to the target consumption device, this device cannot redistribute it to another device.	

Requirement ID	Title
BMM-0016	Teasing facilities
There is a need to give the DRM system the possibility for the device (with forwarding capacities) to forward a content teaser file created on that device, such that this teaser can be freely redistributed.	

Requirement ID	Title
BMM-0017	Distribution model
There is a need to give the DRM system the ability to support different distribution models (e.g; push, pull, super-distribution).	

Requirement ID	Title
BMM-0018	Distribution channel
There is a need to give the DRM system the ability to support different distribution channels: Internet; broadcast over satellite, cable or terrestrial; mobile (point to point delivery), broadband/ADSL, pre-recorded; physical distribution; hybrid bi-directional (e.g. TV over ADSL, Broadcast over Mobile, etc).	

Requirement ID	Title

BMM-0019	Distribution type
There is a need to give the DRM system the ability to support different types of distribution: two-way distribution: streaming or downloading; one-way distribution: broadcasting.	

Requirement ID	Title
BMM-0020	Business model
There is a need to give the DRM system the ability to support different business models (e.g; time period subscription, number of content subscription, pay per view, pre-paid/reservation, etc.)	

Requirement ID	Title
BMM-0021	Usage rules
There is a need to give the DRM system the ability to support different usage rules (view N times, view for N hours, copy once, etc).	

Requirement ID	Title
BMM-0022	Content versioning
There is a need to give the DRM system the ability to propose various business models and usage rules for different versions of a given content[4] (.	

3.1.3 Law enforcing assistance

Advanced DRM systems can help enforcing the law when regulations were violated. To accomplish this function DRM systems are required to:

Requirement ID	Title
BML-0001	Copyright circumvented access to content
There is a need to give the DRM system the ability to allow end-users to be notified when the content being rendered may be copyright circumvented content (with no licence)	

Requirement ID	Title
BML-0002	Content source identification

[4] E.g: a movie may be proposed in several level of quality (HD, SD, CIF, etc.), a song may be proposed as audio only or video clip, in mono, stereo or in 5.1, etc

There is a need to give the DRM system the ability to allow the content source identification.

Requirement ID	Title
BML-0003	Trace and trail content
There is a need to give the DRM system the ability to allow content tracing and trail.	

3.2 Technological Requirements

The previous section has listed and described the business requirements for DRM Systems. This section will deal with the DRM technological requirements. The technological DRM perspective includes hardware and software used to secure digital content. The technical DRM perspective involves a number of technological elements that are often used in combination to secure content.

3.2.1 Closing loopholes

Loopholes are the frail links in the content or key lifecycle, which expose the content to violation. In order to minimize loopholes, DRM systems are required to provide the following capabilities:

Requirement ID	Title
TCL-0001	Content value chain protection
There is a need to give the DRM system the ability to protect the content along the content value chain, from creation to consumption, so that content needs not to be disclosed in clear text at any intermediate value chain point.	

Requirement ID	Title
TCL-0002	Key protection
There is a need to give the DRM system the ability to protect the key against theft attempts and against attempts to use the key for operations which are not allowed by the final license terms.	

Requirement ID	Title
TCL-0003	Key individualization
There is a need to give the DRM system the ability to provide the necessary mechanisms to associate, whenever needed, a unique individual key to each of the content items, avoiding the problem of “cracked once, cracked everywhere”.	

Requirement ID	Title

TCL-0004	Global System Security
There is a need to give the DRM system the ability to prevent the compromise of the whole system security, if a single key or a small number of devices are hacked, by using tamper resistance mechanisms (hardware and software) to enhance the global security. Every sensible element in the content supply chain is required to be tamper resistant.	

Requirement ID	Title
TCL-0005	License factorisation
There is a need to give the DRM system the necessary mechanisms to associate, whenever needed, a common license for all users whishing to consume a specific content item, allowing a one-to-many distribution model (broadcast like) without having to create and distribute as many licences as users	

Requirement ID	Title
TCL-0006	Composite content keys
There is a need to give the DRM system the ability for individual components of a composite content object to be encrypted with different keys.	

Requirement ID	Title
TCL-0007	Confidentiality of content encryption key
There is a need to give the DRM system the ability to ensure the non-disclosure of content encryption keys during their transport.	

