Automating Production of Cross Media Content for Multi-channel Distribution

www.AXMEDIS.org

DE4.5.1

Content Protection and Supervision

Version: 2.7
Date: 10/11/2005
Responsible: FUPF (revised and approved by DSI)

Project Number: IST-2-511299 Project Title: AXMEDIS Deliverable Type: Public Visible to User Groups: Yes Visible to Affiliated: Yes Visible to Public: Yes

Deliverable Number: DE4.5.1 Contractual Date of Delivery: Month 13 (End of September 2005) Actual Date of Delivery: 10/11/2005 Work-Package contributing to the Deliverable: WP4.5 Task contributing to the Deliverable: WP4.5 Nature of the Deliverable: Report and prototype Author(s): FUPF, AFI, ILABS, FHGIGD, DSI

Abstract: This deliverable aim is to show the research work done in the area of content protection and supervision, including digital rights management and contract analysis aspects. It also reports the prototypes implemented to demonstrate the research work done in the different areas studied. The prototypes presented will be used inside the WP5, AXMEDIS Framework, WP9, Demonstrators and, obviously, in the continuation of WP4.

Keyword List:
DRM, Contract Analysis, Content protection, Content supervision, Fingerprinting

Table of Contents

1 Executive Summary and Report Scope

Market and end-users are pressing content industry to reduce prices. This is presently the only solution to setup viable and sustainable business activities with e-content. Production costs have to be drastically reduced while maintaining product quality. Content providers, aggregators and distributors need innovative instruments to increase efficiency. A solution is automating, accelerating and restructuring the production process to make it faster and cheaper. The goals will be reached by: (i) accelerating and reducing costs for content production with artificial intelligence algorithms for content composition, formatting and workflow, (ii) reducing distribution and aggregation costs, increasing accessibility, with a P2P platform at B2B level integrating content management systems and workflows, (iii) providing algorithms and tools for innovative and flexible Digital Rights Management, exploiting MPEG-21 and overcoming its limits, supporting several business and transactions models. AXMEDIS consortium (producers, aggregators, distributors and researcher) will create the AXMEDIS framework with innovative methods and tools to speed up and optimise content production and distribution, for *production-on-demand*. The content model and manipulation will exploit and expand MPEG-4, MPEG-7 and MPEG-21 and others real and de-facto standards. AXMEDIS will realise demonstrators, validated by means of real activities with end-user by leading distributor partners: (i) tools for content production and B2B distribution; (ii) content production and distribution for i-TV-PC, PC, kiosks, mobiles, PDAs. The most relevant result will be to transform the demonstrators into sustainable business models for products and services during the last project year. Additional demonstrators will be 2-3 associated projects launched as take up actions. The project will be supported by activities of training, management, assessment and evaluation, dissemination and demonstration at conference and fairs.

This deliverable is devoted to the description of content protection and supervision done inside WP4.5.

This activity is by no means finished with the completion of this deliverable, but it has to be revised during the development of the project.

Main deliverables in WP4 are:

- DE4.1.1 – Content Modelling and managing (M13), report and prototype;
- DE4.2.1 – Content indexing, monitoring and querying (M13), report and prototype;
- DE4.3.1 – Content Composition and formatting (M13), report and prototype. It also includes the details about the integration of AXMEDIS with workflow management tools;
- DE4.4.1 – Content sharing and production on P2P (M13), report and prototype;
- DE4.5.1 – Content Protection and Supervision (M13), report and prototype;
- DE4.6.1 – Content Distribution via Internet (M13), report and prototype;
- DE4.7.1 – Content Distribution toward mobiles (M13), report and prototype;
- DE4.8.1 – Content Distribution via satellite data broadcast, the push optimisation and the on demand problem (M13), report and prototype;
- DE4.9.1 – The Usability issues for the AXMEDIS production tools (M13), report.

The main activities that have supported the production of this deliverable are related to:

WP4.5 – Content Protection and Supervision – In this subWP, the specification and the design of pilot application for DRM control of the content creation and content distribution scenarios will be performed. This specification will be based on the analysis of the existing standards, security techniques and business models. Formal methods are recommended in order to certify protection properties. The pilot application for DRM control of the content creation and content distribution scenarios will be developed, starting from some basic modules that could be used as reference software of MPEG-21. About legal aspects, the whole value chain coming from the integration of the project partners will be identified and the analysis of contractual and legal aspects including

international aspects and limitations will be carried out as well as the creation of a formal model about legal aspects integrated with the DMR rules and formalisation in MPEG-21 (including international rules). About fingerprint techniques for passive protection the critical issues will be identified and addressed in a definition of strategy. The first versions of the fingerprints will be identified and applied to some specific test cases. Their functionalities as signature and integrity verification code will be assessed. The assessment will be done providing an experimental tool for fingerprint estimation to large content providers. The tool will process all their content offline and it will assess the distribution and the validity of the unique identification. The DRM model will have to integrate the formalisation of licensing aspects and thus of the contract, for the automatic clearance of rights. Detailed analysis of the existing standards, security techniques and business models, Specification and design of a pilot application for DRM control of the content creation and content distribution scenarios, (Pilot application modules specified and designed: Related to Rights Expression Languages (both MPEG-21 REL and ODRL will be considered): License Creation, License Validation, License interpretation, Rights Data Dictionary terms database, Interfacing digital content items and licenses), Check of other modules inside AXMEDIS for performing integration of pilot DRM application, Development of pilot application for DRM control of the content creation and content distribution scenarios (see previous list), Initial integration and test with other chosen modules of the AXMEDIS project of the pilot DRM application, identification of the detailed algorithms and architecture for the protection management using certifier and supervisor approach, report on the MPEG-IPMP mechanisms for the implementation of content protection, including license protection and key usage aspects, identification of the whole value chain coming from the integration of the project partners, Specification and design of the Accounting Managing and Reporting tool, including the database model, analysing contractual and legal aspects including international aspects and limitations, Description of the integration among AXMEDIS Certifier and Supervisor (WP5.6) and Accounting Managing and Reporting tool, formal modelling legal aspects and integrating them with DRM rule and formalisation of MPEG-21, including international rules, Identification critical issues the association of estimation of fingerprint and data integrity, identification of the first versions of the fingerprints and application of them to the test cases provided to assess their functionalities as signature and integrity verification code, an experimental tool fingerprint estimation to large content providers to process all their content offline and assess the distribution and the validity of the unique identification, selecting the best algorithms, integration of the solutions and evaluating and optimising them.

2 Introduction

AXMEDIS will pursue an integrated solution to content distribution, providing flexibility and scalability to support any kind of content over any kind of network, and configurable to support terrestrial, satellite and mobile transport protocols.

The activities that have supported the production of this deliverable are related to the analysis of current protection models and DRM systems as well as contract structure in the different industries and business models involved (music, video, distribution, etc.). Also passive protection techniques, like fingerprinting have been analysed. Apart from this analysis, several prototypes are presented, that provide some solutions to the problems encountered during the analysis of the different aspects of this deliverable.

The main goal of the research and development activities presented in this deliverable are the provision of solutions for content protection aspects (either active and passive), DRM systems based on standards and the connection of DRM with the existing contract models.

2.1 Specification of WP4.5 Content Protection and Supervision

2.1.1 Specification of T4.5.1: Digital Rights management, DRM and licensing model

Major partners involved

FUPF

The objectives of this DRM task can be divided into two different scenarios from the DRM point of view: Content creation and content distribution scenario. In this task, only the fundamental algorithms and protection aspects have been studied and developed.

As a starting point, we have used REL, the Rights Expression Language defined inside the MPEG-21 ISO/IEC international standard, and RDD, the accompanying Rights Data Dictionary, for the description of digital rights associated to content.

The evaluation of existing business models in the area of content distribution and the description of new business models depending on the distribution channel (for example, those for mobile environments) will be a key point. The model of DRM has to allow modification to the DRM and metadata properties for a single or group of objects. This is needed when a content integrator uses protected object components to create a new content object with added value with other DRM rules. These rules include those for distributors and those per eventual direct end user usage. The Distributor may use the content component for creating more complete and sophisticated content. The Rule that one would like to impose upon the final user does not have to violate the initial rules. Thus, verification with formal models is needed. In addition, the distributor may add new rules superseding the previous rules, etc.

State of the art

In section 3, not only the state of the art but also an analysis of the existing DRM systems is described. This analysis will be very useful for a future integration of the tools implemented in AXMEDIS with other DRM systems and solutions.

Research and development plan

The research to be done in this task involves several areas related with the protection and governance of AXMEDIS objects. As a result of these research activities, some modules are going to be implemented.

Coming from the DRM systems analysed, we will look in detail at the different standardisation activities related to rights expression languages, rights data dictionaries and digital rights management systems in order to provide tools that can deal with the most relevant ones related to the AXMEDIS project.

It has been initially decided to create licenses using MPEG-21 REL, as AXMEDIS objects structure is based on the one defined by MPEG-21. Tools for creating licenses in ODRL will be also considered in this part of the project. Nevertheless, the use of different DRM architectures and protection techniques has to be considered during the development of project. As a result, a constant activity research is needed in this task in order to be "up to date" in the different aspects related to these areas.

As MPEG-21 REL is being used, we have the possibility of implementing its authorisation model that could be also applied to other rights expression languages (in particular, to ODRL). This also has a related research activity that is the optimisation of the implementation of this algorithm, as it is quite complex.

Participation in MPEG-21 IPMP standardisation process will be done in the context of the research activity done inside this task. Nevertheless, the implementation of IPMP techniques will be addressed in other tasks of WP4.5.

The evolution of the activities inside DMP will be also followed in this task, considering the possibility of contributing to this initiative as the project evolves. In any case, public results from DMP will be studied in order to apply them to the AXMEDIS project, if possible.

Planned schedule

- M9: Analysis of the existing standards, security techniques and business models related to DRM systems
- M12: Specification and design of a pilot application for DRM of the content creation and content distribution scenarios
- M12: Pilot application modules specified and designed:
    - Related to Rights Expression Languages (both MPEG-21 REL and ODRL will be considered):
        - License Creation
        - License Validation
        - License Interpretation
    - Rights Data Dictionary terms database
- M12: Check of other modules inside AXMEDIS for performing integration of pilot DRM application.
- M13: Development of pilot application for DRM of the content creation and content distribution scenarios (see previous list)
- M18: Initial integration and test with other chosen modules of the AXMEDIS project of the pilot DRM application
- M30: Development of a test-bed with some of the new business models defined for the creation and distribution scenarios. This will be applied in WP8 for the content production.
    - Test bed on business models for creation and distribution may include:
    - RELs translation,
    - DRM and metadata properties modification within the digital item.
- M36: Extension of pilot application for using different initiatives in the description and control of digital rights. The initiatives will be decided at the moment of the extension of the application based on the ones existing at that time.

2.1.2 Specification of T4.5.2: Protection aspect on the AXMEDIS content tools

Major partners involved
DSI

The Content Protection is a fundamental aspect of a Content Production and distribution value-chain. This task involves several stages of the protection domain:

- On the content authoring: Authors and creators expect to freely disseminate and commercially distribute their works, benefiting from a free flow of their content without unwarranted risks due to undesired use or re-use of their creations.
- On the content sharing for production and distribution among B2B partners: content providers must be able to inject content into the AXMEDIS objects with confidence that it will be used consistently with their requirements in order to create rich and intuitive business models and end-user experiences. The content providers are strongly interested in offering attractive services, with the assurance and confidence that they will be remunerated according to applicable agreements.
- On the content distribution over the different channels: new services and usage models must be attractive and secure so that the final users can easily pay for them, and, when given a choice, users will prefer legitimate services. End-users want content to be available and accessible. The rules associated with using content should not be hard to understand and must reflect typical usage of physical assets.

According to this scenario this task brings to AXMEDIS the following innovations:

- Innovative methods to apply protection on authored/compounded AXMEDIS objects, allowing customisable DRM information.
- Analysis of the best technologies to avoid illegitimate usage of the produced content like cryptography for authentication and secure transmission.
- Secure communications framework between content producer/consumer in a unified trusted domain.
- Safe architecture for the authentication of clients to the AXMEDIS Certifier and Supervisor in order to allow content consumption reports and to be robust against terminals, which aim to violate DRM rules.
- Allow protection data to be encapsulated in the AXMEDIS object together with other information about DRM and licensing.

This will lead to the creation in WP5 of the so called Protection tool, a service for protecting content, encryption of content, request of key to the AXMEDIS Certifier and Supervisor, etc. It will allow the protection of single as well as sequences of objects. It will be capable of requesting the key to the AXMEDIS Certifier and Supervisor notifying at the same time that a new object is published in its protected mode with related administrative information: content type, owner, identification, etc.
The MPEG-IPMP part into the MPEG21 standard will be considered and analysed in depth. During the project the innovative methods and architecture will contribute to the development of the standard itself.

State of the art

Nowadays there are several international or de-facto standards, which completely (or in part) deal with the above-listed issues, in particular: Windows Media Series 9 and 10, iTunes and some parts of the MPEG standards such as MPEG-2/4 IPMPX and MPEG-21 IPMP.

Windows Media Series 9 and 10 are a set of tools, which cover the whole distribution chain of digital content. Windows Media provides server-side and client-side tools, which allow to express simple usage condition through a Microsoft custom DRM and to protect digital content using proprietary algorithms. Moreover, Windows Media protection and distribution system works only for Microsoft-specific content formats (e.g. WMA and WMV).

It is to be noticed that, Windows Media security system relies on secrecy of its protection algorithms. Therefore, even if the system demonstrated to be reliable, once the protection algorithms will be discovered the entire system will fail.

Another peculiarity of Windows Media is that it has been designed to control content usage only in the distribution phase of the value chain. Therefore, it does not allow content owner to anyway control their works. In this scenario, content owners have to rely on distributors about revenues originating from their works.

iTunes system works similarly to what Windows Media does, i.e. iTunes relies on proprietary protection method and DRM. iTunes is mainly focused on the MP3 market. In fact, iTunes is also an online market of MP3-encoded music. Moreover, iTunes security system has been already broken demonstrating the liability to be violated of monolithic system.

On the other hand, MPEG standards define general guidelines and specification to realize reliable terminal for the consumption of protected content. MPEG does not specify what kinds of protection tools have to be used to protect content, instead MPEG gives a way to specify for each piece of content the way it has been protected.

MPEG-21 IPMP defines three fundamental XML schemas to:

- declare protected digital item
- express protection information, i.e. how content has been protected
- express general protection information, i.e. which are the prerequisite a compliant terminal should has to manage a given item

MPEG-21 REL and RDD are two powerful means to express rights on the protected content. In particular, REL defines how licenses on digital item have to be expressed and RDD is an expandable dictionary of actions, which can be done on a digital item. In this way whoever in the value chain of digital content can express the rights on its own content, e.g. content owner can decide who can integrate, distribute or change its content.

Using MPEG-21 IPMP, REL and RDD together allow creating powerful and highly configurable and versatile protection systems. Moreover, two different protection systems, which adopt the MPEG-21 standard, can be easily integrated allowing the consumption of content on several platforms.

Research and development plan

According to this scenario this task brings to AXMEDIS the following innovations in terms of research:

- Innovative methods to apply protection on authored/compounded AXMEDIS objects, allowing customisable DRM information
- Analysis of the best technologies to avoid illegitimate usage of the produced content like cryptography for authentication and secure transmission
- Secure communications framework between content producer/consumer in a unified trusted domain
- Safe architecture for the authentication of clients to the AXMEDIS Certifier and Supervisor in order to allow content consumption reports and to be robust against terminals which aim to violate DRM rules
- Allow protection data to be encapsulated in the AXMEDIS object together with other information about DRM and licensing or in separate chunk of information
- Study and development of a Protection Processor for managing the information regarding the protection of the content and the certification
- Study and development of a language for specifying the protection aspects, it can be derived from the IPMP of MPEG-21. The language is processed by the Protection Info and Procedure Interpreter

- Study and development of algorithms and tools for Tool and Device Certification, Tool and Device Registration, Tool and Device Authentication, Tool Profiling, Tool and Device ID estimation, etc.

Planned schedule

- M8: identification of the detailed algorithms and architecture for the protection management using certifier and supervisor approach.
- M12: report on the Protection Processor engine (similarly and extending the MPEG-IPMP mechanisms) for the implementation of content protection, including license protection and key usage aspects.
- M24: first version of the Protection Processor engine (similarly to the IPMP of MPEG21), which coordinates protection tools.
- M36: final support for the Protection tool, which protects content using the keys provided by the Certification Authority implemented in the AXMEDIS Certifier and Supervisor (WP5.6).

2.1.3 Specification of T4.5.3: Contractual and Legal aspects vs. DRM

Major partners involved
AFI, with support of FUPF and DSI

The legal aspects and the impact of DRM on the social attitude of the final user have to be taken into account. In addition, the DRM impact on the behaviour of the performers, publishers, aggregators, etc. Any business model and new mechanism for manipulating IPR must take into account the legal and social aspects. This will involve study, analysis and monitoring of the DRM solution and of the legal issues to be addressed in order to produce, develop, assess and implement the AXMEDIS framework. The task will focus on the content owners' requirements and the specific concerns and current legal issues.

State of the art

On section 4, a study of current legal issues in terms of the different laws involving copyright in Europe are described, as well as the contract analysis on several entertainment models as well as the business models represented by the partners of the AXMEDIS project. It goes beyond state of the art, as it describes an analysis of current contracts.

Research and development plan
As a starting point it has to be taken into account that there is a very important difference between copyright and contract law. Copyright law involves a carefully considered public policy balance that sometime is not reflected in contract law. Copyright law provides a reasonable balance between the rights of copyright owners and the rights of consumers to reasonable access to copyrighted works. Therefore the contractual licensing of copyrighted works should not replace the public policy objectives of copyright law. In determining what rights in pre-existing works may need to be acquired in the digital context, the most important area to examine is copyright. Copyright protects many different types of pre-existing material including, *inter alia*, text, audiovisual works, musical compositions, sound recordings, visual art, photographs, graphics, and animation.

Therefore in order to understand how copyrighted work can be legally used in the digital environment, it is important to start the analysis by evaluating the underlying concepts of IPR and copyright and to identify the key changes to copyright and intellectual property law that have come about as a result of technological changes.

Planned schedule
- M8: identification of the whole value chain coming from the integration of the project partners

- M9: Specification and design of the Accounting Managing and Reporting tool, including the database model
- M12: Analysis of contractual and legal aspects including international aspects and limitations
- M15: Description of the integration among AXMEDIS Certifier and Supervisor (WP5.6) and Accounting Managing and Reporting tool
- M18: Formal modelling of legal aspects and their integration with DRM rules and formalisation in terms of MPEG-21, including international rules
- M24: first prototype of integration of the formalised model into the AXEPTool for right clearance and accounting
- M36: final integration of the formalised model into the AXEPTool for right clearance and accounting

2.1.4 Specification of T4.5.4: Fingerprint and features estimation and data integrity

Major partners involved

FHGIGD

Passive protection techniques such as fingerprinting are still under among current research activities. In contrast to active protection technologies, passive protection technologies do not impede unauthorised access to data. Fingerprinting technologies calculate a unique (irreversible) content related identifier comparable to the human fingerprint. This fingerprint allows the unique identification of the content and can be directly used as a primary key in a database where further content related information (e.g. content creator, content owner, content rights, etc.) is stored. Fingerprinting technologies allow the identification of content, which could have been distributed without any modifications. Different fingerprinting technologies have been developed for audio, images and video. Yet, current research includes the improvement especially to meet the requirements of imperceptibility and robustness. In this WP our activities are driven by the requirements of cross media content and multichannel distribution.

The activities performed in this WP are mainly focussed on study and identifying a solution to the problem of associating or estimating a **unique signature to each content** component that may pass on the AXMEDIS P2P tools and thus towards the distribution side. The main objective is to avoid the passage of non-authorised and identified content in the AXEPTool, thus in the AXMEDIS network and chain. This will guarantee the security of the content and of the content providers.
Study and identifying a solution to the problem of ensure the **data integrity of content**. One of the most important aspects is enabling the application and clients' tools to be fully dynamic, with relayed as soon as it is ready for use, to ensure a smooth user experience. A Data Integrity module should be designed as an open rule-based module, to support any definition and to make sure that only content that has been designated "ready" is supplied to target applications. The Data Integrity Engine should verify automatically that all defined conditions are met, and significantly decreases the risk of user error while consuming the content.
Digital signatures are important for the validation of transaction and also for the verification of data integrity. Hence we will investigate new applications emanating from the combination of existing technologies. Another key aspect in which to work relates to content and owners/users authentication. In this Task also the support for managing the monitoring of digital items on the basis of their unique signature has to be studied. Its development will be performed in the AXMEDIS Certifier and Supervisor.

This can be realised in two manners:

- Estimating unique code on the basis of selected content features, or
- Enforcing a unique and imperceptible code into the digital object content.

On the one hand the second possibility (enforcing a unique and imperceptible code, which is also called watermarking) was already addressed in other projects. On the other hand, the AXMEDIS scenario allows an

efficient and effective usage of perceptual hashing techniques, which are estimating the previously described unique code. Thus, the focus within AXMEDIS is on perceptual hashing. Due to the properties they have in common with human fingerprints, these techniques are also called fingerprinting techniques.

The main requirements of the solution that will be taken are the robustness to the:

- Lossy compression,
- Change of resolution and other technical parameters, especially digital item adaptation,
- A large number of attacks based on video or audio processing.

State of the art

See section 5 for the description and analysis of the different techniques for fingerprint and signature calculation for different kinds of content.

Research and development plan

The activities performed in this WP are mainly focused on study and identifying a solution to the problem of associating or calculating a unique signature to each content component. The research and development plan is in tight connection to that of T4.2.2, where descriptors of different media will be also investigated. In this task research will be mainly focused on fingerprinting algorithms, whereas T4.2.2 integrates all technologies for description, indexing and fingerprinting into a unitary framework.

Research and development within the first 18 month will first be based on the state of the art and its integration within the AXMEDIS framework. After that, steps towards innovations will follow. In general the reimplementation of existing methods is considered as critical for several reasons. Generally, the description of existing solutions is insufficient. Even if the description is extensive, some details like suitable parameters have to be determined by extensive analysis of test sets. Besides these practical problems, existing technologies typically are protected by IPR, which questions the positive effects of a reimplementation. Thereby an obligation of organisations that developed technology is important. As a consequence, the following general steps can be identified:

1. Identification of the research prototypes and products available for the integration within the AXMEDIS framework.
2. A pre-selection will be based on a first analysis. This analysis considers the publicly available information like scientific publications, technical reports or white papers.
3. The pre-selected prototypes or products will be evaluated in practical tests. For these tests the specific requirements within AXMEDIS will be the evaluation foundation.
4. Identified weaknesses or drawbacks will initiate the improvement of existing methods and will lead to the development of new methods

Research in this task is dedicated to the problem of ensure the data integrity of the distributed content.

- Content types used within AXMEDIS and typical processing/production operations
- Investigation of possible features for authentication and verification of multimedia content
- Suitable processing of the features for a targeted improvement according to the identified requirements

The descriptors should be independent of the digital item adaptation used.

Planned schedule

- M12: Identification critical issues of fingerprints for authentication and verification of the data integrity. Identification of the first versions of the fingerprint algorithms. Integration of available algorithms and evaluation based on the test cases
- M14: First version of the fingerprinting algorithm for video, audio, and text files (in terms of MPEG-7 or MPEG-21 if applicable)
- M18: An experimental fingerprint tool for calculating fingerprints for authentication and data integrity verification. Content is processed offline
- M18: Revised first version of the set of fingerprint estimation algorithm for video, audio, and text files
- M24: Study and develop algorithms for the verification of content integrity just before its distribution toward mobiles.
- M28: Study and develop algorithms for the estimation of fingerprint just before its distribution toward mobiles.
- M36: Completion of development of the enabling technologies.

3 Digital rights management and licensing model

This section describes the analysis of digital rights management systems and licensing model issues.

3.1 MPEG-21

MPEG's approach is to define a Multimedia Framework to ensure that the systems that deliver multimedia content are interoperable and that the transactions between them are simplified and automated. This approach should apply to the infrastructure requirements for content delivery, content security, rights management, secure payment, and the technologies enabling them. The result is an open framework for multimedia delivery and consumption for use by all the players in the delivery chain. This open framework will provide content creators, producers, distributors and service providers with equal opportunities in the MPEG-21 [1] enabled open market. This will also be to the benefit of the content consumer providing them access to a large variety of content in an interoperable manner.
The MPEG-21 multimedia framework has two essential concepts the Digital Item, a fundamental unit of distribution and transaction and the Users that interact with Digital Items.