3.2.2 Security

The Security category includes the following requirements:

Requirement ID	Title
TSC-0001	Secure content format
There is a need to give the DRM system the ability for content to be stored and delivered in a protected format that prevents or complicates unauthorized access and copy.	

Requirement ID	Title
TSC-0002	Decryption keys disclosure
There is a need to give the DRM system the ability to distribute decryption key(s) only to authenticated rights holders.	

Requirement ID	Title
TSC-0003	Limited usage
There is a need to give the DRM system the ability to restrict the usage of the content by various parameters (e.g., number of times content played, expiration date, etc.).	

Requirement ID	Title
TSC-0004	Partial asset protection
There is a need to give the DRM system the ability to apply different usage rules/rights to parts of a larger content item (e.g., protect streams within a session, for example for preview purposes). -	

Requirement ID	Title
TSC-0005	Rendering device authentication
There is a need to give the DRM system the ability to authenticate, prior to delivery of rights information to the intended rendering device, at least one of the following: • The virtual identity of the subscriber associated with the rendering device; • The identity of the subscriber associated with the rendering device, except private information; • The identity of the rendering device (for example: serial number; rendering device manufacturer; model number; software version); • The identity of any hardware token (for example: smartcard) inserted in the rendering device. • The identity of the access device or gateway in the case of a home network	

Requirement ID	Title
TSC-0006	Rights issuers particularisation
There is a need to give the DRM system the ability for rights issuers to protect rights (licenses) for a particular rendering device such that only the intended rendering device can process the rights.	

Requirement ID	Title
TSC-0007	Send licenses to devices
There is a need to give the DRM system the ability for license issuers to send licenses to rendering devices.	

Requirement ID	Title
TSC-0008	Users rights information
There is a need to give the DRM system the ability to permit users to be informed about the rights status of both content and users (e.g., shouldn't block access without apparent reason).	

Requirement ID	Title
TSC-0009	User access to information about rights
There is a need to give the DRM system the ability for the User to obtain information, e.g. copyright information, available permissions, regarding rights on the rendering device.	

Requirement ID	Title
TSC-0010	Metadata
There is a need to give the DRM system the ability for a user to obtain and view a metadata description of the protected content.	

Requirement ID	Title
TSC-0011	Protected content integrity
There is a need to give the DRM system the ability to ensure the integrity of the protected content (avoiding any modification to the content) , in a manner independent of the transport mechanism,.	

Requirement ID	Title
TSC-0012	Authenticate the license source
There is a need to give the DRM system the ability for the rendering device to authenticate the identity of the source of the license.	

Requirement ID	Title
TSC-0013	Protected content usage
There is a need to give the DRM system the ability for a device to use protected content only if appropriate licenses have been associated with that protected content and the device possesses the required license.	

Requirement ID	Title

TSC-0014	Renewability
There is a need to give the DRM system the ability for the essential security elements of the DRM system **to** be renewable in case of hacking of the system.	

3.2.3 Monitoring

The purpose of monitoring is to force royalty payment according to license terms and to enable automated levy collection. DRM systems are required to provide the following:

Requirement ID	Title
TMO-0001	Content purchase monitoring
There is a need to give the DRM system the ability of monitoring each content purchase, that is subject to authorization and payment transactions, without ever disclosing the real user identity, in order to detect possible misuse and be able to provide usage-based revenues to the corresponding content life-cycle actors.	

Requirement ID	Title
TMO-0002	Content usage or transit events reporting
There is a need to give the DRM system the ability of reporting content usage or transit events to management or accounting systems, identifying the nature of the operation, the identification of the content item, the licensing information involved, without ever disclosing the real user identity	

Requirement ID	Title
TMO-0003	Report violations to management systems
There is a need to give the DRM system the capability of reporting copyright violations to the management/accounting systems, making the best effort to identify the violators.	

3.2.4 Traceability

When everything fails, the content may have been pirated and then it remains to find and prosecute the violators. A DRM system can help at this stage, if it can provide the following capabilities:

Requirement ID	Title
TRA-0001	Digital signature and fingerprinting
There is a need to give the DRM system the ability to later prove end-user selections or actions that need to be monitored, in front of a 3rd party. This information can only be disclosed to appropriate authorized systems, in specific and clearly announced cases.	

Requirement ID	Title
TRA-0002	Illegal distribution
There is a need to give the DRM system the ability to make difficult the distribution of copyright circumvented content.	

Requirement ID	Title
TRA-0003	Copyright circumvented content consumption
There is a need to give the DRM system the ability to make difficult to consume copyright circumvented content.	

Requirement ID	Title
TRA-0004	Content segments
There is a need to give the DRM system the ability to force the presence of certain content segments as a condition for playing it (e.g., author details or copyright information), even if content is allowed to be modified.	

3.2.5 Interoperability

Interoperability is a very basic requirement of DRM for allowing free choice of services and devices. In order to enable interoperability, DRM systems should:

Requirement ID	Title
TIN-0001	Standard algorithms usage
There is a need to give the DRM system the ability to use a set of selected standard algorithms to cipher or scrambling the content, to the extent that this is required for interoperability.	

Requirement ID	Title
TIN-0002	Standard signalling usage
There is a need to give the DRM system the ability to use a signalling standard for the protected content, to the extent that this is required for interoperability.	

Requirement ID	Title
TIN-0003	Standard key management
There is a need to give the DRM system the ability to use standard key management systems (such as PKI), to the extent that this is required for interoperability.	

Requirement ID	Title
TIN-0004	Standard Content identification
There is a need to give the DRM system the ability to use content identification standards.	

Requirement ID	Title
TIN-0005	Media and Rights interoperability
There is a need to give the DRM system the ability to make possible rights specification and protected content for multiple common existing content formats and/or common computing platforms.	

Requirement ID	Title
TIN-0006	Protected and clear content
There is a need to give the DRM system the ability to make possible rights specification for both protected and clear content.	

Requirement ID	Title
TIN-0007	Proprietary algorithms
There is a need to give the DRM system the ability to provide a transparent mechanism to renew proprietary algorithms into the final user devices, using a standardized framework.	

Requirement ID	Title
TIN-0008	Render unprotected content
There is a need to give the DRM system the possibility to render “old” or “legacy” unprotected content on the current system.	

Requirement ID	Title
TIN-0009	Prevent rendering of protected content
There is a need to give the DRM system the possibility to prevent rendering of protected content in “old” or “legacy” systems.	

Requirement ID	Title
TIN-0010	Hardware Identifiers

There is a need to give the DRM system the ability to **n**ot strongly rely on a specific hardware device internal id (e.g., end user will be able to change hardware player without inherently affecting his/her rights to consume content).

Requirement ID	Title
TIN-0011	Transfer licenses between devices
There is a need to give the DRM system the ability for rendering devices to transfer licenses between them, for a given content item.	

Requirement ID	Title
TIN-0012	Rights and content delivery
There is a need to give the DRM system the ability for licenses and protected content to be delivered via the same or different transport mechanisms.	

Requirement ID	Title
TIN-0013	License transfer
There is a need to give the DRM system the ability to support the possibility for users to transfer licenses between different virtual identities, if the license grants this right.	

3.2.6 Rights Holder Identification

In the old analogue days, the act of buying a licensed content item was simple – buying the physical media. This does not apply in the digital days when there is practically no physical media. Therefore there is a need for Rights Holder Identification or impersonation – association between licenses and virtual identities and to tackle the more general aspect of rights holder identification. The following are the requirements for Rights Holder Identification:

Requirement ID	Title
TIM-0001	Virtual User identification
There is a need to give the DRM system the ability to support the user identification through the existence of virtual user identification or subscription mechanisms, based on hardware or software.	

Requirement ID	Title
TIM-0002	Virtual User identification mobility
There is a need to give the DRM system the ability to support the virtual user identification to be mobile or easily transferred across different sets of devices and environments supporting such impersonation.	

Requirement ID	Title
TIM-0003	Community identification
There is a need to give the DRM system the ability to allow a license to identify a single user virtual identity (a particular virtual rights holder) or to a group of rights holders.	

Requirement ID	Title
TIM-0004	Virtual identity restore and recovery
There is a need to give the DRM system the ability to make possible the virtual user identity to be recovered and restored after some unpredicted loss or damage.	

3.2.7 Content and Rights

One of the methods to fight copyright circumvention, in the case of physical goods trade, is to make it apparent when goods are stolen or illegally traded. DRM systems should apply similar measures for digital content. Such measures may include:

Requirement ID	Title
TID-0001	Content identification within rights
There is a need to give the DRM system the ability to specify content identification within rights, using identification standards.	