MPEG-21 aims to identify and define the different mechanisms and elements needed to support the multimedia delivery chain, the relationships and the operations supported by them. In the different parts of the MPEG-21 standard, these elements are elaborated by defining the syntax and semantics of their characteristics, such as interfaces to these elements. Seventeenth parts currently form the MPEG-21 standard.

Part 1: Vision, Technologies and Strategy [2]. The purpose of this part of the standard is to define a vision for a multimedia framework to enable transparent and augmented use of multimedia resources across a wide range of networks and devices to meet the needs of all users. This part has as objective to achieve the integration of standards to facilitate harmonisation of technologies for the creation, management, distribution and consumption of digital items. Moreover it shall define a strategy for achieving a multimedia framework based on well-defined functional requirements.

Part 2: Digital Item Declaration (DID) [3]. The second part of the MPEG-21 standard describes a set of abstract terms and concepts to form a useful model for defining Digital Items. A Digital Item is the representation of a work, and as such, it is the thing that is acted upon (managed, described, exchanged, etc.) within the model.

Part 3: Digital Item Identification (DII) [4]. This part of the standard provides a schema that can be used to include identifiers into a Digital Item Declaration. Then, Digital Items and parts thereof (such as resources) could be uniquely identified.

Part 4: Intellectual Property Management and Protection (IPMP) [5]. This part of MPEG-21 will define an interoperable framework for Intellectual Property Management and Protection. It includes standardised ways of retrieving IPMP tools from remote locations, exchanging messages between IPMP tools and between these tools and the terminal. It also addresses authentication of IPMP tools, and integration of rights expressions according to the Rights Data Dictionary and the Rights Expression Language.

Part 5: Rights Expression Language (REL) [6]. A Rights Expression Language is seen as a machine-readable language that can declare rights and permissions using the terms as defined in the Rights Data Dictionary. The REL is intended to provide flexible, interoperable mechanisms to support transparent and augmented use of digital resources in a way that protects digital content and honours the rights, conditions, and fees specified for digital contents. It is also intended to support specification of access and use controls for digital content in cases where financial exchange is not part of the terms of use, and to support exchange of sensitive or private digital content.

Part 6: Rights Data Dictionary (RDD) [7]. The Rights Data Dictionary comprises a set of clear, consistent, structured, integrated and uniquely identified Terms to support the MPEG-21 Rights Expression Language. This part of the standard also specifies the methodology and structure of the RDD Dictionary and specifies how further terms may be defined under the governance of a registration Authority. The RDD System is

made up of the RDD Dictionary and RDD Database taken together. It will facilitate the exchange of information between different parties involved in the administration of rights.

Part 7: Digital Item Adaptation (DIA) [8]. One of the goals of MPEG-21 is to achieve interoperable transparent access to distributed advanced multimedia content by shielding users from network and terminal installation, management and implementation issues. This will primarily enable the provision of network and terminal resources on demand so that multimedia content can be created and ubiquitously shared, always with the agreed/contracted quality, reliability and flexibility. Towards this goal, the adaptation of Digital Items is required. Digital Items are subject to a resource adaptation engine, as well as a descriptor adaptation engine, which together produce the adapted Digital Items.
The target for this part of the standard is to specify tools that provide input to the adaptation engine, so that any constraints on the delivery and consumption of resources can be satisfied, and the quality of the user experience can be guaranteed.

Part 8: Reference Software [9]. In the eighth part of the standard is presented the normative and informative reference software developed in other parts of the MPEG-21 standard, such as REL, RDD, DID, DIA, DIP… and software modules that integrates the functionalities of these parts. Reference software will form the first of what is envisaged to be a number of systems-related specifications in MPEG-21. The development of the Reference Software will be based on the requirements that have been defined in the different parts of MPEG-21.

Part 9: File Format [10]. In this part of the MPEG-21 standard a file format shall be defined. An MPEG-21 Digital Item can be a complex collection of information. Both still and dynamic media can be included, as well as Digital Item information, metadata, layout information, and so on. It can include both textual data and binary data. For this reason, the MPEG-21 file format inherits several concepts from MP4, in order to make 'multi-purpose' files possible. A dual-purpose MP4 and MP21 file, for example, would play just the MPEG-4 data on an MP4 player, and would play the MPEG-21 data on an MP21 player. A 'resource map' allows the inclusion of multiple referenced resources in the same or other files, and for systems-level management of those resources.

Part 10: Digital Item Processing (DIP) [11]. The objective of this part of the standard is to provide a normative set of tools for specifying processing of a Digital Item in a predefined manner. In this way, it will be possible to extend Digital Item Declaration Language in order to add user specific functionality inside the Digital Item. Therefore, the standardisation of Digital Item Processing will allow interoperability at the processing level. The main idea behind the Digital Item Processing Architecture is that, on receipt of a DID, a list of DI Methods that can be applied to the Digital Item is presented to the User. After that the User chooses one Method that is then executed by the DIP Engine.
A Digital Item Method, DIM, is the tool whereby a User specifies some desired functionality. It is expressed using the Digital Item Method Language, DIML, which includes a binding for Digital Item Base Operations. The Digital Item Base Operations, DIBOs are the functional building blocks utilised by a Digital Item Method. They can be considered somewhat analogous to the standard library of functions of a programming language. Digital Item Methods are defined by the Digital Item Base Operations they use to accomplish the handling of the Digital Item according to the intentions of the Digital Item Method author.

Part 11: Evaluation Methods for Persistent Association Technologies [12]. This part consists of the comparison of technical report documents that evaluate persistent association technologies, for example, technologies that link information to identify and describe content using the content itself.
This part of the MPEG-21 standard does not contain any normative behaviour, its purpose is to allow evaluations of such technologies to be conducted using a common methodology rather than to standardise the technologies themselves.

Part 12: Test Bed for MPEG-21 Resource Delivery [13]. This part of the MPEG-21 standard provides a software-based test bed for the delivery of scalable media delivery, and testing/evaluating this scalable media delivery in streaming environments, for example by taking into account varying network environments.

Part 14: Conformance Testing [14]. The purpose of this part is to define conformance testing for other parts of MPEG-21.

Part 15: Event Reporting (ER) [15]. The purpose of this part of the MPEG-21 standard is to provide a standardised way for sharing information about events, referred to digital items and peers that interact with them, within the MPEG-21 multimedia framework. Use cases that help to understand the necessity of event reporting are the monitoring of usage of copyrighted material and the necessity for network nodes to know the connectivity condition between peers within a network when trying to deliver multimedia content. This part of the standard specifies how to express Event Report Requests (ER R) that contain information about which Events to report, what information is to be reported and to whom; and Event Reports (ER) which are created by an MPEG-21 Peer in response to an Event Report Request when the conditions specified by an ER-R are met.

Part 16: Binary Format [16]. This part of the standard describes the methods to binarise MPEG-21 documents.

Part 17: Fragment Identification of MPEG Resources [17] specifies a normative syntax for URI Fragment Identifiers.

3.1.1 Digital Item Declaration (DID)

The two major goals of the Digital Item Declaration part [3] within MPEG-21 are first to establish a flexible and interoperable schema for declaring Digital Items and second to be as general and flexible as possible, providing hooks to enable higher-level functionality and interoperability.
A Digital Item is defined in [3] as a structured digital object, including a standard representation, identification and metadata. It is the fundamental unit of distribution and transaction inside MPEG-21.
The Digital Item Declaration technology is defined in three normative parts: DID Model, Representation and Schema. Digital Item Declaration Model consists on the description of a set of abstract terms and concepts to form a useful model for defining Digital Items. Within this model, a Digital Item is the digital representation of a work, and as such, it is the thing that is acted upon within the model. The aim of this model is to be as general and flexible as possible, providing hooks to enable higher level functionality and interoperability. The model provides a common set of abstract concepts and terms that can be used to define a scheme, or to perform mappings between existing schemes capable of Digital Item Declaration, for comparison purposes.
The terms that form the model are described below:

- Container: The structure that allows items and/or containers to be grouped. Descriptors are useful in order to label the containers with the appropriate information.
- Item: A grouping of sub-items and/or components that are bound to relevant descriptors. Descriptor can contain information about the item.
- Component: The binding of a resource to a set of descriptors that contains information about all or part of the specific resource instance. These descriptors contain control or structural information about the resource, such as bit rate, encryption information….
- Anchor: binds descriptors to a fragment. A fragment corresponds to a specific location or a part of a resource.
- Descriptor: associates information with the enclosing element. This information may be a component or a textual statement.
- Condition: describes the enclosing element as being optional. Multiple conditions associated with an element are combined as a disjunction when determining if include or not the element.
- Choice: describes a set of related selections that can affect the configuration of an item.
- Selection: describes a specific decision that will affect one or more conditions within an item.
- Annotation: describes the information about another element of the model.
- Assertion: defines a configured state of a choice by asserting true, false or undecided values for the predicates associated with the selections for that choice.

- Resource: an individually identifiable asset such as an image, audio, video clip or a textual asset. It may also potentially be a physical object. The resources must be locatable via an unambiguous address.
- Fragment: designates a specific point or range within a resource.
- Statement: a literal textual value that contains information. It can include descriptive, control or identifying information.
- Predicate: an unambiguous identifiable declaration that can be true, false or undecided.

Next figure shows the relationship among some of the terms of the model defined. The digital item represented has a container, which inside groups some items together with their descriptors and components.

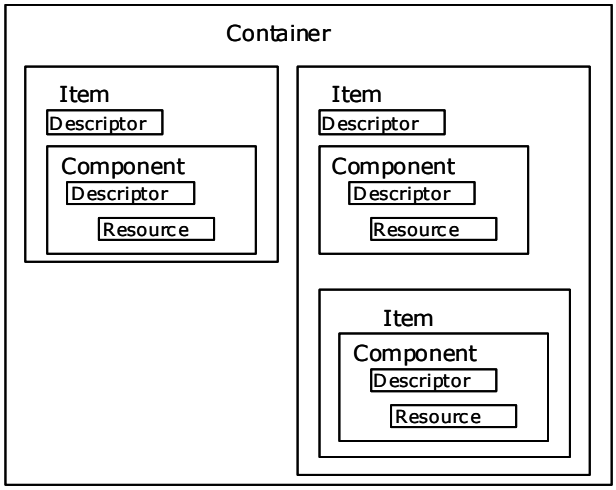


Figure Example Digital Item Declaration

Apart from the declaration model, in MPEG-21 standard part 2 it is also specified the Representation, which describes the syntax and semantics of the Digital Item Declaration elements. The abstract elements defined in the Model that have been represented in DIDL are: Container, Item, Component, Anchor, Descriptor, Choice, Selection, Condition, Annotation, Assertion, Resource and Statement. Two special element types that do not correspond to any of the model elements, Reference and Declarations, have been also defined. The Reference element is used to link the contents of an element inside another element. The Declarations element is used to define a set of Digital Item Description Language elements in a document without actually instantiating them.
A DIDL document consists of a DIDL root element with an Item child element or a Container child element. An Item is a grouping of possible sub-Items and/or Components, bound to a set of relevant Descriptors containing descriptive information about the item. A Component groups a Resource element with a set of Descriptors containing descriptive information about the resource, plus a set of Anchors specifying points or regions of interest in the resource. The Component, being a logical union of a resource with relevant descriptive data and anchors, is intended to be the basic building block of digital content within a DIDL document. A Descriptor associates information with its parent element; this information may be contained in a Component element or in a Statement element. A Statement defines a piece of information pertaining to the parent element. It can include descriptive, control, revision tracking or identifying information. It can contain any data format, including plain text and various machine-readable formats such as well-formed XML. A Statement can also be defined by reference, by specifying the URI of the Statement. A Resource is an individually identifiable asset such as a video or audio clip, an image, an electronic ticket or a textual work.

The ability of inserting data in any kind of data format, specially well-formed XML, inside a Statement provides a wide field for inserting information for the protection and processing of multimedia data. For example, if we want to associate rights expressions to a particular resource within a Digital Item, the REL License can be placed in the Statement of the Descriptor element related to the resource.

3.1.2 Rights Expression Language (REL)

The different parties involved in the online distribution and consumption of multimedia resources need to exchange information about the rights, terms, and conditions associated with each resource at each step in the multimedia resource lifecycle. For example in distribution and super distribution business models, the information related to the rights and the terms and conditions under which the rights may be exercised needs to be communicated to each participant in the distribution chain.
In an end-to-end system, other considerations such as authenticity and integrity of Rights Expressions become important. For example, any content provider or distributor who issues rights to use or distribute resources must be identified and authorised. In addition, different participants may access a Rights Expression, which requires mechanisms and semantics for validating the authenticity and integrity of the Rights Expression. A common Rights Expression Language that can be shared among all participants in this digital workflow is required.

Part 5 of the MPEG-21 standard specifies the syntax and semantics of a Rights Expression Language. MPEG chose XrML as the basis for the development of the MPEG-21 Rights expression language.
MPEG-21 Rights Expression Language (REL) [6] specifies the syntax and semantics of the language for issuing rights for Users to act on Digital Items, their Components, Fragments, and Containers.
The most important concept in REL is the license that conceptually is a container of grants, each one of which conveys to a principal the sanction to exercise a right against a resource. A license if formed by the following elements:

- Title: this element provides a descriptive phrase about the License that is intended for human consumption in user interfaces. Automated processors must not interpret semantically the contents of such title elements.
- Inventory: this element is used for defining variables within a License. In the Inventory element of a license can be defined LicensePart elements that in turn can have licensePartId attributes that can be referenced from elsewhere in the license.
  Therefore, REL provides a syntactic mechanism for reducing redundancy and verbosity in Licenses that can be used throughout a License.
- Grant or GrantGroup: The Grants and GrantGroups contained in a license are the means by which authorisation policies are conveyed in the REL architecture. Each Grant or GrantGroup that is an immediate child of a license exists independently within that license, no collective semantic (having to do with their particular ordering or otherwise) is intrinsically associated with the presence of two or more of them within a certain license.
- Other information: Using the wildcard construct from XML Schema, a License provides an extensibility hook within which license issuers may place additional content as they find appropriate and convenient. This can be useful for conveying information that is peripherally related to, for example, authentication and authorisation, but is not part of the REL core infrastructure.
  It should, however, be carefully understood that not all processors of REL licenses will understand the semantics intended by any particular use of this extensibility hook. Processors of the license may choose wholly at their own discretion to completely ignore any such content that might be present therein.

Next figure shows the structure of a REL License.

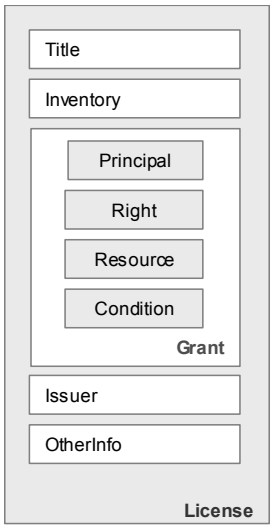


Figure REL License Structure

The most important concept within a license is the grant that conveys to a particular principal the sanction to exercise some identified right against some identified resource, possibly subject to the need for some condition to be first fulfilled. A Grant is an XML structure that is at the heart of the rights management and authorisation policy semantics that REL is designed to express.

A grant is formed by four elements. The Principal represents the unique identification of an entity involved in the granting or exercising of Rights. The Right specifies an action or activity that a Principal may perform on, or using, some associated target Resource. The Resource represents the object against which the Principal of a Grant has the Right to perform. The use of a digital resource in a Grant provides a means by which a sequence of digital bits can be identified within the Grant. The Condition element represents grammatical terms, conditions and obligations that a Principal must satisfy before it may take advantage of an authorisation conveyed to it in a Grant.

The issuer element may contain two pieces of information, a set of issuer-specific details about the circumstances under which he issues the license, and an identification of the issuer, possibly coupled with a digital signature for the license. The optional issuer-specific details are found in the details element of the issuer. These details optionally include any of the following information the specific date and time at which this issuer claims to have carried out his issuance of the license and an indication of the mechanism or mechanisms by which the Issuer of the license will, if he later revokes it, post notice of such revocation. When checking for revocation, REL processing systems may choose to use any one of the identified mechanisms, that is, they are all considered equally authoritative as to the revocation status of the issuance of the License.

The structure of a REL license is the one described if it is in clear text, but a REL license can contain only an encryptedLicense element if the license is encrypted. The encryptedLicense element provides a mechanism by which the contents of a License may be encrypted and so hidden from view from inappropriate parties. This mechanism makes straightforward use of XML Encryption Syntax and Processing (XML Encryption). Specifically, the XML content model of a License is a choice between a sequence containing the elements previously described in this section and an encryptedLicense element that represents the encryption of the contents of the License element.

The principals, rights, resources and conditions of the REL are organised in three main groups. The first one, the Core specifies structural elements and types and how are they related. The standard extension and the

multimedia extension specify standard or multimedia principals, rights, resources and conditions. Each one of the parts is related to a namespace. Next table gives the prefix and the corresponding namespace.

Table Namespace prefixes

Part	**Namespace prefix**	**Namespace**
Core	r	urn:mpeg:mpeg21:2003:01-REL-R-NS
Standard	sx	urn:mpeg:mpeg21:2003:01-REL-SX-NS
Multimedia	mx	urn:mpeg:mpeg21:2003:01-REL-MX-NS

At the heart of REL is the REL Core Schema whose elements and types define the core structural and validation semantics that comprises the essence of the specification. The REL Core Schema includes different elements and types organised in four main groups:

- Principals: Within REL, instances of the type Principal represent the unique identification of an entity involved in the granting or exercising of rights. They represent the subject that is permitted to carry out the action involved in exercising the Right. The principal element and its type are conceptually abstracts. Then, it does not indicate how a particular principal is actually identified and authenticated. Rather, this is carried out in types that are derivations of Principal. Such derived types may be defined in extensions to REL in order to provide, for example, a means by which Principals who are authenticated using some proprietary logon mechanism may be granted certain Rights using the REL License mechanism.
  There are derivations that are important and central enough to be defined within the REL core itself:
  - allPrincipals: Structurally, an AllPrincipals Principal is a simple container of Principals. Semantically, an AllPrincipals a represents the logical conjunct of the Principals represented by all of its children.
  - keyHolder: Instances of a KeyHolder Principal represent entities, which are identified by their possession of a certain cryptographic key. For example, using a KeyHolder, a Principal that uses public-key cryptography may be conceptually identified as that Principal which possesses the private key that corresponds to this-here public key.
- Rights: Within REL, instances of the type Right represent a verb that a Principal may be authorised to carry out under the authority conveyed by some authorised Grant. Typically, a Right specifies an action or activity that a Principal may perform on or using some associated target Resource. The semantic specification of each different particular kind of Right should indicate which kinds of Resource if any may be legally used in authorised Grants containing that Right.
  The element right and its type are conceptually abstract. Therefore, the type Right itself does not indicate any actual action or activity that may be carried out. Rather, such actions or activities are to be defined in types that are derivations of Right. Such derived types will commonly be defined in extensions to REL. However, the following rights are related to the domain of the REL core itself:
  - issue: When an Issue element is used as the right in an authorised grant, it is required that resource against which the right is applied in fact be a grant or grantGroup. The grant then conveys the authorisation for the principal to issue the resource.
    At the instant a License is issued, the issuer of the License with respect to all the grants and grantGroups directly authorised therein must hold the issue right.
  - obtain: When an obtain element is used as the right in an authorised grant, the resource must be present and be a grant or a grantGroup. The use of the obtain right can be conceptualised as an offer or advertisement for the sale of the contained grant

  - possessProperty: The possessProperty right represents the right for the associated principal to claim ownership of a particular characteristic, which is listed as the resource associated with this Right.
  - revoke: The authorised act of exercising the revoke right by a principal effects a retraction of a dsig:Signature that was previously issued and thus accomplishes a withdrawal of any authorisation conveyed by that dsig:Signature.
- Resources: An instance of type resource represents the direct object against which the subject principal of a grant has the right to perform some verb. The actual element resource and its type are conceptually abstracts. That is, the type resource itself does not indicate any actual object against which a Right may be carried out. Rather, such target objects are to be defined in types that are derivations of Resource. Such derived types will commonly be defined in extensions to REL. The relevant resources defined within the REL core:
  - digitalResource: Use of a digitalResource resource in a grant provides a means by which an arbitrary sequence of digital bits can be identified as being the target object of relevance within the grant. Specifically, such bits are not required to be character strings that conform to the XML specification, but may be arbitrary binary data. The means by which this is accomplished breaks down into several cases. For example, the bits are to be physically present within the digitalResource or the bits are to be physically located at some external location (e.g. in a Web site).
  - propertyAbstract: An instance of type propertyAbstract represents some sort of property that can be possessed by principals via possessProperty right.
- Conditions: Within REL, instances of the type Condition represent grammatical terms and conditions that a Principal must satisfy before it may take advantage of an authorisation conveyed to it in a grant containing the condition instance. The semantic specification of each different particular kind of condition must indicate the details of the terms, conditions, and obligations that use of the Condition actually imposes. When these requirements are fulfilled, the Condition is said to be satisfied.
  The actual element condition and its type are conceptually abstracts. That is, the type Condition itself does not indicate the imposition of any actual term or condition. Rather, such terms and conditions are to be defined in types that are derivations of Condition. Such derived types will commonly be defined in extensions to REL. The conditions defined within the REL core that we consider relevant to detail:
  - AllConditions: Structurally, an allConditions is a simple container of conditions. Semantically, the allConditions represents a logical conjunct of the conditions represented by all of its children.
  - validityInterval: A ValidityInterval condition indicates a contiguous, unbroken interval of time. The semantics of the condition expressed is that the interval of the exercise of a right to which a validityInterval is applied must lie wholly within this interval. The delineation of the interval is expressed by the presence, as children of the condition, of up to two specific fixed time instants:
    - notBefore element, of type xsd:dateTime, indicates the inclusive instant in time at which the interval begins. If absent, the interval is considered to begin at an instant infinitely distant in the past
    - notAfter element, also of type xsd:dateTime, indicates the inclusive instant in time at which the interval ends. If absent, the interval is considered to end at an instant infinitely distant in the future.

The Standard Extension schema defines terms to extend the usability of the Core Schema, some of them are:

- Right Extensions: Right Uri.

- Resource Extensions: Property Extensions and Revocable.
- Condition Extensions: Stateful Condition, State Reference Value Pattern, Exercise Limit Condition, Transfer Control Condition, Seek Approval Condition, Track Report Condition, Track Query Condition, Validity Interval Floating Condition, Validity Time Metered Condition, Validity Time Periodic Condition, Fee Condition and Territory Condition.
- Payment Abstract and its Extensions: Payment Abstract, Rate, Payment Flat, Payment Metered, Payment per Interval, Payment per Use, Best Price Under, Call for Price and Markup.
- Service Description: WSDL and UDDI
- Country, Region and Currency Qualified Names: Namespace URI Structure, Country Qualified Names, Region Qualified Names and Currency Qualified Names.
- Matches XPath Function: Regular Expression Syntax and Flags.

The REL Multimedia Extension expands the Core Schema by specifying terms that relate to digital works. Specifically describes rights, conditions and metadata for digital works, that includes:

- Rights: Modify, Enlarge, Reduce, Move, Adapt, Extract, Embed, Play, Print, Execute, Install, Uninstall and Delete.
- Resources: Digital Item Resources.
- Conditions: Resource Attribute Conditions, Digital Item Conditions, Marking Conditions, Security Conditions and Transactional Conditions.
- Resource Attribute Set Definitions: Complement, Intersection, Set and Union.

A typical example of a REL license issued to an end-user. In this case a distributor, MusicDist, issues to a user, Alice, a license that permits her the right of play a song, TheEnd.mp3, during this year. The license is sketched in the following figure.

The elements of the license are the grant and the issuer. The grant element is formed by four elements. The keyHolder represents the user, Alice, which is identified by her possession of a certain cryptographic key. Alice is identified as the Principal that possess the private key that corresponds to this-here public key. The play element represents the right. The definition of Play in the Rights Data Dictionary is to derive a transient and directly perceivable representation of a resource. The digitalResource element provides a means by which an arbitrary sequence of digital bits can be identified as being the target object of relevance within the Grant. Conceptually, an instance of DigitalResource defines an algorithm by which a sequence of bits is to be located. If the bits are to be physically located at some external location, for instance when they are located on a Web site, we use the nonSecureIndirect child element to indicate the algorithm used to allocate the bits. In this example, we indicate that the song is in the URI http://www.webmusic.com/TheEnd.mp3. And the fourth one is the ValidityInterval element. It represents a condition that indicates a contiguous, unbroken interval of time. The semantics of this Condition is that the interval of the exercise of a Right to which a ValidityInterval is applied must lie wholly within this interval. The delineation of the interval is expressed by the presence, as children of the Condition, of up to two specific fixed time instants, notBefore of type xsd:dateTime, indicates the inclusive instant in time at which the interval begins, 1 January 2004. And the notAfter element of type xsd:dateTime, indicates the inclusive instant in time at which the interval ends, 31 December 2004. Therefore, with this license the user can play the song during this year.