Requirement ID	Title
TID-0002	Rights for a virtual user identity
There is a need to give the DRM system the ability to specify rights which are bounded to a particular virtual user identity.	

Requirement ID	Title
TID-0003	Association of license to content
There is a need to give the DRM system the ability to support the association between the content item and references for acquiring a license to use it.	

Requirement ID	Title
TID-0004	Rights identification and protection
There is a need to give the DRM system the ability to support the separation between identifying rights and protecting them.	

3.2.8 Versatility

A DRM system is required to be versatile in the sense that:

Requirement ID	Title
TVR-0001	License and content independence
There is a need to give the DRM system the ability to provide the appropriate mechanisms to make licenses applicable to content items independently of the items format representation, the delivery network type or the consumed type.	

Requirement ID	Title
TVR-0002	Rights and protected content recovery
There is a need to give the DRM system the ability to make possible for the user to delete an instance of protected content, while keeping the rights associated with that content (so that he/she could later restore the protected content on the device, without having to obtain new rights).	

3.2.9 Accessibility

A DRM system is supposed to prevent illegal access to content. It shall not prevent or complicate legal access to content. The rule of thumb is: the only difference between protected and unprotected content should be the price. Specifically this means that:

Requirement ID	Title
TAC-0001	Content geographic availability
There is a need to give the DRM system the ability that content should be accessible in all environments (inside the house, on the road etc.) and in all geographic locations, as long as a consuming device is available, with respect to geographical restriction usage rules.	

Requirement ID	Title
TAC-0002	Content temporal availability
There is a need to give the DRM system the ability that content should be accessible at any time of the day and period of the year, with respect to time restriction usage rules.	

3.2.10 Non-Restrictiveness

A DRM system should allow any legal use of content, specifically usage that is legal with traditional analogue content. Examples of such usage:

Requirement ID	Title
TNR-0001	Device compatibility
There is a need to give the DRM system the ability to allow the content	

playback on any compatible device authorized by the license.

Requirement ID	Title
TNR-0002	Personal backup
There is a need to give the DRM system the ability to allow the creation of personal backup copies of the content, in the context of social use, such as for time shifting or uses for educational purposes.	

Requirement ID	Title
TNR-0003	Render restored protected content
There is a need to give the DRM system the ability to make possible for a device to render protected content, which has been restored from a backup location, in the context of social use.	

Requirement ID	Title
TNR-0004	Excerpts recording
There is a need to give the DRM system the ability to allow excerpts recording for personal or social use.	

Requirement ID	Title
TNR-0005	Lending
There is a need to give the DRM system the ability to allow the lending of content items to other end-users, in the terms of the licensed usage rights.	

Requirement ID	Title
TNR-0006	Selling
There is a need to give the DRM system the ability to allow the selling of used content, in the terms of the licensed usage rights.	

3.2.11 Simplicity

Purchase and use of traditional content is simple. Just pop into a record shop, buy a disc and play it back on a player. Digital content allows even more robust consuming models, such as online delivery. DRM should support the simple models and avoid adding complexity to the users (technical complexity that is handled automatically and is transparent to the users does not count). Specifically it is supposed to support:

Requirement ID	Title
TSM-0001	License acquiring
There is a need to give the DRM system the ability to allow simple	

mechanisms for license acquiring.

Requirement ID	Title
TSM-0002	Device license enabling
There is a need to give the DRM system the ability to provide simple mechanisms for enabling the licenses on devices.	

Requirement ID	Title
TSM-0003	Payment and Subscription
There is a need to give the DRM system the ability to provide simple and straightforward interface with payment and subscription methods.	

3.2.12 Scalability of Content

Requirement ID	Title
TSC-0001	Scalable content coding
There is a need to give the DRM system the ability to support scalable content coding without hindering the full potential of that technology.	

3.3 Socio-Economic Requirements

It is technically possible for users to acquire high-quality copies of copyrighted works without compensating the copyright holders, but it may not be legal. Downloading is not freeloading, and yet many content consumers fail to make the distinction. Some don't understand that a distinction exists, and others choose to ignore it.

Publishers, trade organizations and technology companies should work together to educate users regarding the issues related to piracy and make it easier to report potential issues when they are discovered.

3.3.1 Affordability

This section raises two different economic questions. A first issue is price competition between the different distribution contents networks (physical distribution, broadcast, broadband) on the final market. A second one is the cost of DRMs solutions : it's determined by their design but also by the competition and firms market powers on the DRMs solutions market.