The issuer element indicates the entity that issues the license. In this example, it represents the music distributor that has the right to issue this kind of licenses to end-users.

```
<?xml version="1.0" encoding="UTF-8"?>
<r:license xmlns:r="urn:mpeg:mpeg21:2003:01-REL-R-NS" xmlns:sx="urn:mpeg:mpeg21:2003:01-REL-SX-NS"
xmlns:mx="urn:mpeg:mpeg21:2003:01-REL-MX-NS" xmlns:dsig="http://www.w3.org/2000/09/xmldsig#"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    <r:grant>
        <r:keyHolder licensePartID="Alice">
            <r:info>
                <dsig:KeyValue>
                    <dsig:RSAKeyValue>
                        <dsig:Modulus>KtdToQQyzA===</dsig:Modulus>
                        <dsig:Exponent>AQABAA===</dsig:Exponent>
                    </dsig:RSAKeyValue>
                </dsig:KeyValue>
            </r:info>
        </r:keyHolder>
        <mx:play/>
        <r:digitalResource>
            <r:nonSecureIndirect URI="http://www.webmusic.com/theEnd.mp3"/>
        </r:digitalResource>
        <r:validityInterval>
            <r:notBefore>2004-01-01T00:00:00</r:notBefore>
            <r:notAfter>2004-12-31T12:59:59</r:notAfter>
        </r:validityInterval>
    </r:grant>
    <r:issuer>
        <r:keyHolder licensePartID="MusicDist">
            <r:info>
                <dsig:KeyValue>
                    <dsig:RSAKeyValue>
                        <dsig:Modulus>X0j9q99yzA===</dsig:Modulus>
                        <dsig:Exponent>AQABAA===</dsig:Exponent>
                    </dsig:RSAKeyValue>
                </dsig:KeyValue>
            </r:info>
        </r:keyHolder>
    </r:issuer>
</r:license>
```

Figure REL License Example

The authorisation model is another important concept of the REL. It is used by any implementation of software, which makes an authorisation decision using REL licenses. The central question that lies in this decision-making process *"is a principal authorised to exercise a right against a resource?"*
The REL Authorisation Model makes use of an authorisation request, an authorisation context, an authorisation story, and an authoriser.
An authorisation request can be conceptualised as representing the question if is it permitted for a given Principal to perform a given Right upon a given Resource during a given time interval based on a given authorisation context, a given set of Licenses, and a given trust root.
The authorisation request contains the following members:

- the principal element, which is the identity of the entity for which permission is requested
- the right element, which embodies the semantics of the action which is requested to be permitted
- the resource element identifying the Resource upon which permission is requested
- the interval of time during which the requested performance of the right by the principal upon the resource is considered to take place. This may be either an instantaneous point in time or an unbroken interval of time
- the authorisation context containing properties representing statements that are to be considered true for the purposes of establishing the requested permission

- the set of license elements that may be consulted to establish the requested permission. The algorithm will attempt to find authorised grants or grantGroups within this licenses that it can use to establish a basis for an affirmative authorisation decision
- the set of grant elements that do not require an authoriser for the purposes of establishing the requested permission

Next figure shows the structure of an Authorisation Request.

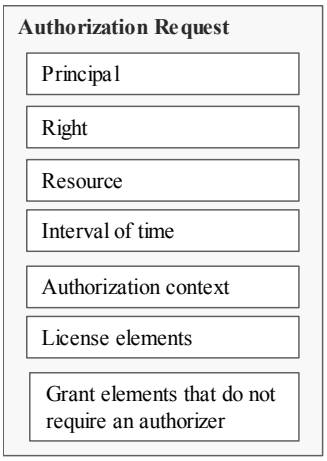


Figure REL Authorisation Request

The authorisation story, the following figure, contains the following elements:

- a primitive grant, it is used to demonstrate to which authorisation requests the authorisation story applies
- either a grant or a grantGroup, it represents the actual grant or grant group that is authorised by the authoriser of the authorisation story
- an authoriser that contains the following members:

  - the license in which the principal is authorised

  - the principal that authorised the license above

  - the time instant in which the license was issued

  - the authorisation context that contains the properties representing statements that were considered true for the purposes of establishing the permission

  - an authorisation story

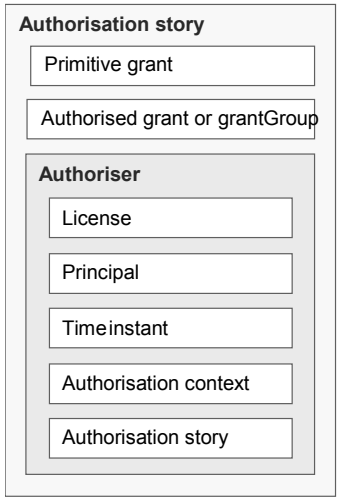


Figure REL Authorisation Story

3.1.3 Rights Data Dictionary (RDD)

The Rights Data Dictionary [7] comprises a set of clear consistent, structured, integrated and uniquely identified Terms to support the MPEG-21 Rights Expression language (REL).

The RDD Dictionary has the characteristics of a structured ontology, in which meaning, once it has been defined, can be passed on from one term to another by logical rules of association such as inheritance and opposition. An ontology, in this context, is a structured catalogue of entities in which meaning, once defined, can be passed on from one term to another by logical rules of association such as inheritance and opposition. The structure of this ontology is designed to provide a set of well-defined terms for use in rights expressions governing the use of Digital Items. In recognition of the great diversity and complexity associated with multimedia content, it is also designed to represent as many different specialisations of meaning as its users require, and to show their relationships in a structured way in order to support the mapping and transformation of terms between different schemas and systems.

The methodology described has been used to create the Standardised Terms for the RDD Dictionary, and may be used in future so that new terms can be introduced under the governance of a Registration Authority. The Standardised Terms in the RDD Dictionary are therefore not a closed list, but the foundations of a widely extensible Rights Data Dictionary.

The RDD System is comprised of the following three elements: the Specifications contained in the RDD Standard, a Dictionary, the Terms and their TermAttributes defined according to this specification and a Database, the tool containing the RDD Dictionary and supporting its maintenance.
The use of the RDD System will facilitate the accurate exchange and processing of information between interested parties involved in the administration of rights in, and use of, Digital Items, and the Rights Expression Language.

The RDD System is designed to support the mapping of Terms from different namespaces. Such mapping will enable the transformation of metadata from the terminology of one namespace (or Authority) into that of another namespace (or Authority). Mapping, to ensure minimum ambiguity or loss of semantic integrity, will be the responsibility of the Registration Authority.
The RDD Dictionary is a prescriptive Dictionary, in the sense that it defines a single meaning for a Term represented by a particular RddAuthorised TermName, but it is also inclusive in that it can recognise the prescription of other Headwords and definitions by other Authorities and incorporates them through mappings. The RDD Dictionary also supports the circumstance that the same name may have different

meanings under different Authorities. Therefore Terms that are directly authorised by the RDD Registration Authority neither define nor prescribe intellectual property rights or other legal entities.

The RDD defines the meaning for the terms defined in the REL. Next table summarises the ActTypes in this part of the MPEG-21 standard that have been defined in response to requirements identified in the process of developing the REL and RDD Standards, particularly focussed on common processes in the use and adaptation of Digital Resources.

Table RDD ActType and its parent and definition

ActType	Parent	Definition
Adapt	Derive, ChangeTransiently	To ChangeTransiently an existing Resource to Derive a new Resource.
Delete	Destroy	To Destroy a DigitalResource.
Diminish	Adapt	To Derive a new Resource to be smaller than its Source.
Embed	Relate	To put a Resource into another Resource.
Enhance	Adapt	To Derive a new Resource to be larger than its Source.
Enlarge	Modify	To Modify a Resource by adding to it.
Execute	Activate	To execute a DigitalResource.
Install	UseTool	To follow the instructions provided by an InstallingResource.
Modify	Change	To Change a Resource, preserving the alterations made.
Move	Modify	To relocate a Resource from one Place to another.
Play	Render, Perform	To Derive a Transient and directly Perceivable representation of a Resource.
Print	Render, Fix	To Derive a Fixed and directly Perceivable representation of a Resource.
Reduce	Modify	To Modify a Resource by taking away from it.
Move	Modify	To relocate a Resource from one Place to another.
Play	Render, Perform	To Derive a Transient and directly Perceivable representation of a Resource.
Uninstall	UseTool	To follow the instructions provided by a UninstallingResource.

When using RDD actTypes in REL is not only important the meaning of the act, it is also important the RDD Hierarchy of the term. In next chapters we will see how it influences the authorisation process. An authorisation can be erroneous if the hierarchy of the right is not taken into account.

3.1.4 Intellectual Property Management and Protection (IPMP) Components

Intellectual Property Management and Protection [5], part 4 of the MPEG-21 standard is in a MPEG Committee Draft phase. MPEG has defined the requirements for MPEG-21 IPMP based on input from a wide variety of interested parties.

In this part of the standard an interoperable framework for Intellectual Property Management and Protection will be defined. MPEG-21 must provide a framework that encourages the creation of new services that can be used to support new business models. These services should meet the needs of the different members of the networks associated with the distribution of digital items.

IPMP is central to the creation of these business models. It must provide more functionally than the existent technologies that have focused its efforts on content protection.

In this part of the MPEG-21 standard is included the expression and enforcement of rights that are associated with digital item distribution, management and usage by all members of the value chain.

The Intellectual Property Management and Protection part deals with the standardisation of a general solution for the management and protection of Intellectual Property. Digital Items can be protected in order to ensure that the access to the contents is done according to the license terms. The solution lies in the use of protection techniques over the digital content, which makes it possible to deploy a business model that ensures the accomplishment of the license terms in a controlled way. These kinds of objects are called IPMP DIDL documents that consist of the protected object (or part of the DIDL document) and the IPMP information expressions. IPMP expressions contain protection information, such as the IPMP tools that protect the content, initialisation settings, keys, etc.; and governance information, such as licenses that govern the content or references to these licenses or license services. In our system, the protection server is the responsible for protecting the content and managing the protection keys and tools. It can also generate the protection information required to be included in Digital Items.

3.2 OMA DRM

The scope of OMA "Digital Rights Management" [18] is to enable the controlled consumption of digital media objects by allowing content providers the ability, for example, to manage previews of DRM Content, to enable superdistribution of DRM Content, and to enable transfer of content between DRM Agents. The OMA DRM specifications provide mechanisms for secure authentication of trusted DRM Agents, and for secure packaging and transfer of usage rights and DRM Content to trusted DRM Agents.
The OMA DRM system enables Content Issuers to distribute Protected Content and Rights Issuers to issue Rights Objects for the Protected Content. The DRM system is independent of media object formats, operating systems, and runtime environments. Content protected by the DRM can be of a wide variety: games, ring tones, photos, music clips, video clips, streaming media, etc. For User consumption of the Content, Users acquire Permissions to Protected Content by contacting Rights Issuers. Rights Issuers grant appropriate Permissions for the Protected Content to User Devices. The Content is cryptographically protected when distributed; hence, Protected Content will not be usable without an associated Rights Object issued for the User's Device.
The Protected Content can be delivered to the Device by any means (over the air, LAN/WLAN, local connectivity, removable media, etc.). But the Rights Objects are tightly controlled and distributed by the Rights Issuer in a controlled manner. The Protected Content and Rights Objects can be delivered to the Device together, or separately. The system does not imply any order or "bundling" of these two objects. It is not within the scope of the DRM system to address the specific payment methods employed by the Rights Issuers.
The OMA DRM specifications define the format and the protection mechanism for DRM Content, the format (expression language) and the protection mechanism for the Rights Object, and the security model for management of encryption keys. The OMA DRM specifications also define how DRM Content and Rights Objects may be transported to devices using a range of transport mechanisms, including pull (HTTP Pull, OMA Download), push (WAP Push, MMS) and streaming. Any interaction between network entities, e.g. between rights issuer and content issuer, is out of scope.

3.2.1 Overall system architecture

The role of DRM in distribution of content is to enable business models whereby the consumption and use of content is controlled. As such, DRM extends beyond the physical delivery of content into managing the content lifecycle. When a user buys content, she may agree to certain constraints - for example by choosing between a free preview version and a full version at cost, or she may agree to pay a monthly fee. DRM allows this choice to be translated into permissions and constraints, which are then enforced when the user accesses the content.

Next figure depicts OMA DRM system architecture [19].

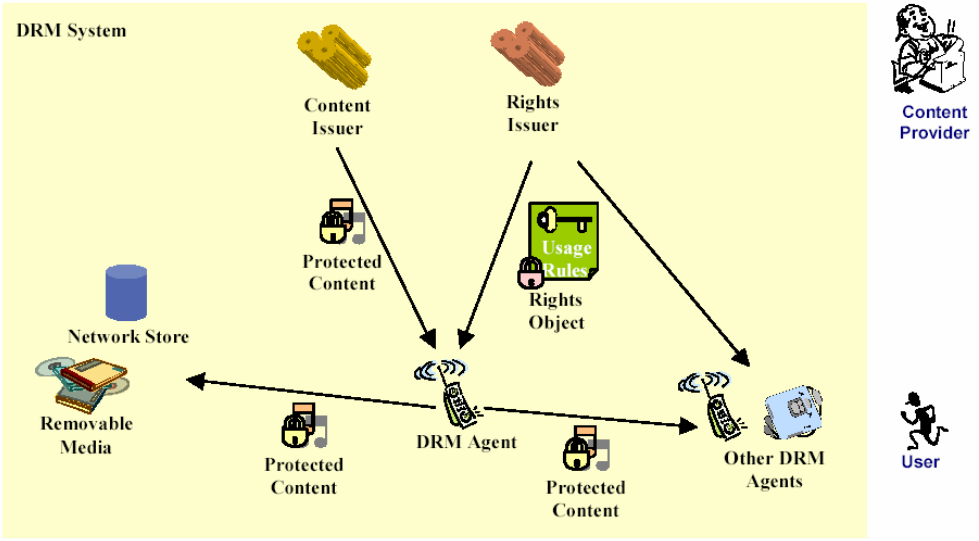


Figure OMA Architecture

Before content is delivered, it is packaged to protect it from unauthorised access. A content issuer delivers DRM Content, and a rights issuer generates a Rights Object. The content issuer and rights issuer embody roles in the system. Depending on deployment they may be provided by the same or different actors, and implemented by the same or different network nodes.
For example, in one deployment, content owners may pre-package DRM Content, which is then distributed by a content distributor acting as both content issuer and rights issuer.
A Rights Object governs how DRM Content may be used. It is an XML document specifying permissions and constraints associated with a piece of DRM Content. DRM Content cannot be used without an associated Rights Object, and may only be used according to the permissions and constraints specified in a Rights Object.
OMA DRM makes a logical separation of DRM Content from Rights Objects. DRM Content and Rights Objects may be requested separately or together, and they may be delivered separately or at the same time. For example, a user can select a piece of content, pay for it, and receive DRM Content and a Rights Object in the same transaction. Later, if the Rights Object expires, the user can go back and acquire a new Rights Object, without having to download the DRM Content again.
Rights Objects associated with DRM Content have to be enforced at the point of consumption. This is modelled in the OMA DRM specifications by the introduction of a DRM Agent. The DRM Agent embodies a trusted component of a device, responsible for enforcing permissions and constraints for DRM Content on the device, controlling access to DRM Content on the device, and so on.
A Rights Object is cryptographically bound to a specific DRM Agent, so only that DRM Agent can access it. DRM Content can only be accessed with a valid Rights Object, and so can be freely distributed. This enables, for example, superdistribution, as users can freely pass DRM Content between them. To access DRM Content on the new device, a new Rights Object has to be requested and delivered to a DRM Agent on that device.
If rights issuers support it, a Rights Object may optionally be bound to a group of DRM Agents. This is known in the OMA DRM specifications as a Domain. DRM Content and Rights Objects distributed to a domain can be shared and accessed offline on all DRM Agents belonging to that domain. For example, a user may purchase DRM Content for use on both her phone and her PDA.

3.2.2 Trust and Security Model

The fundamental challenge facing any DRM solution is how to ensure that permissions and constraints associated with DRM Content are enforced. The main threat comes from unauthorised access to DRM

Content beyond what is stipulated by the associated Rights Objects, or creation of illegal copies and redistribution of valuable content such as music and games. Rights Objects and DRM protection are enforced at the point of consumption. This is modelled in the OMA DRM specifications by the introduction of a DRM Agent. The DRM Agent embodies a trusted environment within which DRM Content can be securely consumed. Its role is to enforce permissions and constraints and to control access to DRM Content.

The basic steps for distributing DRM Content can be summarised as follows:

1. Content packaging: Content is packaged in a secure content container (DCF). DRM Content is encrypted with a symmetric content encryption key (CEK). Content can be pre-packaged, i.e. content packaging does not have to happen on the fly. Although not required by the OMA DRM specifications or the OMA DRM architecture, it is recommended that the same CEK is not used for all instances of a piece of content. Using the same CEK for all content instances would pose a greater risk if a single device were to be hacked and a CEK stored on that device exposed. Using a different CEK for different deliveries or different devices will limit this risk.
2. DRM Agent authentication: All DRM Agents have a unique private/public key pair and a certificate. The certificate includes additional information, such as maker, device type, software version, serial numbers, etc. This allows the content and rights issuers to securely authenticate a DRM Agent. Any privacy aspects with releasing such information are addressed in the technical specifications.
3. Rights Object generation: A Rights Object is an XML document, expressing the permissions and constraints associated with the content. The Rights Object also contains the CEK – this ensures that DRM Content cannot be used without an associated Rights Object.
4. Rights Object protection: Before delivering the Rights Object, sensitive parts are encrypted (e.g. the CEK), and the Rights Object is then cryptographically bound to the target DRM Agent. This ensures that only the target DRM Agent can access the Rights Object and thus the DRM Content In addition, the RI digitally signs the RO.
5. Delivery: The RO and DCF can now be delivered to the target DRM Agent. Since both are inherently secure, they can be delivered using any transport mechanism (e.g. HTTP/WSP, WAP Push, MMS). They can be delivered together, e.g. in a MIME multipart response, or they can be delivered separately.

The DRM Agent has to be trusted by the rights issuer, both in terms of correct behaviour and secure implementation. In OMA DRM, each DRM Agent is provisioned with a unique key pair, and an associated certificate, identifying the DRM Agent and certifying the binding between the agent and this key pair. This allows rights issuers to securely authenticate the DRM Agent using standard PKI procedures.
The information in the certificate enables the Rights Issuer to apply a policy based on its business rules, the value of its content, etc. For example, a rights issuer may trust certain manufacturers, or it may keep an updated list of DRM Agents that are known to be good or bad according to some criteria defined by the rights issuer. It is also possible for a group of stakeholders to establish a joint authority identifying trusted DRM Agents, with legally binding compliance rules.

Revocation in this model amounts to not distributing content any more to DRM Agents that are no longer considered trusted.

What constitutes a trusted DRM Agent depends on the policy and business model of rights issuers. For example, if a hack or a fault compromises a whole class of devices, a rights issuer may decide to stop distributing new content to all devices of that type or class. This is a worst-case scenario. At the other end of the spectrum, maybe there is a known bug in devices of a certain type, but the risk of content leaking is relatively small. In such cases, content and rights issuers may choose to continue to deliver content to existing devices, and instead let manufacturers correct the problems in future versions. Either way, the secure mechanism for authenticating DRM Agents enables rights issuers to enforce such policies.

The DRM Content Format (DCF) is a secure content package for encrypted content, with its own MIME content type. In addition to the encrypted content it contains additional information, such as content

description (original content type, vendor, version, etc.), rights issuer URI (a location where a Rights Object may be obtained), and so on. This additional information is not encrypted and may be presented to the user before a Rights Object is retrieved. Since a DCF is inherently secure, it can be transported using any transport protocol, e.g. in an HTTP response or in an MMS message. It can be stored for back up on any kind of storage, e.g. removable media or a networked PC. It can be copied and sent to another DRM Agent, where a Rights Object may be acquired for use on the receiving device (superdistribution). The content encryption key needed to unlock DRM Content inside a DCF is contained within a Rights Object. Thus it is not possible to access DRM Content without a Rights Object. DRM Content can only be used as specified in a Rights Object. OMA DRM includes a mechanism allowing a DRM Agent to verify the integrity of a DCF, protecting against modification of the content by some unauthorised entity.

Rights Objects are used to specify consumption rules for DRM Content. The Rights Expression Language (REL) defined by OMA DRM specifies the syntax (XML) and semantics of permissions and constraints governing the usage of DRM Content. An instance of a rights document is called a Rights Object, and has its own MIME content type. Rights Objects are made up of permissions (e.g. play, display and execute) and constraints (e.g. play for a month, display ten times). Rights Objects may also include constraints that require a certain user (user identity) to be present when the content is used. These permissions and constraints, along with other information embodied in the Rights Object, (e.g. copyright information) may be presented to the user. The Rights Object also governs access to DRM Content by including the content encryption key (CEK).

A single Rights Object may be associated with multiple pieces of DRM Content. Further, it is possible to assign different permissions to different components of a composite object.

Conversely, a single piece of DRM Content may be associated with multiple Rights Objects. If there are multiple Rights Objects associated with a piece of DRM Content, each Rights Object is treated individually – Rights Objects are not combined. This means that at any one time, there may be more than one Rights Object whose constraints are satisfied. When this is the case, the DRM Agent selects one to enforce. This selection may be made automatically by the DRM Agent based on some selection criteria, e.g. picking the least restrictive Rights Object, or it may be done based on user interaction.

A Rights Object is protected using a rights encryption key (REK). The REK is used to encrypt sensitive parts of the Rights Object, such as the CEK. In addition, the RI digitally signs the RO.

During delivery, the REK is cryptographically bound to the target DRM Agent. In this way only the target DRM Agent can access the Rights Object, and thus the CEK.
Since a protected Rights Object is inherently secure, it can be copied and stored off-device for backup purposes. Some permission requires maintenance of state by the DRM Agent, for example a limited number of plays. Rights Objects containing such permissions cannot be copied or stored off-device, if this would result in loss of state information - e.g. current number of plays.

3.2.3 The Rights Object Acquisition Protocol (ROAP) Suite

The Rights Object Acquisition Protocol (ROAP) is the common name for a suite of DRM security protocols between a Rights Issuer (RI) and a DRM Agent in a Device. The protocol suite contains:

- 4-pass protocol for registration of a Device with an RI and two protocols by which the Device requests and acquires Rights Objects (RO). The Registration protocol is a complete security information exchange and handshake between the RI and the Device and is generally only executed at first contact, but may also be executed when there is a need to update the exchanged security information, or when the Rights Issuer deems DRM Time in the Device inaccurate. This protocol includes negotiation of protocol parameters and protocol version, cryptographic algorithms, exchange of certificate preferences, optional exchange of certificates, mutual authentication of Device and RI, integrity protection of protocol messages and optional Device DRM Time synchronisation. Successful completion of the Registration protocol results in the establishment of an

RI Context in the Device containing RI-specific security related information such as agreed protocol parameters, protocol version, and certificate preferences. An RI Context is necessary for execution of the other protocols in the ROAP suite.

- 2-pass RO acquisition protocol encompasses request and delivery of an RO. It is the protocol by which the Device acquires Rights Objects. This protocol includes mutual authentication of Device and RI, integrity-protected request and delivery of ROs, and the secure transfer of cryptographic keying material necessary to process the RO. The successful execution of this protocol assumes the Device to have a pre-established RI Context with the RI.
- 1-pass RO acquisition protocol is only a delivery of an RO from an RI to a Device (e.g. messaging/push). Its successful execution assumes the Device to have an existing RI Context with the sending RI. In contrast to the 2-pass RO acquisition protocol, it is initiated unilaterally by the RI and requires no messages to be sent by the Device. One use case is distribution of Rights Objects at regular intervals, e.g. supporting a content subscription. The 1-pass protocol is essentially the last message of the 2-pass variant.
- 2-pass Join Domain protocol is the protocol by which a Device joins a Domain. The protocol assumes an existing RI Context with the RI administering the Domain. Successful completion of the Join Domain protocol results in the establishment of a Domain Context in the Device containing Domain-specific security related information including a Domain Key. A Domain Context is necessary for the Device to be able to install and utilise Domain ROs.
- 2-pass Leave Domain protocol is the protocol by which a Device leaves a Domain. The protocol assumes an existing RI Context with the RI administering the Domain.

3.2.4 Rights Expression Language

OMA (Open Mobile Alliance) has developed the OMA DRM Rights Expression Language versions [20] based on ODRL [21].

Rights are the collection of permissions and constraints defining under which circumstances access is granted to DRM Content. The structure of the rights expression language enables the following functionality:

1. Metadata such as version and content ID
2. The actual rights specification consisting of
    a. Linking to and providing protection information for the content, and
    b. Specification of usage rights and constraints

Models are used to group rights elements according to their functionality, and thus enable concise definition of elements and their semantics. The following models are used throughout this specification:

- Foundation model: constitutes the basis for rights. It contains the rights element bringing together meta-information and agreement information. The foundation model serves as the starting point for incorporating the agreement model and the context model.
- Agreement model: expresses the Rights that are granted over DRM Content. It consists of the agreement element connecting a set of Rights with the corresponding DRM Content specified with the asset element. The agreement model incorporates the permission model and the security model
- Context model: provides meta-information about the rights. It augments the foundation model, the agreement model, and the constraint model by expressing additional information.
- Permission model: augments the agreement model. It facilitates the expression of permissions over assets by specifying the access granted to a device. The permission model incorporates the constraint model allowing fine-grained consumption control of DRM Content. The set of permissions comprises play, display, execute, print, and export. Usage of the DRM Content MUST only be granted according to the permissions explicitly specified by the corresponding Rights Object(s). A permission that does not contain a constraint child element is unconstrained and access according to the respective permission element(s) MUST be granted. Note that the REL only specifies consumption and export rights and not management rights, e.g., install, uninstall, delete, or distribution rights. This is made possible by the separation of DRM Content and Rights Objects (although DRM Content and Rights Objects may be delivered together) freeing the REL from unnecessary complexity and overhead. Content can be stored; however, it can only be accessed if a

corresponding Rights Object is available. Similarly, encrypted content can be super-distributed without unnecessarily complicating the REL; no separate distribution permissions are necessary, since DRM Content without the decryption key is of no value. The DRM Agent MUST ignore unknown or unsupported permission elements. The DRM Agent MUST NOT grant alternative, not explicitly specified rights to access Content instead. Known and supported permission elements defined by the same Rights Object MUST remain unaffected and the DRM Agent MUST grant access according to those. A Permission that is not granted due to unknown or unsupported constraints (section 5.5) MUST NOT affect the granting of other permissions.

- Constraint model: enhances the permission model by providing fine-grained consumption control of content. Constraints are associated with one permission element at a time. For a permission to be granted all its constraints MUST be fulfilled. If a constraint is not understood or cannot be enforced by the consuming device the parent permission is invalid and must no be granted. If present, a constraint element should contain at least one of its child elements. If a constraint element does not contain any constraints such as count, date/time, etc. it is unconstrained, and a DRM Agent must grant unconstrained access according to the permission containing such an unconstrained constraint element.
- Inheritance model: describes how a parent Rights Object can specify Permissions and Constraints for one or more pieces of DRM Content each governed by a child Rights Object, using a limited subset of the ODRL inheritance model. The DRM Agent must not accept parent child Rights Objects constellations with more than one level of inheritance (i.e. parent-child). In other words, a parent Rights Object must not inherit Permissions and Constraints from another Rights Object.
- Security model: Security constitutes an important part of a DRM system. OMA DRM 2.0 provides confidentiality for the CEK of Rights Objects, integrity of the association between Rights Objects and DRM Content and Rights Object integrity and authenticity. The ODRL security model, which forms the basis for the security model of this specification, is based on XMLENC [22] and XMLSIG [23].

3.3 Windows Media DRM

Windows Media digital rights management (DRM) [24] is a proven platform to protect and securely deliver content for playback on a computer, portable device, or network device. It's flexible to support a range of business models from single downloads or physical format delivery. The latest version of Windows Media DRM enables new scenarios and provides consumers even greater access to protected audio and video content.

Scenarios below present some business models and acquisition scenarios that Windows Media DRM can enable.

- Direct License Acquisition
- Indirect License Acquisition
- Subscription Services
- Purchase and Download Single Tracks
- Rental Services
- Video-on-Demand and Pay-Per-View

The Windows Media DRM platform enables the secure delivery of protected content for playback on a computer, portable device, or network device.

- Windows Media DRM 10 for Portable Devices
- Windows Media DRM 10 for Network Devices
- Windows Media Rights Manager 10 SDK
- Windows Media Format 9.5 SDK
- Windows Media Data Session Toolkit

Windows Media Rights Manager allows content providers to deliver songs, videos and other digital media content over the Internet in a protected, encrypted file format. Windows Media Rights Manager helps protect digital media (such as songs and videos) by packaging digital media files. A packaged media file contains a version of a media file that has been encrypted and locked with a "key." This packaged file is also bundled with additional information from the content provider. The result is a packaged media file that can only be played by a person who has obtained a license.

3.3.1 Architecture

The basic Windows Media Rights Manager process is as follows:

- Packaging: Windows Media Rights Manager packages the digital media file. The packaged media file has been encrypted and locked with a "key." This key is stored in an encrypted license, which is distributed separately. Other information is added to the media file, such as the URL where the license can be acquired. This packaged digital media file is saved in Windows Media Audio format (with a .wma file name extension) or Windows Media Video format (with a .wmv file name extension).
- Distribution: The packaged file can be placed on a Web site for download, placed on a media server for streaming, distributed on a CD, or e-mailed to consumers. Windows Media Rights Manager permits consumers to send copy-protected digital media files to their friends, as well.
- Establishing a License Server: The content provider chooses a license clearing house that stores the specific rights or rules of the license and implements the Windows Media Rights Manager license services. The role of the clearinghouse is to authenticate the consumer's request for a license. Digital media files and licenses are distributed and stored separately, making it easier to manage the entire system.
- License Acquisition: To play a packaged digital media file, the consumer must first acquire a license key to unlock the file. The process of acquiring a license begins automatically when the consumer attempts to acquire the protected content, acquires a pre-delivered license, or plays the file for the first time. Windows Media Rights Manager either directs the consumer to a registration page where information is requested or payment is required, or "silently" retrieves a license from a clearinghouse.
- Playing the Media File: To play the digital media file, the consumer needs a media player that supports Windows Media Rights Manager. The consumer can then play the digital media file according to the rules or rights that are included in the license. Licenses can have different rights, such as start times and dates, duration, and counted operations. For instance, default rights may allow the consumer to play the digital media file on a specific computer and copy the file to a portable device. Licenses, however, are not transferable. If a consumer sends a packaged digital media file to a friend, this friend must acquire his or her own license to play the file. This PC-by-PC licensing scheme ensures that the packaged digital media file can only be played by the computer that has been granted the license key for that file.

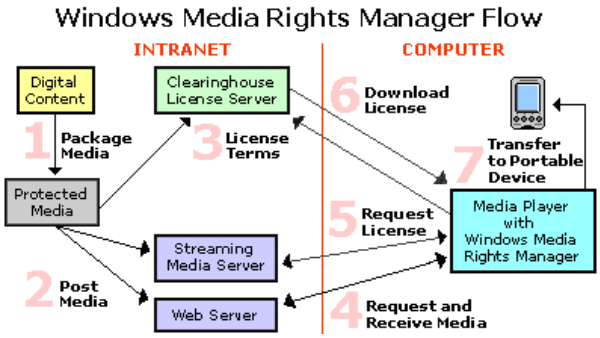


Figure WindowsMedia Rights Manager Flow

3.3.1.1 Licenses and keys

The content owner locks their content with a "key" to create a packaged file. Before the consumer can play the file, the license-clearing house creates a license containing the key that can unlock the packaged file and download the license to the consumers PC. The following diagram shows how keys are created and used in Windows Media Rights Manager.
To generate a key, a license key seed and a key ID are needed:

- The license key seed is a value that is known only to the content owner and license-clearing house.
- The content owner creates a key ID for each Windows Media file. This value is included in the packaged file.

When the license-clearing house needs to issue a license for a packaged file, a key can be recreated by retrieving the key ID from the packaged file. The Windows Media License Service uses the license key seed (which the clearing house provides) and the key ID from the packaged file to create a key. The key is included in the license sent to the consumer's computer. Using the key included in the license, the player on the consumer's computer can open and play the protected file.

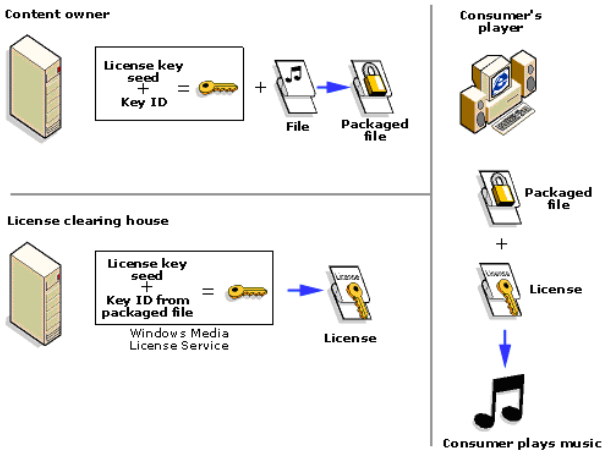


Figure Licenses and keys

Each license contains the key to unlock the Windows Media file. The license also contains the rights, or rules, that govern the use of the digital media file. The content owner sets these rights to determine which actions are allowed from minimal control over playback to more restrictive licenses. The licenses in Windows Media Rights Manager can support a wide range of different business rules, including:

- How many times a file can be played.
- Which devices a file can be played or transferred on. For example, rights can specify if consumers can transfer the file to portable devices that are compliant with the Secure Digital Music Initiative (SDMI).
- When the user can start playing the file and what is the expiration date.
- If the file can be transferred to a CD recorder (burner).
- If the user can back up and restore the license.
- What security level is required on the client to play the Windows Media file.
- And many others.

Licenses can be delivered in different ways and at different times, depending on the business model. The content owner might want licenses pre-delivered, or they might want the license delivered after a consumer

has downloaded and attempted to play a packaged file for the first time. Licenses can be delivered with or without the consumer being aware of the process using silent or non-silent license delivery.

3.3.2 Windows Media DRM 10

Microsoft is introducing two new technologies that allow devices to use media files protected with Microsoft® Windows Media® digital rights management (DRM) technology.

- Microsoft Windows Media DRM 10 for Portable Devices: a lightweight DRM technology that enables portable devices, for example music players, digital video recorders and mobile phones, to use protected content. A portable device built on this technology can host a player that allows approved users to acquire and play protected content, subject to the rights in the license.
- Microsoft Windows Media DRM 10 for Network Devices: Network devices use Windows Media DRM 10 for Network Devices to render protected content from a computer running Microsoft Windows® XP or Windows XP Media Center Edition over a home network. These devices include set-top boxes for video playback (sometimes called Digital Media Receivers), or audio playback (sometimes called Digital Audio Receivers). A network device only requests protected content and renders it immediately. It cannot store or perform any other actions on content.

Both technologies require the device designer to sign a licensing agreement with Microsoft.
It is a porting kit that enables portable devices to play content that was protected using the Windows Media Rights Management Software Development Kit (SDK).

3.3.2.1 Windows Media DRM 10 for Portable Devices

Windows Media DRM 10 for Portable Devices is a porting kit that enables portable devices to play content that was protected using the Windows Media Rights Management Software Development Kit (SDK). The porting kit provides ANSI C source code for functions that are required to build a playback application for Windows Media–protected content on a portable device. These functions are a subset of those in the Windows Media Rights Manager SDK, optimised for the smaller RAM and storage sizes of portable devices. These functions only cover the tasks that a portable device can perform, such as license acquisition, playback (subject to the license associated with a piece of content), and license management functions. These functions do not allow license creation or content encryption.
As well as the porting kit, it is also necessary a Windows Media license server to develop a Windows Media application.
The rights valid on a portable device include most rights valid on a personal computer, plus a few rights specific to portable devices. These rights enable or require an application to play content, maintain a metered play count, prevent playback on compromised or out-of-date systems, require periodic security updates, and enforce time-related play conditions for content, such as starting and ending license validity dates. Portable device licenses do not allow content editing or copying.
Windows Media DRM 10 for Portable Devices allows devices like mobile phones to acquire, manage, and play protected content as if they were computers.
The portable device functions are provided to the developer as ANSI C source code. The device designers reference this code and compile it into their applications. Because the source code is written in ANSI C, devices running non-Windows operating systems may use it.

Windows Media DRM 10 for Portable Devices supports the following new DRM features. Some of these features only apply to portable devices.

- **License chaining.** License chaining allows multiple "leaf" content licenses to be attached to a single "root" license that is bound to a device. The "leaf" content license contains only information specific to the song, like the play count or specific rights, while the "root" license may include an overall validity period, such as one month. This is useful for subscription services, because a subscription provider now only needs to update a single root license each renewal period, instead of renewing hundreds or thousands of individual content licenses.

- **Sync lists.** Windows Media DRM 10 for Portable Devices can return an index of time-based licenses or licenses with counts that need to be refreshed. This allows for improved license updating, as the device can quickly locate and update licenses before they expire.
- **Improved license store performance.** License lookup speed has been greatly improved, providing a near constant license location time, no matter how many licenses are in the store.
- **Secure clock.** To use content with time-bound licenses, devices must synchronise a secure clock with a time provider over the Internet or on a computer. This prevents rollback attacks on time-bound content, such as subscription services.
- **Metering.** Play counts for individual songs can be kept, allowing content providers to accurately monitor royalty payments to artists. To maintain user privacy, play counts are not associated with specific users.
- **Output protection.** Licenses can specify what kind of outputs a device may or may not have (video/audio, digital/analogue) and what kinds of security must be attached to these outputs (such as Secure Audio Path).
- **Automated license store garbage collection.** The Windows Media DRM 10 for Portable Devices system automatically deletes expired licenses to optimise memory storage for devices.

Windows Media DRM 10 for Portable Devices supports content license acquisition from either the user's computer, or directly over the Internet, as the following diagram shows.

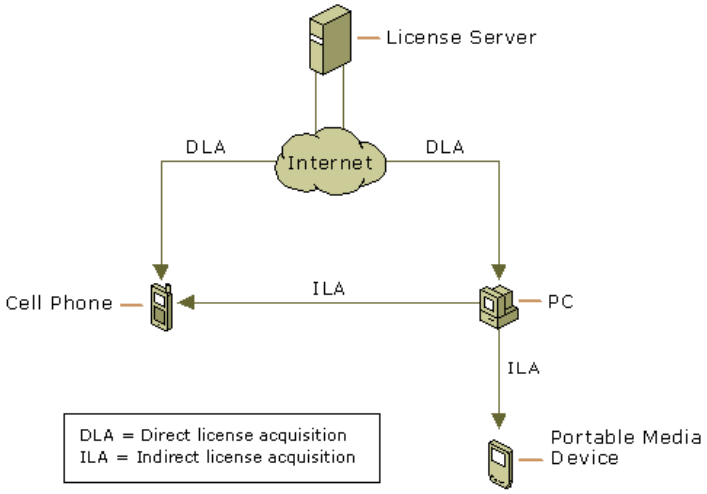


Figure Diagram showing portable devices acquiring licenses

Here are a few scenarios that Windows Media DRM 10 for Portable Devices could enable.

- Music Purchase Service: Using a personal computer and a portable device, or an Internet-enabled portable device, a customer can purchase music. The license associated with the music can allow unlimited play, a specific number of plays, and/or a specific validity period.
- Music Subscription Service: For a monthly fee, a customer using a personal computer and a portable device, or an Internet-enabled portable device could download and play an unlimited number of songs. Once a month, the customer would be required to connect to his or her personal computer or the music service to refresh the music subscription. When the customer docks the device to his or her computer, any licenses that require updating can be updated automatically and silently.
- Movie Rental Service: Portable devices that have video capabilities could allow a customer to download a movie over the Internet with a variety of playback options, such as a limited number of viewings or unlimited viewing for a set period of time (such as 30 days from download time or 48 hours from first play). To prevent content copying, associated rights dictate what kind of video

output capabilities the device can have. Set-top boxes with cable or DSL Internet connections could enable pay-per-view services with all the replay options that a license permits.

- Cell-Phone Ring-Tone Sales: Ring tones with associated licenses to prevent copying could be acquired by Internet-enabled mobile phones.
    - Metering: Portable devices and licenses allow metering. With metering, the application increments a file play count each time it plays a particular media file. When the portable device connects to a personal computer or the Internet, this metering count is uploaded to the content provider. To ensure user privacy, metering counts are not available to the application itself.
    - Metering information is intended solely for use by the content provider or licensor. Metering does not alter or affect any behaviour on the user's system and does not identify the user. Privacy concerns of the user are always respected.
    - Metering allows the content provider to accurately assess royalties, allowing more content to be delivered to portable devices. Metering also allows a content provider to adjust their catalogue to suit their customers' preferences, based on aggregated reports of what content is being played.

3.3.2.2 Windows Media DRM 10 for Network Devices

Windows Media DRM 10 for Network Devices is a porting kit that includes documentation, sample applications, and reference code to help programmers develop applications with Windows Media DRM 10 for Network Devices. These tools ensure that developers can write applications that a device can use to request and receive protected content from a personal computer on a home network. The Windows Media DRM 10 for Network Devices Porting Kit describes the requests and headers that must be exchanged in order for the device to request and receive content. The content can be encoded using any codec included with the Windows Media Format Software Development Kit (SDK).
By using this protocol, the network device acts as a simple rendering device in a home network. This network can be wired or wireless. Whether or not the device is within the home is determined by periodic proximity detection. The network computer storing the content must be running any version of Microsoft Windows® XP and host the Windows Media Connect software component (also called Media Connect). This component handles all media requests from the network device and can also handle license acquisition for content that needs a new or updated license. If licenses must be acquired through the Internet, the computer must have an Internet connection and a browser. A network device can only request files currently on the network computer; it cannot receive streaming Internet content.
Examples of network devices include Digital Media Receivers that stream video to a television and Digital Audio Receivers that play music on a home stereo.

Here is how a network device works:

- The first time a device is used, it must be registered and authorised by the server through Universal Plug and Play. Registration involves a device ID number supplied during manufacturing and a signed XML device certificate. This certificate identifies the device and contains information used to ensure secure communication.
- During initial registration, the server pings the device to verify that it is close enough to be considered inside the home. This is determined by measuring whether the device responds to server proximity detection within 7 milliseconds. This proximity detection also validates the device.
- Periodically, the server repeats proximity detection to revalidate the device.
- The device requests content for playback from the server.
- If the server determines that the device is validated and has the right to play the content, it sends a response containing a new, encrypted session key, a rights policy statement specifying the security restrictions that the device must enforce, and finally the content. The session key encrypts the content. Each time content is requested, a new session is established.
- The network device must parse the rights policy and determine if it can adhere to the required rights. If it can, it may render the content.

The following diagram illustrates devices around the home streaming content over a home network.

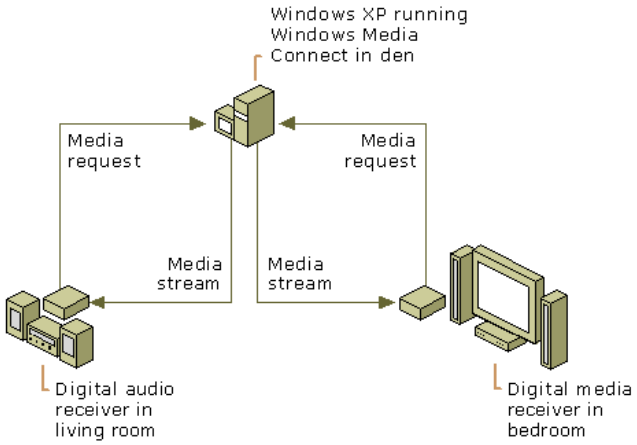


Figure Diagram showing network devices streaming protected content

3.4 TV-Anytime DRM

3.4.1 Introduction

The global TV-Anytime Forum is an association of organisations which seeks to develop specifications to enable audio-visual and other services based on mass-market high volume digital storage in consumer platforms - simply referred to as local storage.

The TV-Anytime Forum was formed at an inaugural meeting held in Newport Beach, California, USA, on 27-29 September 1999. It has started work to develop open specifications designed to allow Consumer Electronics Manufacturers, Content Creators, Telecoms, Broadcasters and Service Providers to exploit local storage.

As part of its formation, the TV-Anytime Forum has established four fundamental objectives for the organisation, which are:

- The TV-Anytime Forum will define specifications that will enable applications to exploit local persistent storage in consumer electronics platforms.
- The TV-Anytime Forum is network independent with regard to the means for content delivery to consumer electronics equipment, including various delivery mechanisms (e.g. ATSC, DVB, DBS and others) and the Internet and enhanced TV.
- The TV-Anytime Forum will develop specifications for interoperable and integrated systems, from content creators/providers, through service providers, to the consumers.
- The TV-Anytime Forum will specify the necessary security structures to protect the interests of all parties involved.

Member organisations from Europe, the USA, and Asia, are drawn from a wide variety of industries: Traditional Broadcasters, Internet Broadcasters, Content Owners, Service Providers, Telecoms, Consumer Electronics Manufacturers, IT Industries, Professional Equipment Manufacturers, Component Manufacturers and Software Vendors.

3.4.2 Rights Management and Protection (RMP)

TV-Anytime [25] has specified a minimum set of usage rules and conditions required to enable protection of broadcast digital television content within a TVA Rights Management and Protection (RMP) compliant domain. When associated with a broadcast signal, RMP Information (RMPI) for Broadcast Applications is

called RMPI-Micro Broadcast (RMPI-MB). When associated with content present in a TVA RMP compliant domain (post broadcast / acquisition) it is called RMPI-Micro (RMPI-M).
RMPI for Broadcast Applications can be used in conjunction with both free-to-air broadcasts and broadcasts protected by CA or DRM systems.

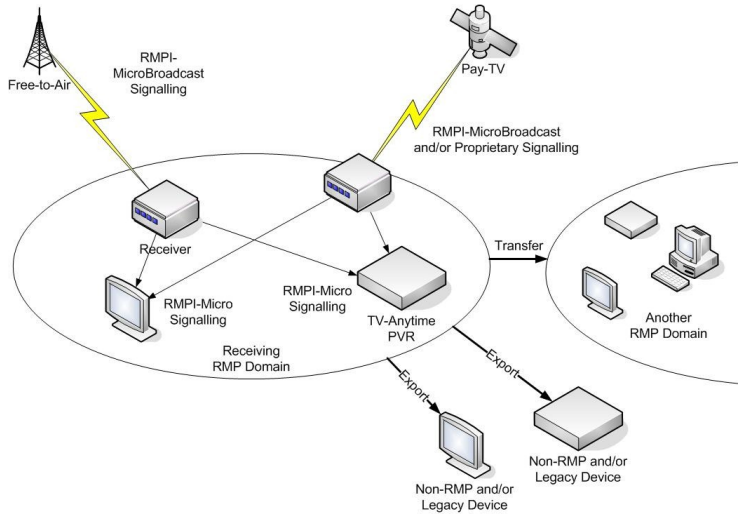


Figure RMPI in the broadcast environment

In the previous figure, transfer of content from one RMP domain to another is not regulated by the RMPI-M/MB but the use of this content is.
"TV-Anytime Phase 1" (TVA Phase 1) is the first full and synchronised set of specifications established by the TV-Anytime Forum. TVA Phase 1 features enable the search, selection, acquisition and rightful use of content on local and/or remote personal storage systems from both broadcast and online services.
The features are supported and enabled by the specifications for Metadata, Content Referencing, Rights Management and Bi-directional Metadata Delivery Protection.

3.4.3 RMP Information for Broadcast Applications

RMP information is a set of usage rules and conditions required to enable protection of broadcast digital television. In TV-Anytime RMPI-MB rights are positively asserted and never implied. These rights are granted to the RMP System and not to a person. When a right is exercised, asserted conditions are validated. If those asserted conditions are not met then the right cannot be exercised, e.g. a user could hit pause without asking for permission, however hitting play after pause would cause the conditions to be validated and the rights to be acquired. If conditions are not asserted, then they do not constrain the rights.

3.4.3.1 RMPI - Micro Broadcast and RMPI – Micro semantics

The elements defined are listed below:

- Principals:
  - Receiving Domain: The receiving domain is the first TVA RMP-compliant domain that receives the content and associated RMPI–MB via broadcast. Once the content is in the domain, the receiving domain is explicitly identified.
  - Any Domain: Any TVA RMP-compliant domain that can respond to the usage conditions stated within RMPI-MB and RMPI-M.
- Rights:
  - Play: is the right to derive a transient and directly perceivable representation of content within the TVA RMP domain.