One of the main factors affecting the motivation to tamper with security systems is the price of the goods. As for digital content, DRM technology can succeed only if it there is a parallel decrease in the cost of the protected content. While the cost factor is beyond the DRM scope, a good DRM system shall contribute to the efforts to keep the costs low by avoiding of adding extra cost due to the DRM technology itself. It is required the following capabilities:

Requirement ID	Title
SAF-0001	Technology costs for content providers

There is a need for the technical costs of content protection **to** be marginal in relation to the financial gains of content protection with DRM.

Requirement ID	Title
SAF-0002	Protected content delivery costs
There is a need, for the DRM designer, **to** take care of limiting the burden of delivering protected content comparing to unprotected content.	

3.3.2 Privacy

One of the important rights of consumers of traditional content is privacy. A record can be purchased in a record shop without disclosure of the customer real identification. DRM systems should respect this right. Although this issue is not straightforward, from the technical point of view, DRM systems can address virtual identity techniques and Trusted Third Parties (TTP) schemes in open environments, to enforce Privacy requirements.

Requirement ID	Title
SPV-0001	User privacy
There is a need to give the DRM system the ability to respect and ensure user privacy except for the information for which consent has been given by that user for divulgation .	

Requirement ID	Title
SPV-0002	Content and source privacy
There is a need to give the DRM system the ability to prevent the license from exposing details about the content item or its source.	

Requirement ID	Title
SPV-0003	User information disclosure
There is a need to give the DRM system the ability to not disclose User and device specific information to the content provider and/or to other parties without the explicit consent of that User.	

Requirement ID	Title
SPV-0004	Notification of changes in privacy rules
There is a need to give the DRM system the ability for the user to be aware if the privacy rules changes.	

Requirement ID	Title

SPV-0005	User anonymity
There is a need to give the DRM system the ability to support the user anonymity, never disclosing the real user identity that is related to its own virtual identification. This information can only be disclosed to appropriate authorized systems, in specific and clearly announced cases.	

3.3.3 Legal Requirements according to the EU

Since DRM focuses in managing "rights," its scope inevitably reaches the legal issues, such as copyright law and contract law. A detailed discussion of the laws associated with rights management across the EU countries, is outside the context of this document. Readers interested in this area should refer to the appropriate legislation. The legal perspective includes:

- Legislation;
- Compliance:
- Investigation:
- Enforcement.

Nevertheless, regarding legal issues, a there is the need to give the DRM system the ability to:

- Respect the freedom of services within the European Union Internal Market;
- Respect copyright laws including the European Copyright Directives;
- Respect exceptions or limitations under national copyright laws and practices, since different national laws and practices may apply when restricting copying.

Requirement ID	**Title**
LR-0001	Export license regulations
There is a need to give the DRM system the ability not to be limited in deployment and usage due to existing export license regulations.	

4 DISTRIBUTION CHANNELS

Today we find an increasing variety of distribution channels for multimedia content. End user devices for content consumption support one or more of those channels with different characteristics, e.g. unidirectional or bidirectional data transport. Applications that use the distribution channels to enable content consumption are expected to fulfil the DRM requirements to satisfactory extend. The following paragraphs suggest the restrictions on the DRM requirements that apply when a certain distribution channel is used by an application.

4.1 Internet (Possible combinations of Streaming, Downloading)

The internet as a distribution channel for multimedia content can be characterized as a bidirectional communication channel with broadband capacity that works on a best effort basis. Multiple data transfer protocols do exist, that support download and streaming applications. In download scenarios the content is transferred to the end device completely, where as in streaming applications the content is not fully stored on the end device beyond the use within the application's scope.

4.2 Mobile (point to point delivery, forward lock, trusted device)

Typically mobile distribution channels like GSM, GPRS or UMTS are bidirectional communication channels. So far they are mainly used for point-to-point delivery of multimedia content to trusted devices. State-of-the-art DRM-Systems use forward lock, combined delivery of content and license as well as separate delivery of content and license.

4.3 Broadcast (Possible combinations of Streaming, Downloading)

Broadcast delivery channels are typically unidirectional data transfer channels. There's a trend towards overcoming the lack of a back-channel through combination with other communication channels (e.g. GPRS), but this is not focused here.