  - Analogue Export: is the right to create a user accessible analogue signal representing the content as an output, and thus outside of the TVA RMP system. An example of an analogue export would be sending the content over S-Video to a VCR or TV.
  - Digital Export Standard: is the right to create a Standard Definition digital signal representing the content as an output outside of the TVA RMP system.
  - Digital Export High Definition: is the right to create a High Definition digital signal representing the content as an output outside of the TVA RMP system.
  - Extend Rights: this right allows the RMP System to apply additional rights to the content. The absence of this right means that only the originally transmitted rights may be applied.
- Conditions:
  - Geographical Control: This condition limits the use of a right to within one or more specified territories. The granularity of territoriality is to be defined by the compliance body.
  - Single Point of Control: The purpose of this condition is to allow for implementation of device-bound rights within the TVA RMP domain. If present in the broadcast this means that the broadcaster intends that once the content enters the TVA RMP domain, only one RMP entity can make usage decisions about the content based upon the expressed RMPI-MB. Upon reception a received instance of content is now married to a specific RMP entity and that entity can no longer be changed. The entity is then characterised by its identifier.
  - Physical Proximity: This condition limits the use of a right to RMP compliant devices within close physical proximity of the receiver that first received the broadcast content. Close physical proximity is provisionally defined as immediate vicinity e.g. limited to the home network on the same local area network and transmission over a wide area network is not permitted.
  - Buffer Duration: This condition limits the use of a right in such a way that each frame of broadcast content is used only within a specified duration after that frame was broadcast. For instance, if a buffer duration condition of 10 minutes were applied to the right to play content broadcast taking place from 8:00 to 9:00, the content broadcast at 8:00 would be playable until 8:10, the content broadcast at 8:25 would be playable until 8:35, and the content broadcast at 9:00 would be playable until 9:10. If a buffer duration condition of 0 were applied to the right to play content broadcast from 8:00 to 9:00, the content would be only immediately viewable, with no trick play allowed.
  - Time Window Start Date & Time Window End Date: These conditions define the window of time during which the rights are granted. It is defined as absolute start time and absolute expiry time.
  - Standard Definition Digital Export Control: This condition forwards content management rules to external content protection systems on standard definition outputs whilst exercising the Digital Export SD right for immediate viewing only bound to device or media for future viewing. If the content is marked “for immediate viewing only”, then the external content protection system should treat it as “do not store”. If the content is marked “bound to device or media for future viewing”, then the external content protection system is instructed to permit the storage of the content as long as the playback of that content is in the presence of the single device or media to which it was exported. The content can be viewed as well as recorded or stored.
  - High Definition Digital Export Control: This condition forwards content management rules to external content protection systems on high definition outputs whilst exercising the Digital Export HD right: for immediate viewing only bound to device or media for future viewing. If the content is marked “for immediate viewing only”, then the external content protection system should treat it as “do not store”. If the content is marked “bound to device or media for future viewing, then the external content protection system is instructed to permit the storage of the content as long as the playback of that content is in the presence of that single device or media to which it was exported. The content can be viewed as well as recorded or stored.

- Analogue Export Signalling: This condition forwards content management rules to external content protection systems: for immediate viewing only bound to device or media for future viewing (includes immediate viewing).
- Analogue Standard Definition (SD) control: This condition constrains the resolution of the exported analogue signal. If set then Standard Definition resolution only is permitted for an analogue output.
- Security Level: This condition constrains the execution of rights based on the invoked components' robustness level. Security levels are to be based upon the aggregate robustness of all invoked components needed to exercise a right.
- Simultaneous Rendering Count: This condition limits the number of simultaneous Plays, Analogue Exports and Digital Exports of content within a domain. For purposes of this condition a Play counts as a rendering, an Analogue Export counts as a rendering, a Digital Export SD counts as a rendering and a Digital Export HD counts as a rendering.
- Source of additional rights: This condition identifies the authority, which may assign new rights to the content.

Next table depicts ancillary RMPI-MB and ancillary RMPI-M that do not convey usage rules or conditions, but carry further information that is required when handling the content.

Ancillary RMPI-MB and ancillary RMPI-M	**Information to be conveyed**	**Intent**
Scrambling Control	No scrambling Maintain broadcast scrambling Apply RMP cipher	This is to control the scrambling of content when it enters and is stored in the RMP controlled domain. Content is not to be scrambled when stored in the RMP controlled domain. However it may be scrambled when transmitted between devices or when bound to removable media. Self-explanatory do not add RMP cipher. Remove broadcast scrambling if any and apply RMP cipher.
Cipher algorithm	AES Camellia DVB Common Scrambling Algorithm v1 DVB Common Scrambling Algorithm v2 3DES M2 Cipher outside of the control of TV-Anytime RMP	To specify the cipher algorithm used to (de)scramble the content within the TVA RMP Domain.
Version of RMPI	Version of RMPI specification	To identify version of RMPI specification
Origin of RMPI	Identifier / pointer to authority having granted rights	For forensic purposes; this is not to authenticate the origin

Table Ancillary RMPI-MB and ancillary RMPI-M

3.4.3.2 Syntax and encoding for RMPI-MB and RMPI-M

The syntax and encoding for the RMPI-MB and RMPI-M payload is given below. The payload describes the minimum set of usage rights and rules that can be conveyed alongside a digital television broadcast. It is composed of at most four grants including:

- A grant for the "Receiving Domain" that signals the rights and conditions that apply to content once it has entered a given "Receiving Domain". This grant excludes the "Extend Rights" right.
- A grant for "Any Domain" that signals the rights and conditions that apply to content once it has entered "Any Domain". This grant excludes the "Extend Rights" right.
- A grant for the "Receiving Domain" that signals the "Extend Rights" right and associated conditions.
- A grant for "Any Domain" that signals the "Extend Rights" right and associated conditions.

The last two grants are always identical and therefore share the same encoding.
The encoding of the payload allows for the signalling of all relevant conditions for each of the rights expressed in each respective grant. The encoding also allows signalling that no rights have been granted by assigning null values to the respective rights flags. For example, a broadcaster can signal that rights were granted to a "Receiving Domain", and not to "Any Domain", then "Any Domain" rights flags would be set to null. The result of this would be that only those devices in the "Receiving Domain" would have access to the content based on the grants, unless the "Extend Rights" right provided for the acquisition of additional rights.

Table below describes the fixed encoding of RMPI-MB and RMPI-M.

Table RMPI-MB and RMPI-M codes

Syntax	No. of bits	Identifier
RMPI_MB_and_RMPI_M_payload (){		
Ancillary RMPI		
RMPI_type_flag	1	bslbf
Version_of_RMPI	15	bslbf
Origin_of_RMPI	128	bslbf
Scrambling_control	1	bslbf
Cipher	4	bslbf
Extend Rights (Grant is common to Receiving Domain and Any Domain)		
Extend_rights_flag	1	bslbf
Security_level	2	uimsbf
Source_of_additional_rights	128	bslbf
Grant to Receiving Domain		
Domain_ID	128	bslbf
Play_Right_flag	1	bslbf
Analogue_export_right_flag	1	bslbf
Digital_export_SD_right_flag	1	bslbf
Digital_export_HD_right_flag	1	bslbf
Buffer_duration	2	bslbf
Security_level	2	uimsbf
Time_window_start_date	16	uimsbf
Time_window_end_date	16	uimsbf
Geographic_control	128	bslbf
Analogue_export_signalling	2	bslbf
Analogue_SD_control	1	bslbf
Standard_Definition_digital_export_control	2	bslbf
High_Definition_digital_export_control	2	bslbf
Reserved_for_future_use	1	bslbf
Single_point_of_control_flag	1	bslbf
Physical_proximity_flag	1	bslbf
Simultaneous_rendering_count	4	uimsbf
Reserved_for_future_use	2	bslbf
Single_point_of_control_ID	128	bslbf
Grant to Any Domain		
Play_Right_flag	1	bslbf
Analogue_export_right_flag	1	bslbf
Digital_export_SD_right_flag	1	bslbf
Digital_export_HD_right_flag	1	bslbf
Buffer_duration	2	bslbf
Security_level	2	uimsbf
Time_window_start_date	16	uimsbf
Time_window_end_date	16	uimsbf
Geographic_control	128	bslbf
Analogue_export_signalling	2	bslbf
Analogue_SD_control	1	bslbf
Standard_Definition_digital_export_control	2	bslbf
High_Definition_digital_export_control	2	bslbf
Reserved_for_future_use	1	bslbf
}		

3.4.3.2.1 Ancillary RMPI

RMPI_type_flag: This 1-bit field indicates the type of RMPI carried (table below).

Table RMPI_type_flag

Value	Meaning
0	RMPI-Micro Broadcast (RMPI-MB)
1	RMPI-Micro (RMPI-M)

Version_of_RMPI: This 15-bit field is used to identify the version of RMPI for future-proofing purposes. 15 bits for version to be allocated by compliance body.
Origin_of_RMPI: This 128-bit field is used to identify the entity that originated the RMPI. 128 bits to be allocated by compliance body.

Scrambling_control: This 1-bit field indicates the scrambling policy to implement (table below).

Table scrambling_control

Value	Meaning for RMPI-MB	Meaning for RMPI-M
0	Maintain original scrambling status, including no scrambling. "cipher" field: cipher used in the broadcast.	Original scrambling status has been maintained, including no scrambling. "cipher" field: cipher currently used on the content.
1	Change scrambling including replacing scrambling "cipher" field: cipher to be used to scramble the content. It is assumed that the broadcast receiver knows which scrambling algorithm is used to protect the broadcast signal (e.g. DVB CSA for DVB receivers).	The original scrambling has been changed. "cipher" field: cipher currently used on the content.

Cipher: This 4-bit field specifies the cipher algorithm used to (de)scramble the content in the TVA RMP compliant domain (table below).

Table cipher

Value	**Meaning**
0x0	No cipher.
0x1	AES
0x2	Camellia
0x3	DVB CSA 1
0x4	DVB CSA 2
0x5	3DES
0x6	M2
0x7	Scrambling / descrambling outside of the control of RMP
0x8 to 0xF	Reserved

3.4.3.2.2 Rights

Extend_rights_flag: This 1-bit field indicates whether the Extend Rights right is granted (table below).

Table extend_rights_flag

Value	**Meaning**
0	Extend Rights right is not granted.
1	Extend Rights right is granted.

Play_right_flag: This 1-bit field indicates whether the Play right is granted (table below).

Table play_right_flag

Value	Meaning
0	Play right is not granted.
1	Play right is granted.

Analogue_export_right_flag: This 1-bit field indicates whether the Analogue Export right is granted (table below).

Table analogue_export_right_flag

Value	Meaning
0	Analogue Export right is not granted.
1	Analogue Export right is granted.

Digital_export_SD_right_flag: This 1-bit field indicates whether the Digital Export SD right is granted (table below).

Table digital_export_SD_right_flag

Value	Meaning
0	Digital Export SD right is not granted.
1	Digital Export SD right is granted.

Digital_export_HD_right_flag: This 1-bit field indicates whether the Digital Export HD right is granted (table below).

Table digital_export_HD_right_flag

Value	Meaning
0	Digital Export HD right is not granted.
1	Digital Export HD right is granted.

3.4.3.2.3 Conditions and identifiers

Unless otherwise stated, conditions apply to Play, Analogue Export, Digital Export SD and Digital Export HD. If conditions are not asserted they do not apply.

Security_level: This 2-bit field indicates the minimum security level required to exercise the right. Security levels are to be defined by the compliance body.
Note: Security levels should be based upon the aggregate robustness of all invoked RMP components required to exercise the right.
Note: This condition applies to all rights, including extend rights.
Source_of_additional_rights: This 128-bit field identifies the entity from which new rights can be assigned to the content. 128-bit identifier to be allocated by compliance body.
Note: This condition only applies to Extend Rights.
Domain_ID: This 128-bit field identifies the RMP Domain to which the rights are granted. It is the first domain that has received the broadcast signal. 128-bit identifier to be allocated by compliance body.
Note: If the RMPI_type_flag is set to 0 then this field is not applicable.
Buffer_duration: This 2-bit field limits the use of a right in such a way that each frame of broadcast content is used only within a specified duration after that frame was broadcast (table below). Buffer_duration is valid only if both Time_window_start_date and Time_window_end_date are not asserted.

Table buffer_duration

Value	Meaning
00	Condition not asserted.
01	Condition not asserted.
10	Condition set, no buffer (immediate viewing)
11	Condition set, buffer duration is a reasonable period of time to be determined by compliance body (e.g. 90 minutes).

Time_window_start_date: This 16-bit field defines the start date of the window of time during which the rights are granted. It is defined as absolute start time. It is expressed in number of days since January 1st, 2004. A value of 0x0000 means that the condition is not asserted (there is no start date).
Time_window_end_date: This 16-bit field defines the end date of the window of time during which the rights are granted. It is defined as absolute expiry time. It is expressed in number of days since January 1st, 2004. A value of 0xFFFF means that the condition is not asserted (unbounded end date).
Geographic_control: This 128-bit field is used to indicate geographical regions and territories for which the rights are valid. It is to be defined by the compliance body.
Informative: It is suggested that the compliance body could use these bits for signalling up to four territories in the following format: 2 bytes ISO country code and 2 bytes region within the country. Alternatively the compliance body could decide to specify territories for which the rights are not granted. A value should be reserved for "condition not asserted".
Analogue_export_signalling: This 2-bit field is used to signal content management rules to an external analogue content protection systems (table below).

Table analogue_export_signalling

Value	Meaning
00	Condition not asserted.
01	Condition not asserted.
10	For immediate viewing only.
11	Bound to device or media for future viewing, does not preclude immediate viewing.

Analogue_SD_control: This 1-bit field constrains the resolution of the exported analogue signal (table below).

Table analogue_SD_control

Value	Meaning
0	Condition not asserted.
1	While doing analogue output Standard Definition resolution only is permitted.

Standard_Definition_digital_export_control: This 2-bit field is to control the configuration of Standard Definition digital outputs as to whether the content can be recorded or only viewed immediately (table below). This condition applies only to the Digital Export SD Right.

Table standard_definition_digital_export_control

Value	Meaning
00	Export conditions not asserted. Hand-off to any non-RMP content protection system is permitted.
01	Export conditions asserted. Hand-off to compliance body certified non-RMP content protection system only is permitted. RMPI-MB/M is mapped to certified system as defined by compliance body.
10	Export conditions asserted, bound to device or media for immediate viewing, includes immediate viewing. Hand-off to compliance body certified non-RMP content protection system only is permitted.
11	Export conditions asserted, immediate viewing only. Hand-off to compliance body certified non-RMP content protection system only is permitted.

High_Definition_digital_export_control: This 2-bit field is to control the configuration of High Definition digital outputs as to whether the content can be recorded or only viewed immediately (table below). This condition applies only to the Digital Export HD right.

Table high_definition_digital_export_control

Value	Meaning
00	Export conditions not asserted. Hand-off to any non-RMP content protection system is permitted.
01	Export conditions asserted. Hand-off to compliance body certified non-RMP content protection system only is permitted. RMPI-MB/M is mapped to certified system as defined by compliance body.
10	Export conditions asserted, bound to device or media for immediate viewing, includes immediate viewing. Hand-off to compliance body certified non-RMP content protection system only is permitted.
11	Export conditions asserted, immediate viewing only. Hand-off to compliance body certified non-RMP content protection system only is permitted.

Single_point_of_control_flag: This 1-bit field indicates that the broadcaster intends that once the content gets into the RMP Receiving Domain only one RMP entity can make usage decisions about the content based upon the expressed RMPI-MB (table below). The content is irrevocably married to the device identified as single point of control, if that device is destroyed or lost, then this grant becomes no longer exercisable. Single point of control is only used in the context of Receiving Domain as principal.

Table single_point_of_control_flag

Value	Meaning
0	Condition not asserted.
1	Single point of control applies.

Physical_proximity_flag: This 1-bit field limits the use of a right to RMP compliant devices within close physical proximity of the receiver that first received the broadcast content (table x). When a device checks that condition, it needs to be in close physical proximity of the receiving device in order to exercise the right. Precise definition of close physical proximity is to be determined by compliance body. The compliance body may decide to limit the use of this condition to live broadcasts. For instance close physical proximity could be defined as immediate vicinity e.g. content use is limited to the home network on the same local area

network and transmission over a wide area network is not permitted. Physical proximity is only used in the context of Receiving Domain as principal.

Table physical_proximity_flag

Value	Meaning
0	Condition not asserted.
1	Physical proximity applies.

Simultaneous_rendering_count: This 4-bit field limits the number of simultaneous independent Plays, Analogue Exports, Digital Export SDs and Digital Export HDs of content within a domain (table x). For purposes of this condition a Play counts as a rendering, an Analogue Export counts as a rendering, a Digital Export SD counts as a rendering, and a Digital Export HD counts as one rendering. Simultaneous rendering count is only used in the context of Receiving Domain as principal.

Table simultaneous_rendering_count

Value	Meaning
0	Condition not asserted.
1 to 15	Maximum permitted number of simultaneous renderings.

Single_point_of_control_ID: This 128-bit field identifies the entity that is the single point of control. This is triggered by the condition single point of control = 1 in the incoming RMPI-MB granted to the receiving domain. 128-bit identifier to be allocated by compliance body. This condition is only applicable if RMPI_type_flag and single_point_of_control flag are set to 1.

3.4.4 Binding of Rights Management and Protection Information

Binding of Rights Management and Protection Information is a component of the TV-Anytime Rights Management and Protection system suite of specifications. When used in conjunction with the RMPI specification as components of an end-to-end RMP system, binding ensures that RMPI is appropriately applied. TVAF RMP defines Binding as the process of creating a strong association between a given set of RMPI and the content to which it applies.
TVAF RMP defines Secure Binding as a Binding adequate to ensure that bound RMPI cannot be reassigned to unintended content without detection. Non-secure binding is binding which is not secure, and includes insufficient mechanisms to protect against tampering and/or modifications to RMPI.

3.4.4.1 Non-secure binding by transport

This binding method is only applicable to in-the-clear content. It protects against RMPI modifications, but does not protect against tampering with the binding itself.
In this method, the binding is provided by the content transport scheme: if RMPI is provided within the content transport scheme in a synchronous manner, that RMPI is considered bound to the content.
Using this method, the association of RMPI and CID is authenticated through the generation of a cryptogram that is appended to the RMPI. The cryptogram is verified to check the authenticity of the RMPI. If the verification fails, this means the RMPI has been tampered with.

3.4.4.2 Secure binding by content scrambling

This method is applicable to scrambled content. The security of this binding method depends on the use of content scrambling keys that are sufficiently unique for each binding.

This method tests for the association of the content keys with the RMPI and then tests the content with the content keys.
The content license includes RMPI, content scrambling keys or a reference to their location, the Content Identifier and a cryptogram. Content scrambling keys, when present, are encrypted. The cryptogram is computed over RMPI, content identifier and clear scrambling keys.
Upon content usage, RMPI is retrieved. If no RMPI is present, content is unusable. Otherwise, scrambling keys are first deciphered or obtained from their location and the cryptogram is verified. A verification failure means RMPI has been tampered with. If verification is successful (and applicable rights are granted in the RMPI), scrambling keys are tested to descramble the content. If the keys do not descramble the content, the binding has been tampered with. Otherwise, binding verification is successful.

3.4.4.3 Secure binding by watermark and RMPI authentication

This method applies only to in-the-clear content. In this method, the binding is provided using both cryptography and watermarking techniques. Successful use of this method depends upon the selection of watermarking technologies and cryptography, which are sufficiently robust.
Prior to distribution, content is watermarked with a Content Identifier. Then, the RMPI is bound to the content using cryptography techniques. To that end, a cryptogram (a signature or a Message Authentication Code) is computed on the RMPI and the content identifier. The cryptogram ensures secure binding of the content identifier and the RMPI. The watermarking ensures the secure binding of the content and the Content Identifier.
The content license includes RMPI, the Content Identifier and the cryptogram.
Upon content reception, RMPI is retrieved. If no RMPI is present, the verifier tries to extract the watermark from the content. If a watermark is present, binding has been tampered with. Otherwise content is viewed as non-RMP content.
If RMPI is present, the cryptogram has to be first verified in order to check the authenticity of RMPI. If the verification fails, this means the RMPI has been tampered with.
After RMPI integrity has been verified, the RMP system extracts the watermark from the content and compares it with the Content Identifier. This comparison may be a one-to-one matching or any other mapping mechanism defined by the compliance body. This makes it possible to allow a single license to apply to multiple bodies of content (e.g. an entire catalogue, series, channel, producer, subscription…). If the verification fails (including if the content is not watermarked), this means the binding has been tampered with.
In addition to the case of content transmitted in the clear, this method may also be applied to content that is initially transmitted scrambled and is eventually carried within the domain in the clear or recorded in the clear (e.g. post domain acquisition). In order to obtain secure binding, content has to be watermarked before its initial transmission. “Secure binding by content scrambling” is applied to the scrambled version of the content.
As the content is converted into the clear, the RMP system applies “secure binding by watermark and RMPI authentication”. Since the content was initially watermarked, standard secure binding verification can be performed.
Legacy devices may not be able to deal with the watermark extraction. In this case, the compliance body may allow the non-secure binding by transport verification as. This would allow both legacy devices and devices capable of processing the watermark to share the same content.

3.5 ISMA (Internet Streaming Media Alliance) DRM

The Internet Streaming Media Alliance [28] is composed of companies from the information technology, consumer electronics and media industries. Apple Computer, Cisco, IBM, Kasenna, Philips and Sun Microsystems Inc. are the founder members of the ISMA. In addition there are more than 30 other companies in the ISMA. They are jointly specifying protocols for media streaming over IP networks.

The ISMA/DRM must preserve the ISMA interoperability goals using standard encryption, authentication and integrity validation for ISMA conforming media and protocols. There are three general goals for the first release of the ISMA DRM specification according to the ISMA DRM Recommendations.

1. Ensure the "support and consistency" of ISMA 1.0 specifications when DRM is added.
2. Remove technical barriers to the dissemination of rights-managed content on platforms that run the ISMA protocols. If ISMA media and protocols are to serve as open, standard interfaces to "content protection" devices, ISMA needs to accommodate the technical protection measures (TPM) in those devices and it needs to implement the change control needed for platform licensing.
3. Identify what needs to be standardised, which bodies are developing needed standards and what needs to be invented. For example, MPEG is developing the decoder interfaces and services for DRM; the IETF, SMPTE, and OMA are developing cryptographic and key management protocols. The IETF defines cryptographic protocols for IP-network applications, particularly for the high-security needs of governments, enterprises, and individuals.

3.5.1 ISMA DRM Architecture

This section briefly reviews the ISMA DRM architecture. Figure below summarises the flow within the architecture.

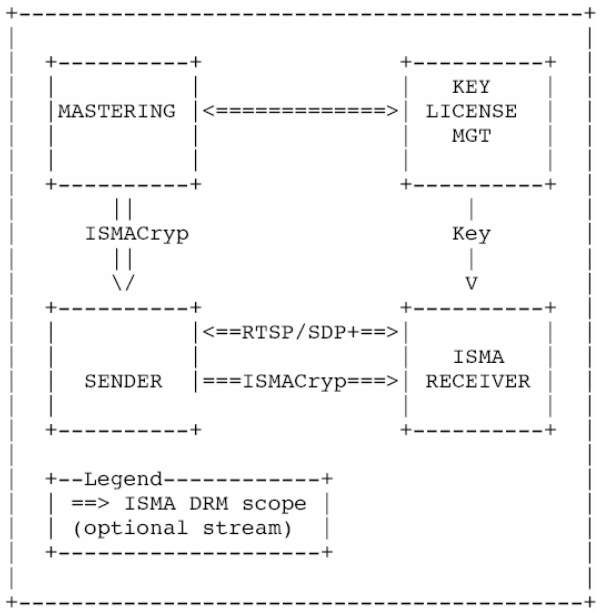


Figure ISMA DRM architecture

In previous figure, mastering is where a content work is prepared for dissemination. It may be encrypted and associated with a rights specification that is formatted according to a "rights expression language". Mastering is important to interoperability when cryptographic transforms are applied: The standard receiver needs standard cryptographic transforms for the decryption, authentication, and integrity of content works. The Mastering step may apply encryption to the mastered media work.

The Key/License MGT entity associates a rights specification and cryptographic keys with an ISMA content work. Key/License MGT translates the rights specification into a license. The license authorises particular types of access to the work, possibly according to a set of "business rules." The access may be at a highly granular level of access such as to view/hear the content, write to a DVD, or send to a friend. Key/License Management is referenced but not specified; ISMA needs to accommodate a variety of Key/License management systems, both standard and proprietary.

Although the previous figure shows Key/License MGT providing only keys to the Receiver, the Sender may obtain the key using the same elements of procedure as the Receiver. The process may be completely different on the Sender if the content is pre-encrypted at the Mastering step leaving the Sender with no need to hold the key to the content work.

The Receiver decrypts and authenticates content works contained in the media flow and may decrypt and authenticate control flows. Depending on the nature of the key management protocol in use, the Receiver may perform mutual authentication with the Key/License MGT entity to prove that the receiver is an authorised platform. This process is controlled by the license, which specifies the terms and conditions under which a key is provided to an ISMACryp device. The license determines what authenticating information is exchanged, such as information about the Receiver's hardware, software or human user. This information needs to be governed by a specification as to what can be collected and how it can be used. Exchanges with Key/License MGT need to be secured in practically all circumstances to protect the user identity and the user's content-work transactions as well as the content-work keys. The media decryption keys must also be secured, and the receiver may be a licensed content-protection platform [CPRM]. The first release of ISMA DRM supports but does not specify the interfaces, messaging, or processing of content-protection platforms.
Thus, the information assets to be protected go beyond content works; they include information related to the user's privacy and authenticating information. These assets also include resources such as the CPU, storage, service and bandwidth of the provider and the user.

3.6 Digital Media Project (DMP)

The Digital Media Project (DMP) [29] is a non-profit Association registered in Geneva, Switzerland. Its mission is to promote the successful development, deployment and use of digital media that respect the rights of creators and rights holders to exploit their works, the wish of end users to fully enjoy the benefits of digital media and the interests of value-chain players to provide products and services.

3.6.1 DMP DRM

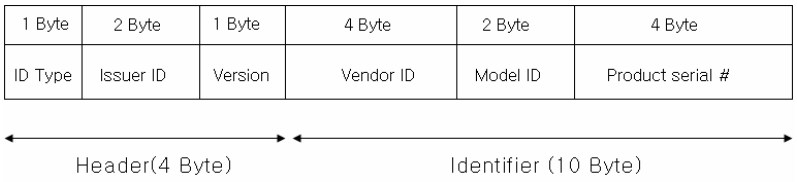
DMP has noted that DRM has the potential to substantially alter the balance that has been in existence in the analogue world between different Users of Content, in particular when one of them is the End-User. If not appropriately remedied, this imbalance may lead to a significant reduction of the scope of Traditional Rights and Usages (TRU) of Users. A possible outcome is the outright rejection of the new technology on the part of some Users, in particular End-Users perceiving the DRM media experience as inferior.
DMP is not claiming that an established TRU necessarily implies a *right* of a User to a particular Use of digital media but simply that, if Users have found a particular Use advantageous in the analogue domain, they are probably interested in continuing to exercise that Use in the digital domain as well. Leveraging upon this interest may provide opportunities for new "Digital Media Business Models" that are attractive to Users but respectful of the Rights of those who have created Works and invested in making Content.
Therefore DMP will be adding technologies to its specifications to make the exercise of TRUs technically possible. However, even a summary analysis shows that many TRUs have a legislative/regulatory impact that needs to be addressed by proper authorities. This can only be done within individual jurisdictions by determining which TRUs shall be supported in a mandatory way by the Interoperable DRM Platforms operating under their jurisdiction and which TRUs can be left to private negotiations between Users. This is a challenging task because it requires blending knowledge encompassing the legal, social and economic fields with in-depth knowledge of the highly sophisticated and unusual DRM technologies.

DMP has specified basic standard technologies [30], called Tools that are required to build Value-Chains. For ease of treatment these Tools has been grouped in categories as listed below:

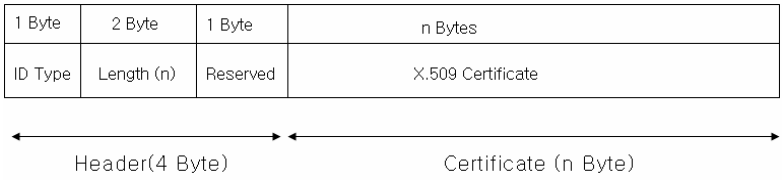
1. Represent: specifies the set of Tools used to Represent combinations of Resource Types and Metadata that constitute Content Items.
    - Content: DMP refers to this Content Representation Tool as DMP Content Information (DCI). DCI is an XML structure, based on a DMP-defined subset of the MPEG-21 Digital Item Declaration (DID) [3], MPEG-21 Digital Item Identification (DII) [4] and MPEG-21 IPMP Components [5], and extended by the DMP namespace to express DMP-specific information.

- Keys: DMP has specified the element KeyInfo is in XMLDSIG [23] in order to enable the recipient(s) to obtain the key needed to validate digital signatures. KeyInfo may contain keys, names, certificates and other public key management information, such as in-band key distribution or key agreement data. The XMLDSIG specification defines a few simple types but applications may extend those types or altogether replace them with their own key identification and exchange semantics using the XML namespace facility. However, questions of trust of such key information (e.g., its authenticity or strength) are out of scope of the XMLDSIG specification and left to the application.
- Rights Expressions: Specifies the Tool to Express Rights associated with Content that in turn map onto specific End-User Device behaviour consistent with the semantics of the Rights Expressions. It does not cover the expression of commercial offers or of details of financial transactions between the Service Provider and the End User.

2. Identify:
   - Content: The Content Identifier satisfies the characteristics defined in RFC 1737 [31], which is known as URN (Uniform Resource Names) scheme. Therefore identifiers that conform to URN schemes can be used to identify Content. Currently, there are several registered URN schemes such as ISBN and ISSN, each of them serving a specific purpose and having a unique namespace under IANA (Internet Assigned Numbers Authority).
   - License: License identification is performed as content identification, as a license can be represented as a DCI.
   - Device: Device identifier is mainly used for device authentication. There can be two kinds of device identification:
     - Device info-based identification: the identifier is generated only based on the device information by the device identification server run by the Registration Agency. Figure below shows the identifier format of device info based identification.



     - Certificate-based identification: in which a X.509 certificate is utilised for device identifier. Figure below shows the identifier format for the certificate-based identification.



   - Domain: The allocation of Domain Identifiers is carried out by Domain Registration Agencies, which are appointed by the Domain Registration Authority. The format of the Domain ID is:

     <element name = "Domain_ID " type = "r:Keyholder"/>

     As a Domain is typically utilised by a group of Users it is often beneficial to be able to Identify sub-Domains within a given Domain, where each sub-Domain corresponds to a member of the group. The creation of a sub-Domain is achieved in the same way as the original Domain was established, this time generating a sub-Domain ID. The sub-Domain ID can be included in a Content License as representing the target of the Content in the same way as the Domain or Device ID. Multiple sub-Domains may appear within a Content License. Format of Sub-Domain ID is:

<element name="SubDomain_ID" type="anyURI"/>

3. Package
    - Content: DMP provides Tools to Package Content in files whose format using a DMP-defined subset of the MPEG-21 File Format [10], which contains the DCI with some or all of its ancillary Resources, potentially in a single package. The MPEG-21 File Format is based on the ISO Base Media File Format, which defines how to contain timed media information for a presentation. The file structure is object-oriented; a file can be decomposed into constituent objects very simply, and the structure of the objects inferred directly from their type. Files are formed as a series of objects, called boxes. All data is contained in boxes; there is no other data within the file. Each Box is characterised by two attributes: boxtype and size.
4. Authenticate
    - Device: DMP defines three different types of Device Authentication, which are closely related with the Identification part of this Approved Document. This section will provide means to Authenticate Devices for the three classes of Device Identification.
        - Devices having unique certificates
        - Devices that are uniquely identified by data
        - Devices without a unique data with certificate proxy
5. Manage
    - Domains: DMP specifies the Domain Management Protocols. The functionality of these protocols includes:
        - Setting up a Device Domain Context
        - Controlling the Use of Content within the Domain.
        - Managing Device Domain membership – joining and leaving
6. Access
    - Content: DMP specifies the Protocol to Access a Content Item with a License Bundled within the Content and bound to a specific Device and/or Domain. The Remote Content Access Protocol (RCAP) is used by an eXternal Device (XD) connected to a PAV Device to obtain a Content Item with a License Bundled within, granting the Use of this Content Item to that PAV Device or to a Domain. This protocol is based on the exchange of messages between two basic components: the XD and the Content Provider.
    - License: DMP specifies two Protocols:
        - Remote License Access Protocol (RLAP) employed when an external device (XD) connected to a PAV Device Accesses a License from a License Provider;
        - Local License Access Protocol (LLAP) employed when a PAV Device Accesses a License Bundled within a Content Item.
    - Update/Upgrade License:
7. Process
    - Binarise XML
    - Encrypt/Decrypt

3.7 MI3P Project

MI3P (Music Industry Integrated Identifier) [32] was initiated to develop a global infrastructure to support the management of on-line music e-Commerce. The goal of the project is the development of an integrated identification and description system (the MI3P Framework), which enables all parties in the electronic music industry value chain to interoperate within an automated electronic trading environment. The project has defined the requirements of the music industry and is close to finalisation of a number of Standards, which will enable this integrated information management approach. The Standards under development are:

- The **Global Release Identifier Standard** (GRid), which is to be assigned to, releases which can contain one or more sound recordings and music videos together with other multimedia resources.
- The **Musical Work License Identifier Standard** (MWLI), which is to be assigned to licences in respect of the musical works embodied in the sound recordings and music videos contained in releases.

- Three **MI3P Message Suite Standards** are being designed to enable record companies, music rights societies, music service providers and other business partners to efficiently exchange information about releases, sound recordings, musical works and licences for the automated management of music e-Commerce.
- The **MI3P Data Dictionary Standard**, which provides the methodology for developing and maintaining a common vocabulary for the messages being developed under the auspices of MI3P. This vocabulary will be used by music industry value chain participants to integrate their own systems into the MI3P Framework.

MI3P was commissioned in late 2000 by the Recording Industry Association of America (RIAA), the International Federation of the Phonographic Industry (IFPI) the Confédération Internationale des Sociétés d'Auteurs et Compositeurs (CISAC) and the Bureau International des Sociétés Gérant les Droits d'Enregistrement et de Reproduction Mécanique (BIEM).

3.7.1 MI3P Data Dictionary Standard

The MI3P Data Dictionary [33] provides the canonical definition of all Elements to be used in all MI3P Message Standards and other MI3P Framework Components. This Standard also specifies how the MI3P Data Dictionary is created and maintained (including how new Elements are added to the MI3P Data Dictionary) by specifying the requirements for an MI3P Data Dictionary Registration Authority.
The purpose of the MI3P Data Dictionary is:

- To support the consistent and efficient development, use and understanding of MI3P Messages Standards and other MI3P Framework Components
- To prevent ambiguity in the meaning of terms used in the MI3P Framework
- To enable the effective mapping of Elements and MI3P Framework Components to other metadata standards

An *Element* is a term in the MI3P Data Dictionary. *Element* is also the top-level term in the MI3P Data Dictionary, to which all other Elements are related.
The Core Elements of the Dictionary are depicted in table below. Further Elements may be added at any time following the procedures laid down in this Standard.

Table Core elements

Headword	**Description**
Element	A data element
ComponentElement	A part of a Composite.
Context	An intersection of Time and Place in which something may happen (an Act) or exist (a State).
Event	A Context in which some act happens
State	A Context in which some Resource or Party exists in an unchanging state
State	A geographical or virtual location.
GeographicalPlace	A Place, which may be defined by spatial co-ordinates.
VirtualPlace	A non-Geographical location, such as an Internet address or a telephone number.
Composite	A group of two or more entities combined for any purpose.
Time	A point or period of linear time. In MI3P, Times (including Dates) are expressed in an ISO 8601:2004 compliant format.
Date	Date A Date represented as a Calendar Year, Month or Day (in ISO 8601 format: YYYY, YYYY-MM or YYYY-MM-DD).
DateTime	A Time represented by a Date and a Time within that Date (in ISO 8601 format: YYYY-MMDDThh:mm:ss)
Period	A Time between two other Times. Periods in MI3P are always described using the Mi3pC:Period Composite or one of its derivatives.
PeriodEnd	A Time that marks the end of a period of time
PeriodStart	A Time that marks the beginning of a period of time

TimeOfDay	A Time in a day (in ISO 8601 format: hh:mm:ss)
Resource	Something which plays a role in a Context but is not a Time or a Place
Category	A type, quality or measurement of another entity.
Creation	An entity that is made, directly or indirectly, by one or more human beings
Descriptor	A textual attribute of another entity, which may function as a Name or Annotation or both.
Party	A human or other animal being (real or imaginary), a legal person or an organisation capable of playing a role as an agent in an Event.
Relator	An entity that describes the relationship between two other entities
Set	A set of one or more entities.

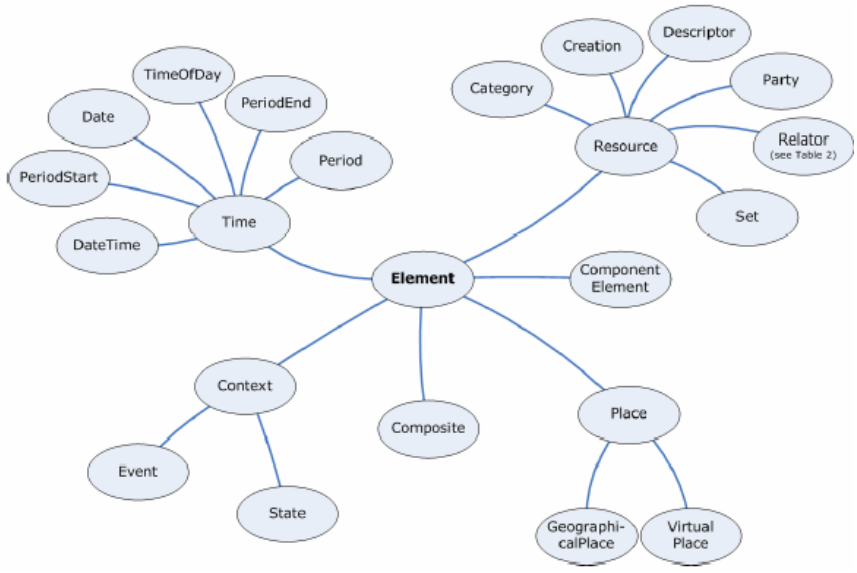


Figure Core elements relationship

Semantically, all Elements belong to one of the following basic types:

- Simple Elements: Element in the MI3P Data Dictionary which has a simple value or is itself a simple value when used in an MI3P Message Standard or other Framework Component
- Composites: A Composite is a group of two or more Elements combined for any purpose.

Elements are related to one another, hierarchically and in other ways, so that the MI3P Data Dictionary is a structured "ontology". Elements depend on other Elements for the inheritance and specialisation of meaning. The relationships between Elements are defined by the use of Relators, which are themselves defined as Elements within the MI3P Data Dictionary.

The syntax of the Elements contained in the MI3P Data Dictionary will be represented in one or more XML schema files – collectively called the MI3P Baseline Schema – for use by various MI3P Messaging Standard and other MI3P Framework Components. A Registration Authority (RA) shall be established for creating and maintaining the Schema files. This RA shall be the same RA as for the MI3P Data Dictionary.

3.7.2 European Licensing Message Suite (ELMS)

The suite of messages contained in this Standard [34] provide a technical infrastructure that can be used for the communication of Musical Work, Sound Recording and Release-related information between music

industry value chain participants in Europe, primarily to enable the efficient management of the licensing of Musical Works in the context of on-line distribution.
This Standard includes six principal messages (plus a set of four auxiliary messages for updates).

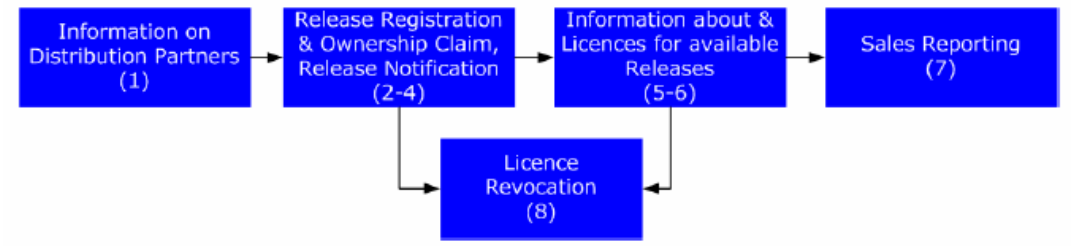


Figure Overall choreography within the European Licensing Message Suite

Next table shows all the messages in the European Licensing Message Suite.

Table Messages in the European Licensing Message Suite

Message Name	Initiating Event	Sender	Recipient
NewDistribution-PartnerMessage (1a)	A Release Creator has acquired a new Distribution Partner and provides this information to its Musical Work Licensor who may want to have a direct relationship with the Distribution Partner.	Release Creator (typically a record company)	Musical Work Licensor (typically a music rights society)
DistributionPartner-UpdateMessage (1b)	Some details of a relationship change and need to be sent	Release Creator	Musical Work Licensor
ReleaseRegistration-Message (2a)	A Release Creator and/or a Distribution Partner wants to release sound or music video recordings in a Release and informs a Musical Work Licensor about the Release and the sound and/or music video recordings contained in it. The message also allows the exchange of information on other assets.	Release Creator and/or a Distribution Partner (typically a DSP)	Musical Work Licensor
ReleaseRegistration-UpdateMessage (2b)	The Release Creator and/or Distribution Partner have additional information about the sound recordings and/or music video recordings embodied in a Release and inform the Musical Work Licensor about this.	Release Creator and/or a Distribution Partner	Musical Work Licensor
ReleaseRegistration-WithdrawalMessage (2c)	The Release is to be withdrawn	Release Creator and/or a Distribution Partner	Musical Work Licensor
OwnershipClaimMessage (3)	After a Musical Work Licensor receives a Release registration (or an update thereto), it matches it against its sound recording and musical work data and informs the Release Creator and/or Distribution Partner about its ownership claims and available exploitation rights.	Musical Work Licensor	Release Creator and/or a Distribution Partner
ERN (4)			
ReleaseAvailability-Message	A Release Creator and/or a Distribution Partner informs a Musical Work Licensor	Release Creator and/or	Musical Work Licensor

(5a)	that a specific Release is now available through a specific Distribution Partner	a Distribution Partner	
ReleaseAvailability-UpdatedMessage (5b)	The Release Creator and/or a Distribution Partner inform the appropriate Musical Work Licensor about changes to the availability of a specific Release through its Distribution Partners(s). The message is also used by a Release Creator and/or a Distribution Partner to inform a Musical Work Licensee that a Release is no longer available from a Distribution Partner or is no longer available for a specific use.	Release Creator and/or a Distribution Partner	Musical Work Licensor
DistributionLicense-Message (6)	The Musical Work Licensor issues a Distribution Partner a Musical Work licence (either a blanket licence or a licence for a specific Release) and sends appropriate information to the Distribution Partner. The syntax for this message is the same as for the Ownership Claim message.	Musical Work Licensor (typically a music rights society)	Distribution Partner (typically an DSP)
DSR (7)			
MusicalWorkLicense-RevocationMessage (8)	A Musical Work licence is to be withdrawn	Musical Work Licensor (typically a music rights society)	Distribution Partner (typically an DSP)

Colour coding for the messages:

- Blue – indicates information that is sent in the first message of the cycle (i.e. Release Registration and Availability of a Release respectively). This information is in many cases repeated in the second message of the cycle; European Licensing Message Suite Final Draft Standard (MI3P-ELMS-10-FDS)
- Red – indicates information that is returned in the second message of the cycle (i.e. Ownership Claim and Distribution Partner Licence respectively);
- Green – indicates information that is provided in the first message and significantly updated in the return message. This is not to say that blue information may not be corrected in the response message, however green coloured elements are substantially edited and enhanced backing the return message;
- The curved black arrows depict internal references from one element of a message (a MWLI) to a different part of the message (licence details of the licence identified with a MWLI)).

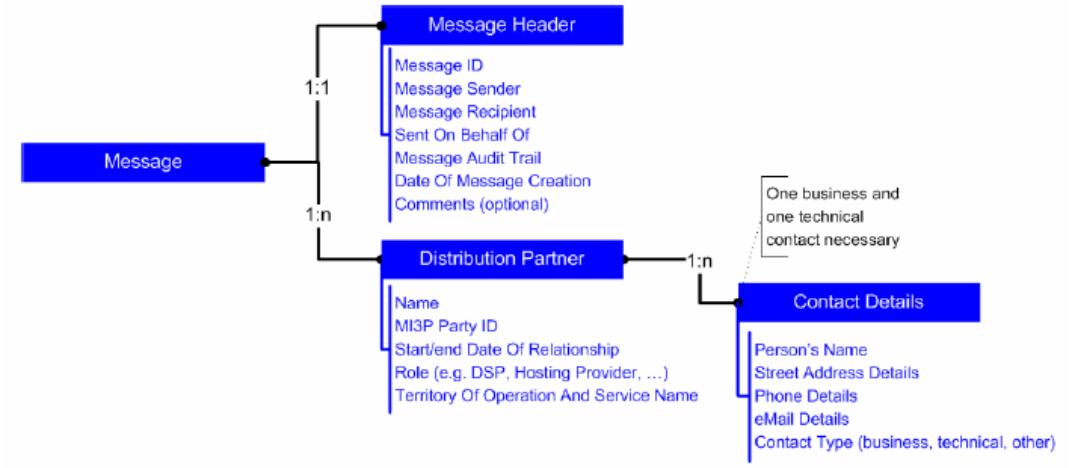


Figure Information Content: Distribution Partner Information Messages

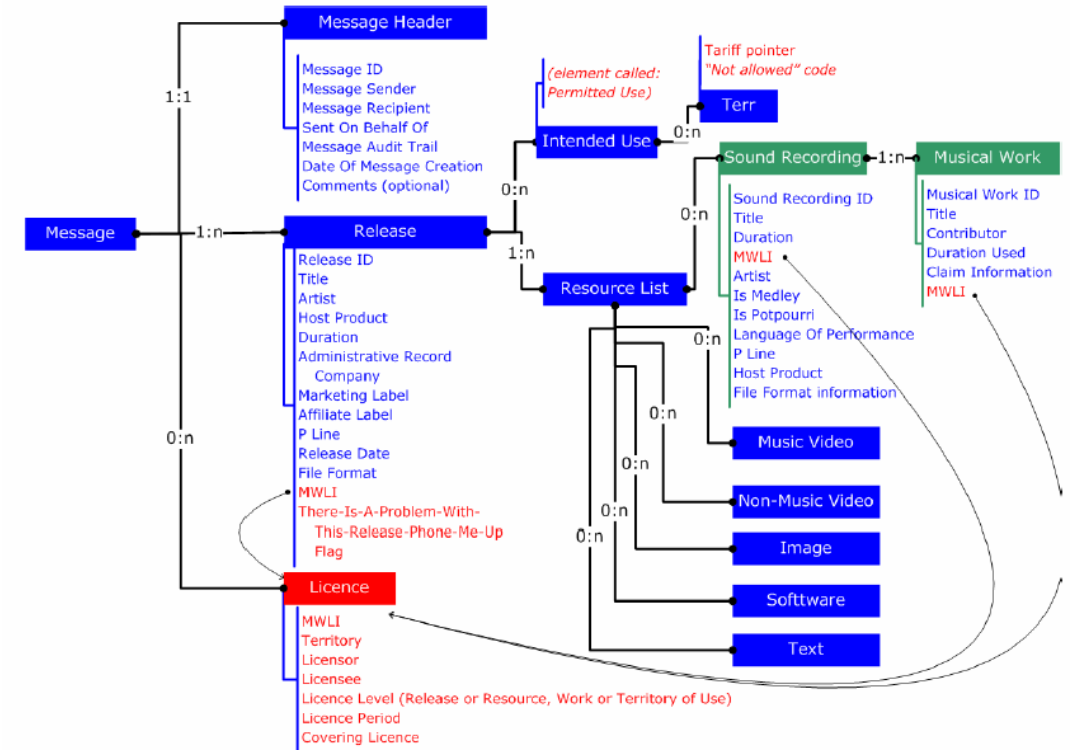


Figure Information content: Release Registration cycle

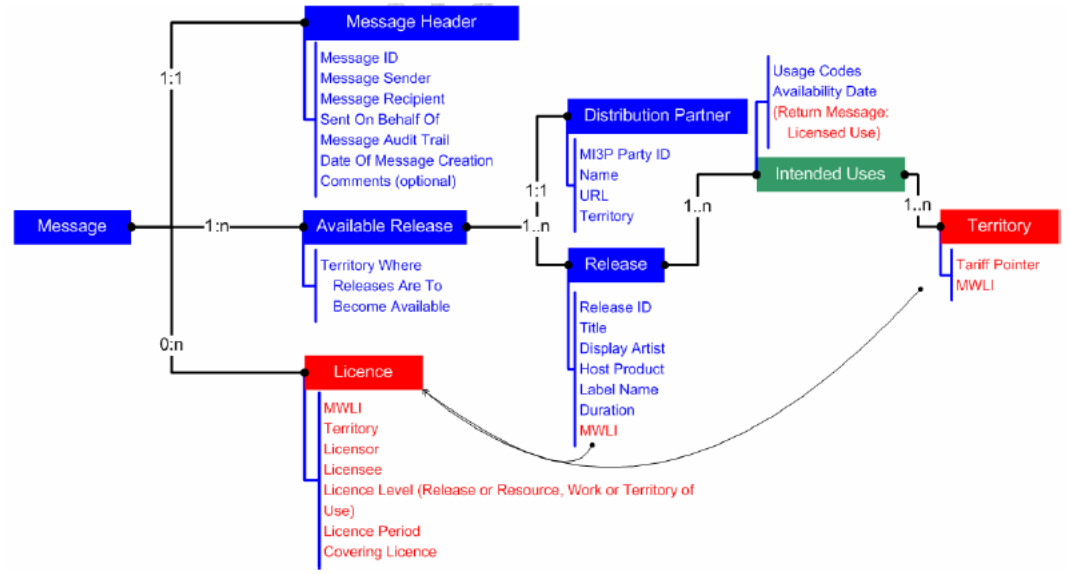


Figure Information content: Release Availability cycle

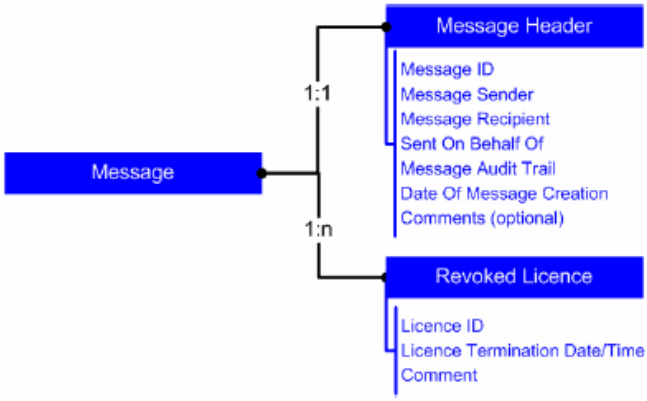


Figure Information content: Licence Revocation

3.7.3 Digital Sales Report Message Suite (DSRM)

The suite of messages contained in this Standard [35] provides a mechanism for Licensees (typically Digital Service Providers) to report to Licensors (typically Music Rights Societies and/or Record Companies) Sales (as defined in Clause 4.1.5) of Products and/or to report information regarding the revenue generated from Selling Products based on electronic Releases containing Sound Recordings and/or Music Audio-Visual Recordings which embody Musical Works and/or other Resources.