4.4 Physical

Physical distribution channels can be used to acquire content or licenses or both in order to feed the consuming device with this data.

4.5 Hybrid bi-directional (e.g. TV over ADSL, Broadcast over Mobile, cross platform requirements)

Hybrid bi-directional distribution channels make use of two ore more of the above introduced channels. It can be combinations of Broadcast with Internet- or Mobile-Channels as well as combinations with physical channels (e.g. buying licenses on a smartcard).

4.6 Restrictions on Requirements

Lack of certain capabilities in some of the distribution methods pose restrictions on which DRM requirements can be fulfilled. In the following we present the most important restrictions with lists of the affected requirements. In some cases, these restrictions can be overcome by technological means but nonetheless they affect the ease with which the requirements can be met.

4.6.1 Unidirectional channels

Especially in a pure broadcast scenario, there is no back-channel which would allow the device to respond to the server.

Affected requirements:

BME-0002	Lack of a back-channel poses restrictions on the types of payment systems that can be used.
BML-0003	Without a back-channel, the device cannot send information about content received, viewed or otherwise processed to a server.
TSC-0002	As for payment systems above, lack of a back-channel restricts the types of authentication systems that can be employed.
TSC-0012	Without a back-channel it might be impossible for the end-device to authenticate the identity of the license source (depending on implementation details).
TMO-0001	Same as for TSC-0002.
TMO-0002	Same as for TSC-0002.
TMO-0003	Same as for TSC-0002.
TRA-0001	Depending on implementation, it might be hard or even impossible to prove end-user actions made without information about these being sent to monitoring services.
TAC-0003	In a broadcast scenario, content is only available when sent by the playout center, not on-demand and hence it can't be made available at any time.
TSM-0003	Same as for BME-0002.

4.6.2 Non-identifiable end-devices

End-devices may be unknown in advance or generally not identifiable due to lack of a unique device ID.

Affected requirements:

BMM-0011	Without the possibility to uniquely identify end-devices, content delivery to single or groups of selected devices is impossible.
BMM-0012	This requirement is all about identifiable end-devices, hence without identifiable end-devices, the preconditions aren't fulfilled.
BMM-0013	Same as for BMM-0011.
TSC-0002	If rights holders are to be identified by their end-devices, the lack of end-device identifications makes sending keys to selected rights holders impossible.
TSC-0005	Same as for BMM-0012.

4.6.3 Non-identifiable customers

Potential service customers might be anonymous, either because no generally available, accepted identification and authentication service is available or because such services aren't used.

Affected requirements:

BME-0002	Depending on the kind of payment systems used, anonymity of users might be impossible to guarantee. In most cases it might still be possible to keep the user anonymous with respect to the content delivery service, though.
TSC-0002	If customers are anonymous, it is questionable whether rights can be given to them separately.
TSC-0005	As for unidentifiable devices: this requirement might need possibilities to identify users (or virtual identities).
TIM-0001	Same as for TSC-0005.
TSM-0003	Same as for BME-0002.

4.6.4 Streamed content

In a pure streaming scenario, the content is never stored in full on the end-device which makes, inter alia, saving and restoring of the content impossible (a license, on the other hand, could be saved and restored).

Affected requirements:

TNR-0002	Since the content isn't stored on the device, no personal backup can be made.
TNR-0003	Same as for TNR-0002.
TNR-0005	Since no access to the whole content items is available, they can't be lent. The only thing that could be lent is access to the stream.

5 CONCLUSION

This report is the result of joint efforts from Delegates from six FP6 Projects of the NAVSHP priority, with contributions from EBU and FP5 project ELIN, which have been collaborating in the framework of Coordination Group 1 - CG1, DRM and expresses the common view of these FP5 and FP6 Projects and Institutions.

The report is an attempt at providing a set of requirements that a DRM system should support. Because DRM systems may be designed having in mind different requirements for particular businesses and for different stakeholders, it is clear that some of the derived DRM requirements may contradict each other. Therefore most of these requirements are “optional”, in the sense that a designer of a DRM system may need support for a given set of requirements, while another designer may need support for a different set of requirements. This aspect becomes even more important if we consider the different perspectives that different stakeholders of the value chain may have and that can be translated in new legislation, that can enable or disable certain technical features of DRM systems.

The obvious conclusion of this joint effort is that DRM technologies are to be developed as a toolkit, in other words, there should be technologies available to support the different requirements.