The Message Suite comprises two messages:

- SalesReportToRecordCompanyMessage, a sales reporting Message in the DSR Message Suite sent to a MusicalWorkLicensor; and
- SalesReportToSocietyMessage, a sales reporting Message in the DSR Message Suite sent to a RecordCompany

The two messages in this Digital Sales Reporting Message Suite contain similar information as depicted below in Figure below. The differences lie mostly in additional information provided in the SalesReportToSocietyMessage message. The main differences are highlighted in red in the diagram below.

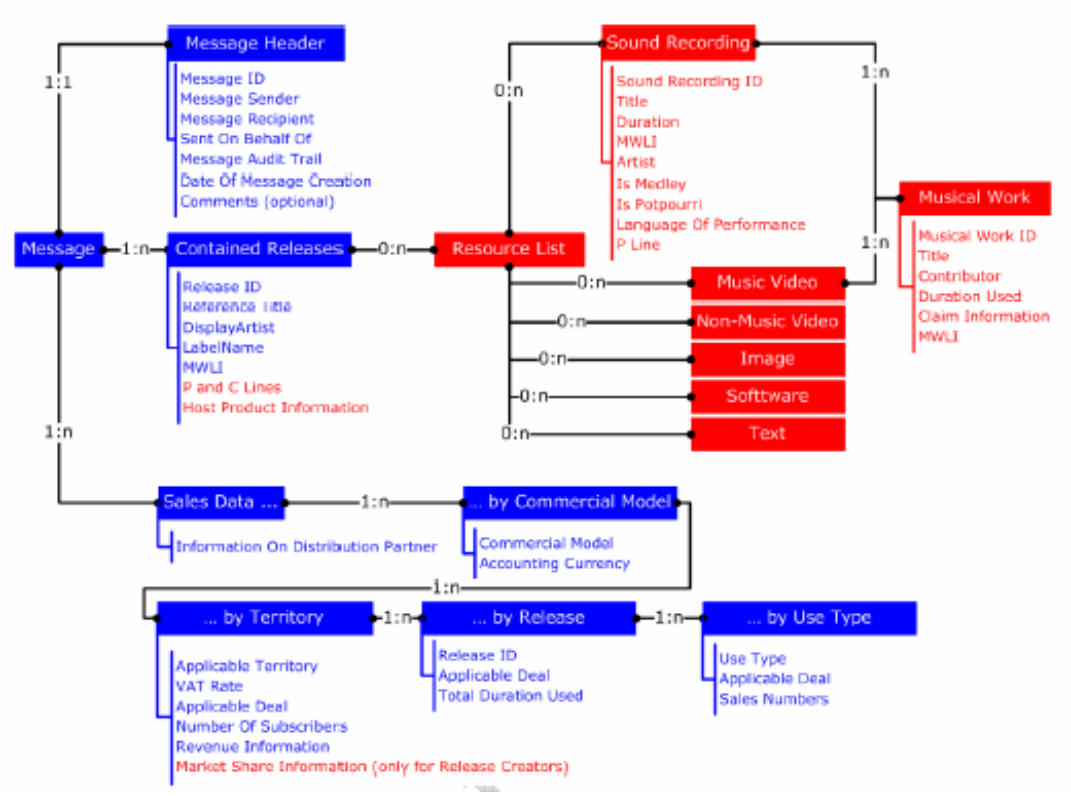


Figure Information content in the Messages within the Digital Sales Reporting Message Standard

3.7.4 Electronic Release Notification Message Suite (ERNM)

The suite of messages contained in this Standard [36] provides a mechanism for Release Providers (usually record companies) to inform their Distribution Partners (such as Digital Service Providers (DSPs) and Mobile Service Providers (MSPs)) about Releases that can to be made available to the public as electronic Products. The messages will allow such standardised information flow about the Releases themselves (i.e. Release metadata) as well as information about the commercial terms under which such Releases can be made available.

Figure below shows the choreography of processes that the Electronic Release Notification Message Suite enables.

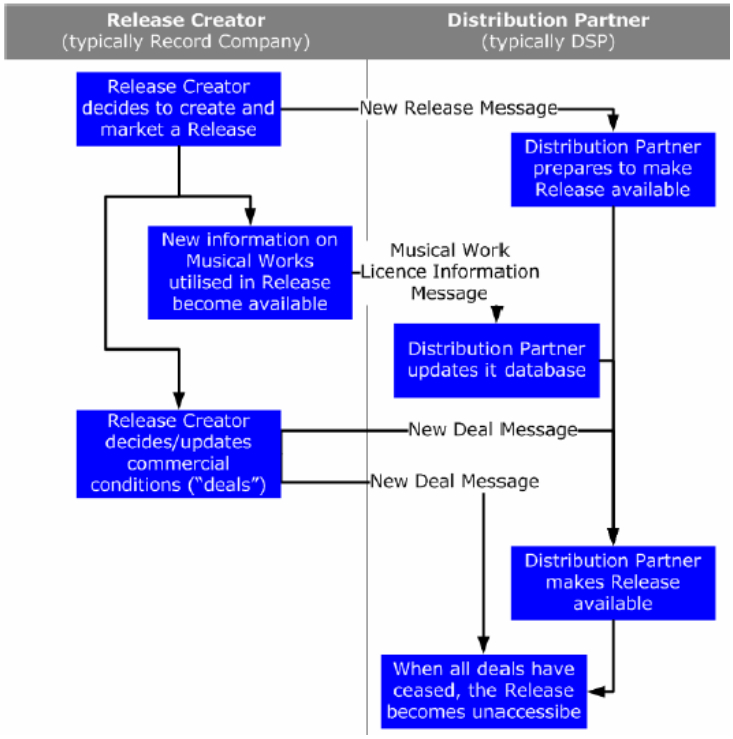


Figure Choreography of the Electronic Release Notification Message Suite

Table Messages in the Electronic Release Notification Message Suite

Message Name	Initiating Event	Sender	Recipient
NewReleaseMessage	The Release Provider decides to take a Release to the market and collates all necessary information about the Release. This does not necessarily include information about the commercial conditions under which the Release may be made available.	Release Creator, typically a record company	Distribution Partner, typically a DSP
NewDealMessage	The Release Provider has decided on the commercial conditions under which the Release may be made available.	Release Creator, typically a record company	Distribution Partner, typically a DSP
MusicalWorkLicense-InformationMessage	After sending a NewRelease-Message to the Distribution Partner additional information, especially on the Musical Work utilised in the Release, become available to the Release Provider.	Release Creator, typically a record company	Distribution Partner, typically a DSP

Figures below show information elements of the previous presented messages.

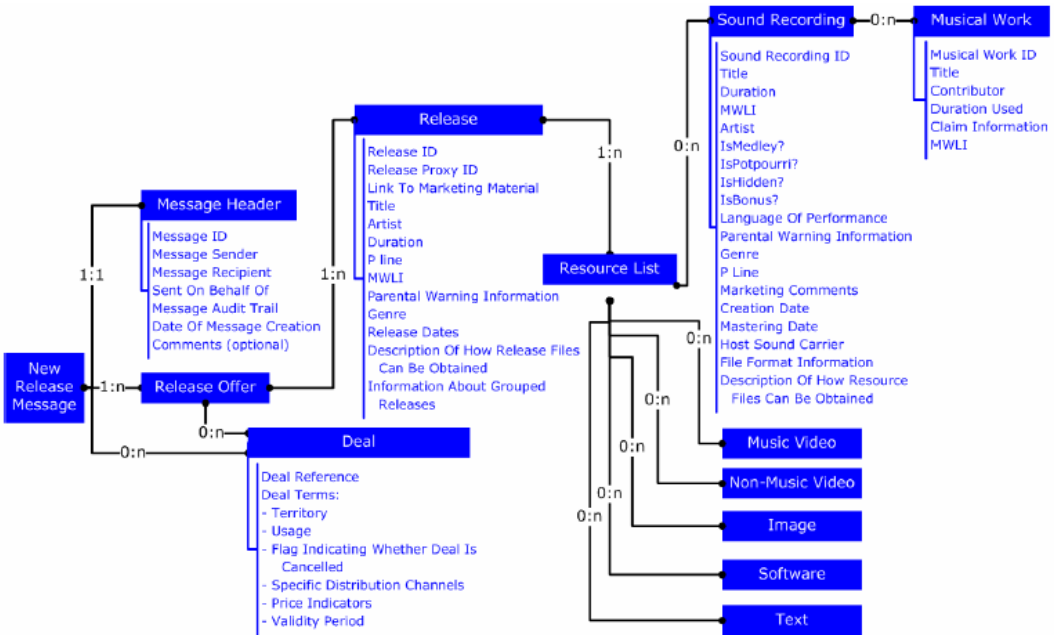


Figure Information content in the NewReleaseMessage

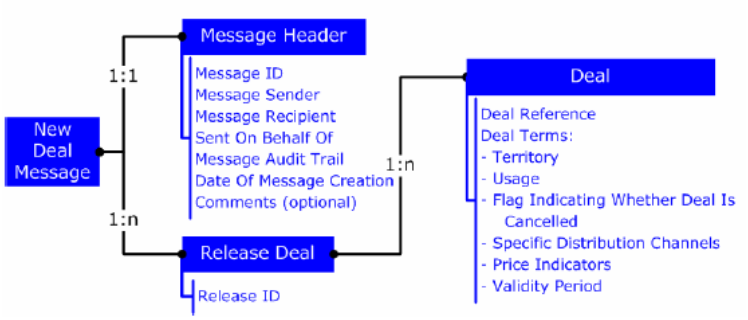


Figure Information content in the NewDealMessage

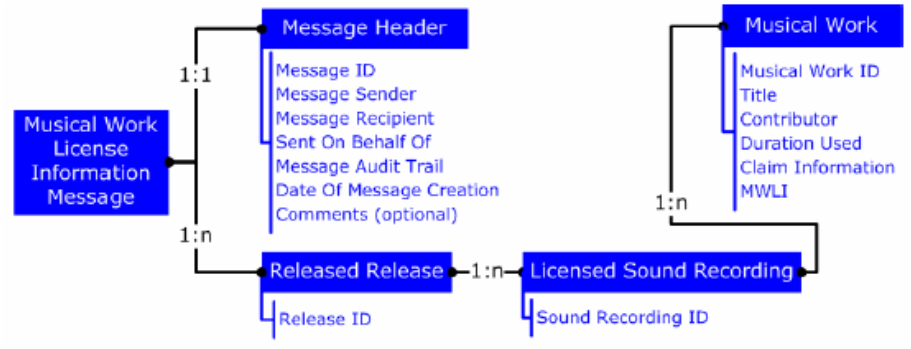


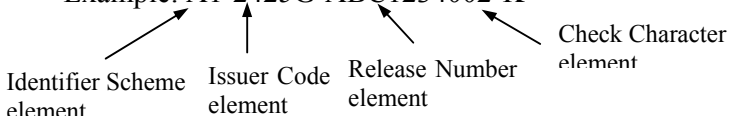
Figure Information content in the MusicalWorkLicenseInformationMessage

3.7.5 Global Release Identifier (GRid)

This Standard [37] specifies a means of uniquely identifying a "Release". It standardises and promotes internationally the use of a standard identification code so that Releases can be unambiguously distinguished from one another within computer databases and in related documentation and electronic messages, to support the efficient administration of all types of information about Releases and communication about Releases between record labels and their business partners.
The Global Release Identifier (GRid) identifies Releases as abstract entities representing bundles of one or more Digital Resources compiled for the purpose of electronic distribution.

A GRid consists of 18 characters, made up of an Identifier Scheme element followed by an Issuer Code element, a Release Number element and a Check Character as follows:

- Identifier Scheme element (2 characters)
- Issuer Code element (5 characters)
- Release Number element (10 characters)
- Check Character element (1 character)



Unless it is clear from its context of use that the identifier is a GRid, a GRid should always be presented in the following format:

MI3P:A1-2425G-ABC1234002-K

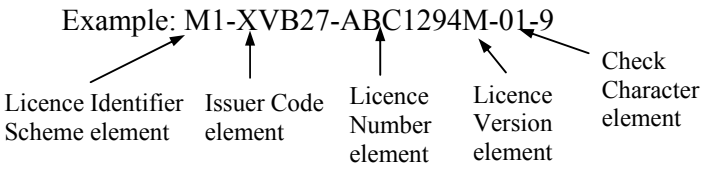
3.7.6 Musical Work Licence Identifier (MWLI)

The MWLI [38] provides an efficient means of identifying Licences in computer databases, in related documentation and in electronic messages for the exchange of information between music rights societies, music publishers, record companies, electronic retailers of music and other interested parties on an international basis.

An MWLI consists of 18 characters, made up of an Identifier Scheme element followed by an Issuer Code element, a Licence Number element, a Licence Version element and a Check Character as follows:

- Licence Identifier Scheme element (2 characters): distinguishes the MWLI Scheme from any other Standard identification scheme within the MI3P domain which adopts the same or a similar structure; it also identifies different Licence Types. It shall be composed of two Valid Characters. All MWLI Licence Identifier Scheme Elements shall take the form "Mx" where "x" is a Valid Character. The MWLI shall initially use three different Licence Identifier Scheme Elements, to identify the following different types of Licence:
    - M1 for a Licence governing a specified set of Usages by a specified Licensee of all or of a specified subset of the Musical Works that are represented by the Licensor

  - M2 for a Licence governing the mechanical reproduction by a specified Licensee of a specified Musical Work or Musical Works that are represented by the Licensor, in a The Licence Identifier Scheme element single sound recording
  - M3 for a Licence governing the Usage by a specified Licensee of a set of Musical Works that are represented by the Licensor in a specific Release or in a set of Releases.
- Issuer Code element (5 characters): identifies the Issuer of the MWLI.
- Licence Number element (8 characters): uniquely identifies the specific Licence to which the Issuer wishes to assign a unique identity.
- Licence Version element (2 characters): uniquely identifies a Licence Version. The first issue of a Licence shall always be identified with the Version Element "01"; subsequent versions of the same Licence shall be identified by incrementing the Licence Version Element, from 02 to 99, and then in the range of AA…AZ, BA, … ZZ. The value "00" is invalid.
- Check Character element (1 character): is a calculated value for each MWLI to ensure that it has not been corrupted. It shall be calculated in accordance with ISO 7064 Mod 37, 36 part of ISO 7064:1983.



3.8 Creative Commons

3.8.1 Introduction

Creative Commons [39], an initiative launched in the beginning of 2003. A non-profit organisation founded on the notion that some people would prefer to share their creative works (and power to copy, modify, distribute works) instead of exercising all of the restrictions of copyright law. It offers a flexible solution that situates itself between traditional copyright and the strict open source and open content licenses. It allows rights owners to specify that their content is "Some Rights Reserved", not "All Rights Reserved". Users can choose and combine a custom-made license, based on four fundamental choices. Should the work always be attributed to its original maker? Can the work be reused for commercial purposes? Are derivatives allowed or should the work be reproduced in its original form? Should the work be reproduced under the same conditions?

Creative Commons legal solidness, flexibility and simplicity, combined with the wide exposure it received, makes it a promising new initiative - many agree that more flexibility is needed in order to bring the current, disproportioned copyright system back to a realistic framework.

Creative Commons main goals are to provide an easy way to announce that works are available and an easy way for people to find such works that are in the public domain or licensed on generous terms

3.8.2 Creative Commons licenses

Creative Commons first project, in December 2002, was the release of a set of copyright licenses free for public use. Taking inspiration in part from the Free Software Foundation's GNU General Public License (GNU GPL), Creative Commons has developed a Web application that helps people dedicate their creative works to the public domain — or retain their copyright while licensing them as free for certain uses, on certain conditions. Unlike the GNU GPL, Creative Commons licenses are not designed for software, but

rather for other kinds of creative works: websites, scholarship, music, film, photography, literature, courseware, etc.
They hope to build upon and complement the work of others who have created public licenses for a variety of creative works. Their aim is not only to increase the sum of raw source material online, but also to make access to that material cheaper and easier. To this end, they have also developed metadata that can be used to associate creative works with their public domain or license status in a machine-readable way. They hope this will enable people to use their search application and other online applications to find, for example, photographs that are free to use provided that the original photographer is credited, or songs that may be copied, distributed, or sampled with no restrictions whatsoever. They hope that the ease of use fostered by machine- readable licenses will further reduce barriers to creativity.
Creative Commons offer to work creators the possibility offer their work using CC licenses without giving up their copyright. It means offering some of creators' rights to any taker, and only on certain conditions.
The different licenses offered by Creative Commons are:

- Attribution. You let others copy, distribute, display, and perform your copyrighted work — and derivative works based upon it — but only if they give you credit.
- Non commercial. You let others copy, distribute, display, and perform your work — and derivative works based upon it — but for non can commercial purposes only.
- No Derivative Works. You let others copy, distribute, display, and perform only verbatim copies of your work, not derivative works based upon it.
- Share Alike. You allow others to distribute derivative works only under a license identical to the license that governs your work.

Creative Commons Metadata files have two major parts: a work description, and a license description. The work description uses Dublin Core properties to provide information about the work. Here are the properties that are used:

- dc:title: A title or name for the resource.
- dc:description: A text description of the resource.
- dc:subject: Key words and phrases describing the topic of the resource.
- dc:publisher: A cc:Agent responsible for making the resource available.
- dc:creator: A cc:Agent who created the resource.
- dc:contributor: A cc:Agent who contributed to the creation of the resource.
- dc:rights: A cc:Agent who holds the copyright on the resource.
- dc:date: A copyright date for the resource.
- dc:format: The Media Type of the resource.
- dc:type: The DCMI Type (schema) of the resource.
- dc:source: A Work that the resource was derived from.
- cc:derivativeWork: A Work that was derived from the resource.
- cc:license: A copyright license for the resource, a structured cc:License. If there are two cc:licenses, then the licensee gets to pick which to use.

Licenses are described by their characteristics, which come in three types:

- Permissions (rights granted by the license)
    - Reproduction: the work may be reproduced
    - Distribution: the work (and, if authorised, derivative works) may be distributed, publicly displayed, and publicly performed
    - DerivativeWorks: derivative works may be created and reproduced
- Prohibitions (things prohibited by the license)
    - CommercialUse: rights may be exercised for commercial purposes
- Requirements (restrictions imposed by the license)
    - Notice: copyright and license notices must be kept intact
    - Attribution: credit must be given to copyright holder and/or author
    - ShareAlike: derivative works must be licensed under the same terms as the original work
    - SourceCode: source code (the preferred form for making modifications) must be provided for all derivative works

Example of what a full file will look like:

```
<rdf:RDF xmlns="http://web.resource.org/cc/"
  xmlns:dc="http://purl.org/dc/elements/1.1/"
  xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#">
<Work rdf:about="http://example.org/gnomophone.mp3">
 <dc:title>Compilers in the Key of C</dc:title>
 <dc:description>A lovely classical work on compiling code.</dc:description>
 <dc:creator>
   <Agent>
    <dc:title>Yo-Yo Dyne</dc:title>
   </Agent>
 </dc:creator>
 <dc:rights>
   <Agent>
   <dc:title>Gnomophone</dc:title>
   </Agent>
 </dc:rights>
 <dc:date>1842</dc:date>
 <dc:format>audio/mpeg</dc:format>
 <dc:type rdf:resource="http://purl.org/dc/dcmitype/Sound" />
 <dc:source rdf:resource="http://example.net/gnomovision.mov" />
 <license rdf:resource="http://creativecommons.org/licenses/by-nc-nd/2.0/" />
 <license rdf:resource="http://www.eff.org/IP/Open_licenses/eff_oal.html" />
</Work>

<License rdf:about="http://creativecommons.org/licenses/by-nc-nd/2.0/">
 <permits rdf:resource="http://web.resource.org/cc/Reproduction" />
 <permits rdf:resource="http://web.resource.org/cc/Distribution" />
 <requires rdf:resource="http://web.resource.org/cc/Notice" />
 <requires rdf:resource="http://web.resource.org/cc/Attribution" />
 <prohibits rdf:resource="http://web.resource.org/cc/CommercialUse" />
</License>
</rdf:RDF>
```

3.9 Real Networks DRM

3.9.1 Introduction

In 1995, RealNetworks, Inc. [40] pioneered the entire Internet media industry, and continues to fuel its exponential growth. Because the Internet was built to handle text-based information, not audio and video and other rich media, RealNetworks, Inc. foresaw the need for specific solutions that could handle the creation, delivery and consumption of media via the Internet. That led RealNetworks, Inc. to invent and release the RealPlayer and RealAudio in 1995.

RealNetworks, Inc. develops end-to-end solutions that allow everyone — from Fortune 500 companies with locations worldwide to individuals at their desktops or other Internet-enabled devices — to create, send and receive audio, video and other multimedia services over the Internet. With the introduction of the Helix Initiative and the Helix Servers and RealProducer product families from RealNetworks, Inc., they continue to lead the way in delivering the highest quality Internet media experience delivering any media format, from any point of origin, across any network transport, running any OS to any person on any Internet-enabled device anywhere in the world.

Helix DRM [41] replaces the company's Media Commerce Suite (MCS) [42], which provided DRM only for RealAudio and RealVideo formats, and is part of RealNetworks ambitious open-source push for adoption among content producers and consumer electronics manufacturers

3.9.2 Helix DRM 10

Helix DRM is the first multiformat digital rights management platform for secure delivery of media to any device. It is a comprehensive and flexible platform for the secure media content delivery of standards-based as well as leading Internet formats, including RealAudio, RealVideo, MP3, MPEG-4*, AAC*, H.263 and AMR*. Helix DRM makes it possible to deliver these formats not only to PCs but also to a wide array of non-PC devices, including mobile devices and home appliances.

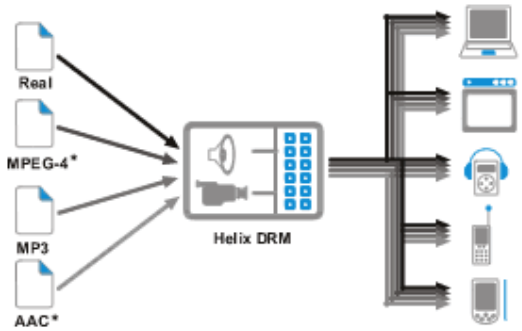


Figure x. Helix DRM overview

Helix DRM includes a set of products and services enabling business models through secure rights managed distribution of movies, music and other digital content to millions of media player users worldwide.
It empowers rights holders to create a range of robust business models for distributing rich media to the broadest worldwide audience, and will create many new ways for consumers to access and enjoy digital media.
Helix DRM provides secure media packaging, license generation and high-quality content delivery to a trusted media player base across all major platforms to multiple devices. It extends the RealPlayer and Helix Platform open architecture to accommodate the incorporation of a wide range of rights management systems. It easily integrates into all types of existing infrastructures and back-end systems, supporting a broad set of business models including purchase, rental, video on-demand, and subscription services.

Consumers want to access their favourite audio and video content via the Internet and play it on a variety of home and mobile devices. Content owners want to meet this demand in a way that protects their copyrighted material. Until now, that has required them to use a different digital rights management (DRM) system for each major format they want to support, or to avoid making their content available at all for certain devices.

Helix DRM is a complete, end-to-end secure digital delivery platform that is comprised of four major components Helix DRM Packager, Helix DRM License Server, Helix DRM Client and Helix DRM Device Support.

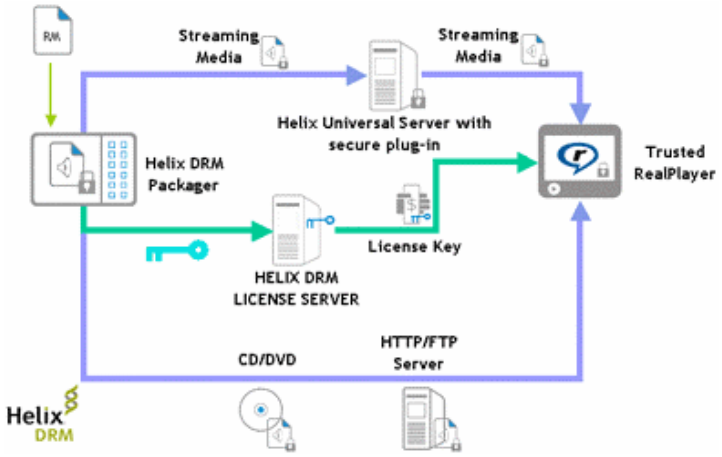


Figure x. Helix DRM

3.9.3 Helix DRM Features

3.9.3.1 General features

Helix DRM general features are:

- The content is separate from the rights. This means content owners can change the business rules associated with the content without re-encoding or re-packaging.
- Supports multiple usage rights: Content owners have the ability to issue licenses for playback of a specific duration, playback during a specific window of time, and to limit the number of plays for each media file distributed.
- Supports multiple business models: such as rental, subscription services, content syndication, content transaction and promotion, pay-per-view and video on demand.
- Supports multiple content delivery modes: Secure content can be distributed content via streaming (live or on-demand), downloads, physical media or peer-to-peer file sharing networks.

3.9.3.2 Back-end system interoperability

Helix DRM was built to integrate with existing systems such as clearinghouses, payment systems, retail storefronts, databases, customer relationship management software, and other essential commerce systems.
Real Networks currently offer two models for integration of Secure Receivers through their Helix Device DRM Community:

- Native Device Support: A Helix DRM Native Device is a network-connected device such as a PC, Set Top Box, Home Media Server, or Mobile Phone. The Native Device can connect directly to the Internet, and has local storage. Helix DRM Native Device support requires both the Helix DRM and the Helix DNA client to run natively on the consumer device. With the Helix DRM Native Device implementation, consumers are able to perform content acquisition, licensing, and playback all on the Native Device. The network connection allows for content retrieval for download and streamed presentations as well as request and receipt of content licenses from the Helix DRM License Server. The storage on the Native Device holds the secure license store containing the content licenses that have been issued as well as any downloaded content. Playback of the media through the Helix DNA Client with the Helix DRM Client Plug-in provides high quality playback of the widest variety of content formats as well as enforcement of the business rules defined by the content owner.
- Secure Receiver Device Support: Helix DRM for Secure Receiver Devices enables Consumer Electronics Manufacturers to enable Industry Supported, Standards Based, Industry Leading secure

media experiences such as subscription & purchase business models on a wide range of consumer, mobile, and portable devices as well as connected home appliances. A Secure Receiver Device is a device that requires a connection to a Native Device for the transfer of content and enforcement of the business rules defined by the content owner.

3.9.4 Helix DRM Components

3.9.4.1 Helix DRM Packager

The Helix DRM Packager uses strong encryption algorithms and secure container technology to prevent unauthorised use of content and to prepare content for distribution via streaming, download or other delivery methods. The packaged media content and the associated business rules for unlocking and using that content are stored separately, so that multiple sets of business rules can be applied to a single file over time. The Helix DRM Packager can support a wide range of media formats and can deliver secure live content when used in conjunction with the RealProducer.

3.9.4.2 Helix DRM License Server

The Helix DRM License Server is a scalable, flexible server that allows retailers, Internet music and movie services, and enterprises to manage, authorise, and report content transactions. The Helix DRM License Server verifies content licensing requests, issues content licenses to trusted, authenticated Helix DRM end-user clients, such as RealPlayer, and provides auditing information to facilitate royalty payments. The content owner, in the event of a security Player breach, can also revoke licenses.

3.9.4.3 Helix DRM Client

The Helix DRM client enables download and streaming playback of secure formats in a tamper-resistant environment based on the usage rules specified by the content owners. Client applications, such as the RealPlayer can be built on top of the Helix DRM client.

3.9.4.4 Helix DRM Device

The evolution of digital media is moving quickly beyond the PC. Consumers throughout the world are moving to take their music with them wherever they go. As connected and non-connected audio and video devices become more prevalent, it becomes critical to enable new business models that take advantage of consumer demand. Content rights holders are quickly seeking proven, reliable methods to deliver their content securely beyond the PC. To secure the media content that is on consumer devices, Helix DRM for Devices enables chip and consumer electronic device manufacturers to include DRM on their consumer devices and to keep content secure beyond the PC. As part of Real strategic initiatives to deliver media anytime, anywhere, and on any device, the flexibility of Helix DRM means that content rights holders can determine the rules for which they want to deliver content to devices. It also means that device manufacturers can provide a complete DRM solution on their devices that will meet the needs of consumers.

Helix DRM 10 for Devices works in two different ways-Primary Device and Secondary Device -thus giving content rights holders and device manufacturers maximum flexibility over their business models.

- **Helix DRM 10 Primary Device**: it is a network-connected device such as a PC, Set Top Box, Home Media Server, or Mobile Phone. The Primary Device can connect directly to the Internet, and has local storage. Helix DRM 10 Primary Device support requires both the Helix DRM 10 and the Helix DNA client to run natively on the consumer device. In the Helix DRM 10 Primary Device implementation, the consumer acquires the secure media file from a media server, and then attempts to play the encrypted file on their Helix DRM 10 Primary Device. Because a license key is required to decrypt the secure media file, the Helix DRM 10 client running on the Primary Device makes a license request and the Helix DRM 10 License Server generates a license with the license key and the associated business rules defined by the content owner.

- **Helix DRM for Secondary Devices**: it enables Consumer Electronics Manufacturers to enable Industry Supported, Standards Based, Industry Leading secure media experiences such as subscription & purchase business models on a wide range of consumer, mobile, and portable devices as well as connected home appliances. A Secondary Device is a device that requires a connection to a Primary Device for the transfer of data and rules for that data. There are two models for integration with Secondary Devices through our private Helix Device DRM Community:
    - Secure Memory Device - With the Secure Memory protocol, manufacturers implement device compatibility with stored secure content and enable the transfer of secure content to the device from an application with native Helix DRM 10 support, such as the RealPlayer 10. By enabling the Secure Memory protocol, CE manufacturers will be able to offer secure download services such as the RealPlayer 10 Music Store to their consumers.
    - Secure Streaming Device - With the Secure Steaming device protocol, device manufacturers allow secure content to be streamed to their devices over a home network. By enabling the Secure Streaming protocol, CE manufacturers can make their devices compatible with premium content services to help drive demand for their device technology.

RealNetworks does plan to enable Secure Streaming via Digital Transmission Copy Protection over Internet Protocol (DTCP-IP).

3.10 Trymedia ActiveMark DRM SYSTEM

ActiveMARK DRM [43] is also the only single protection solution that works on both physical media (CD/DVD) and via download. ActiveMARK DRM ensures that content is used only as intended. Rather than preventing copies from being made by consumers, ActiveMARK is designed to enable copies to revert-to-trial mode (if required), creating additional sales without incremental cost. Additionally, consumers may make backup copies of their content without exposing any additional security risk.
ActiveMARK DRM performs the following client-side operations:

- Business model support
- Rules enforcement
- User interfacing
- License management
- Security

3.10.1 Business model support

ActiveMARK DRM supports different business models, the most common are:

- CD Activation: Product is purchased offline and is then activated to gain access to copying/backup features
- Try Before You Buy: Consumers can try your products, with limitations, before making a purchase decision
- Rent and Buy: Consumers can pay to try your products (rent) before deciding to buy
- Buy without Trial: Consumers can/must purchase your content without being able to run a trial period
- Subscription: Consumers pay a monthly fee for access to a range of content. Access is turned on or off based on the subscription status
- Beta/Demo Uses (non-commercial): Content cannot be purchased, but can be used in trial mode up to a specified limit (time, date, etc.)

3.10.2 Rules enforcement

Rules enforcement articulates how the above business models are implemented. The content owner specifies rules that grant different access controls to his/her content during its lifecycle. Supported rules are:

- Time-based: Allow a trial version to be used during a specified time period
- Use-based: Allow a trial version to be used a certain number of times

- Date-based: Allow a trial version to be used until a certain data
- Space-based Allow a trial version to be played through a certain number of levels or disable the print function
- Complex: Allow a trial version to be used a certain number of times unless the date is before to certain date, and then allow a certain time of use
- Authentication-based: If user has a valid subscription, then allow use for a certain time period and check validity again

3.10.3 User interfacing

It is handled via in-product HTML pages. Pages are typically displayed at launch, close and trial expiration with an emphasis on encouraging consumers to purchase.
Interfaces are packaged within the product itself, allowing users to render and conduct basic operations without needing an Internet connection. These branded pages present product information along with buttons to share it with friends, play trials, reactivate (when licenses have been lost), activate and purchase the product.

Figure x. User interface example

3.10.4 License management

In this process licenses are created, stored and validated on the user's computer.
Typically, a license is requested once a consumer clicks on "BUY" or "ACTIVATE" and payment/authentication is validated. Licenses are created based on the configuration of the user's computer, and allow a customisable level of tolerance for configuration changes before requiring reactivation. These licenses are issued by ActiveMARK License Web Services and are downloaded in the background to the end-user's computer without user intervention.
Once a valid license is installed, it is validated each time the product is executed without requiring a persistent Internet connection. License information can be stored remotely allowing users to retrieve licenses as needed after reformats or to activate products on multiple machines based on the specified rules.

3.10.5 Security

Trymedia follows the established principles of prevention, detection, response and healing to ensure maximum efficacy in the security process throughout the lifecycle:

- Prevention: It is possibly the most important aspect of effective content protection. In addition to the sophisticated design of the ActiveMARK security system, extensive anti-hacking, code obfuscation, cryptographic machine-binding, tamper-proofing, 128-bit encryption and intrusion-detection methodologies are deployed to keep content safe as it travels around the network.

- Detection: It is the process of identifying threats against ActiveMARK and the content protected by it. The earlier Trymedia finds a threat, the more time there is to respond to it. For this reason, the Trymedia R&D team is constantly monitoring underground message boards and hacker communities to identify the most pressing dangers.
- Response: Once a real threat has been identified and isolated, a response is prepared. These responses can take the form of an update to the ActiveMARK Technology (i.e. a new release of the ActiveMARK Packaging Tools), or simply a change in trial criteria. In any case, the objective is to balance the customer experience against the potential risk resulting from an attack.
- Healing: Once a response has been agreed upon, the product is prepared for the healing cycle. A benefit of the ActiveMARK Technology is the ability to update content with the latest version on the server immediately upon repackaging, although this does not change any files that are being passed from person to person. Once a new version of a file is available, the old version ceases to be available immediately on the Trymedia Network, thus reducing the risk from multiple, older versions being made available.

3.11 Light Weight Digital Rights Management

Light Weight Digital Rights Management (LWDRM) [44] has been developed by Fraunhofer-Institute for Integrated Circuits IIS [45] in Erlangen, Fraunhofer-Institute for Digital Media Technology IDMT [46] in Ilmenau and Fraunhofer-Institute for Secure Telecooperation SIT [47] in Darmstadt. Based on personalisation instead of copy protection, LWDRM offers a reasonable balance of security on the on hand and user-friendly handling of content on the other hand. The basic idea is to allow fair use and private copying if the consumer is willing to mark the content with his identity by applying his personal digital signature, thus accepting the responsibility not to use the content in a way that is considered infringing. The concept of accepting responsibility by applying a signature has been common and accepted practice in the area of print media for years, and has been adapted for the handling of audio-visual content. Depending on the prevalent legislation, consumers can transfer content to portable devices or share them with family members and friends. In case of public dissemination through open file sharing systems or websites, however, content can be traced back to the consumer. Thus, rampant infringement can be prosecuted while the user's experience remains as it is today.

3.11.1 LWDRM-System

The philosophy of the LWDRM-System is to enable users to share contents between different devices or among friends in a secure manner. The basic idea corresponds to the procedure in the print media: Every printed publication has to be signed by its author, who thereby declares his or her legal responsibility for the content. This regulation makes it possible to trace back the original author. The LWDRM-System, by applying digital signatures to multimedia contents, transfers this concept from print to digital media.
A user is allowed to transfer contents to other playing devices or pass them on to other friends if and only if he or she is willing to attach their certificate to the contents. This certificate contains a signed public user key along with some information connected to the user. It is assigned together with the accompanying private user key by a certificate authority (CA). Each user, who would like to pass contents on, must register once only at a certification authority. However, if the user does not register, the content can only be played on one device. In the context of LWDRM the act of encoding and subsequently signing content is called publishing.
To realise the described user behaviour, two different file formats are defined within the LWDRM-System. The secure, locally bound format LMF (Local Media Format) can be played only on the device (e.g. a PC) to which it was bound during its creation or download whereas, the signed format SMF (Signed Media Format) is accepted by every LWDRM-compliant playback unit.
The LWDRM system has been developed along the lines of already existing open standards. Therefore, the underlying file format is the ISO Media File Format, which is used by MPEG-4 and Motion JPEG 2000. Different audio and video coders like MPEG-4 AAC (Advanced Audio Coding) and MPEG-4 (Advanced Simple Profile Video Coding) can be used for the coding of multimedia content.

3.11.2 Security

In the philosophy of LWDRM, the term security does not mean protection against the occasional copying of contents but against large scale abuse. Enclosing the digital user certificate within the content ensures this. Each user must have such a certificate issued once only by a certification authority in order to be able to publish contents to pass them on to other persons or to transfer them to other playback units.

As a consequence, the system does not prevent copying of contents explicitly. A distribution on a small scale is possible with the LWDRM-System. However, abuse on a large scale, can be easily traced back to the origin by the LWDRM-System. If a title is found in public, e.g. in a peer-to-peer network, then by definition, it is no longer a copy for family members. In this case the originator can be traced back by mean of the enclosed certificate and faces the risk of prosecution. It is to be expected, that the system encourages users to distribute contents only to trustworthy friends from their personal background. Otherwise they run the risk that the media files could be traced back to them and that they would consequently be held legally responsible. The overall effect will be a decrease in illegal copying compared to recent figures.

3.12 SafeNet Digital Rights Management

SafeNet [48] acquired past April DMDsecure B.V. [49], a global leader in carrier grade server-side Digital Rights Management (DRM) components for solution providers and software vendors as well as broadcasters, broadband & mobile operators and service providers. SafeNet, the seventh largest information security company in the world, has encryption technologies to protect communications, intellectual property, and digital identities, and offers a full spectrum of products including hardware, software and chips. SafeNet has a successful and growing rights management business focus. The combination of SafeNet's strong security and DMDsecure's content DRM server provides customers with a complete suite of strong standards-based security to protect the electronic delivery of content whether in software, audio, video or gaming formats.

SafeNet partners with leading organisations, Windows Media Product Vendors [50], ContentGuard [51], Sun Microsystems, Inc. [52], TANDBERG Television [53] and SeaChange International [54], to provide the best in integrated solutions and to deliver local expertise.

SafeNet provides rights management products and services that protect and enable revenue for intellectual property (IP). SafeNet's Rights Management solutions address the entire licensing and distribution process and are flexible enough to adjust to the business needs of our customers. SafeNet rights management solutions serve three key industry segments:

- Software: Application developers need to protect themselves from the relentless threat of piracy. An effective rights management scheme can also benefit organisations far beyond a reduction in revenue leakage.
- Entertainment: Providers of movies, music, games and other entertainment must also defend their revenue against piracy. Technology that has made piracy easier, such as P2P networks and broadband access can actually represent new distribution channels for content providers equipped with rights management systems.
- Enterprise: Enterprises need to protect the sensitive data they regularly create. From corporate financial data to private customer information, DRM technology enables enterprises to effectively control access to information.

3.12.1 Software Protection

Sentinel products enable application developers to enforce the terms of their license agreements and protect revenue streams. As Sentinel Products provide flexible licensing options and automate license fulfilment and management, they allow ISVs to realise increased revenue opportunities and lower operational costs. Sentinel has been setting the standard for software protection since 1992.
Sentinel RMS is a complete software rights management solution that includes components for design, automated fulfilment, and ongoing management of licenses.

- Sentinel Hardware Keys - UltraPro keys speed integration, manage licenses and offer the highest level security against piracy and license non-compliance
- Sentinel Hardware Keys - SuperPro For current clients only

3.12.2 Entertainment Rights Management

These products are addressed to content providers. Using these DRM solutions, content providers can create additional distribution channels and increasing revenue streams by securely distributing digital content to mobile and consumer devices. Mobile networks in particular offer advantages to content owners, with their vast reach and the continued advancement of standards in the mobile world.
DRM Mobile is a fast, flexible and scalable server-side solution for mobile Digital Rights Management. DRM Mobile enables the entire DRM process: content protection, rights management, license generation and license delivery to handsets as well as consumer electronic devices.

- OMA DRM Server Toolkit is a server-side DRM software developer toolkit. OMA DRM Server Toolkit implements and complements the OMA V1.0 and V2.0 DRM specifications.
- DRM Fusion is a carrier grade, flexible and scalable server DRM solution implementing and extending multiple DRM technologies such as Windows Media DRM 9 and 10 and OMA DRM while providing common integration interfaces.

3.12.3 Enterprise Rights Management

These products are addressed to corporations to protect sensitive information both to prevent release to external sources as well as restricting access among employees. SafeNet's Enterprise Rights Management solutions enables an administrator to control and manage access, but can register the number of employees who accessed certain content.

DRM Enterprise is an out of the box DRM solution based on Microsoft's Windows Media DRM and enables corporate communication without adding any client software. It enables live and on-demand corporate content and applies to downloadable as well as streaming video and audio.

3.13 SDC DRM

The DRM solution from SDC [55] consists of server (packager) and client software.

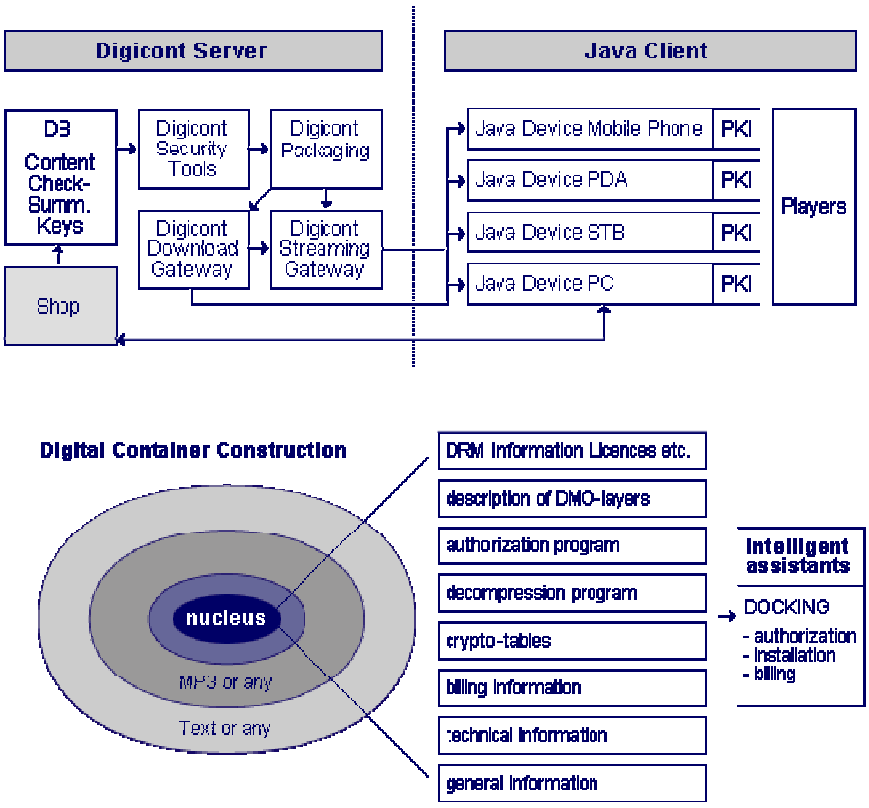
The core technology is based on the "Digital Multi Media Object"; a concept which was developed by Rolf Brugger in 1994 and patented in Europe and USA in 1996 as the first DRM patent in the content delivery industry.

DRM Java-based technology characteristics:

1. No client installation on the device is required, only a Java Virtual Machine is needed to execute the license rules
2. The content can be transferred to different devices belonging to the customer without losing the DRM protection - we call it Multi-Device DRM
3. Superdistribution of content is possible to increase the customer base
4. All kind of content can be delivered with a DRM protection
5. Different kind of authentication system per customer can be used to give the customer access to his content, we call it Multi-PKI DRM
6. By using the Java platform, SDC Java DRM has the broadest native user base in the market which is approximately 70% of all digital devices used by consumers

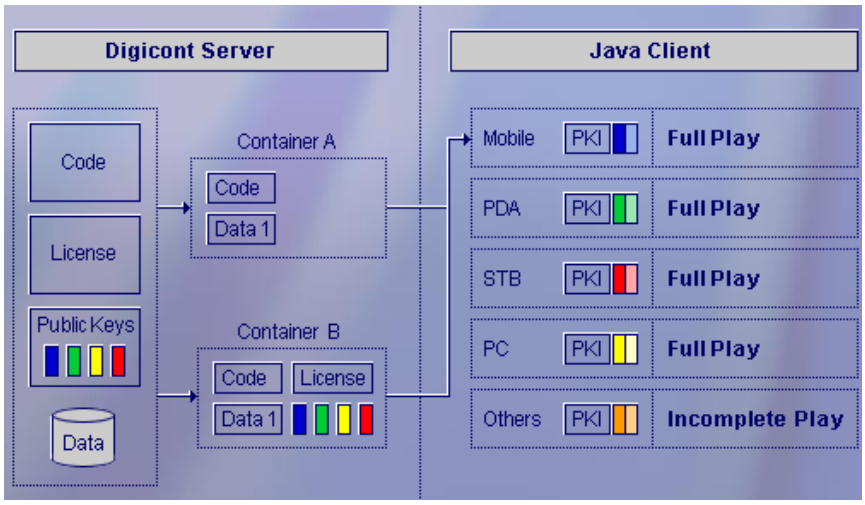
3.13.1 Mobile Code Architecture & "Digital Container Object"

SDC Java DRM is a technology based on mobile code architecture. Because of this advanced architecture the system is able to package content together with code in a "container". This object works as a transport unit for content, software and code. The client is within the container and is interpreted by the Java Virtual Machine on the device. An installation of the client is not necessary.



3.13.2 Multi Device & Multi PKI

The demand for a secure transfer of purchased content to other devices belonging to the same customer with different authentication systems used, is a critical topic for a successful commercial content delivery service. SDC Java DRM provides these functionalities in a unique manner.



3.13.3 Superdistribution

To offer customers the option the share content with friends by protecting the license restriction, SDC has developed a secure process for superdistribution. The content file is spitted into 2 or more containers. In the case of music the content is split in a container A and B. Container A is carrying 95% of the content by snipping pieces of the music out of the file. The music can be played back and instead of the missing pieces advertising or promotion sound files can be filled in. Container A can be shared with the world. In the container B the missing pieces are encrypted and personalised watermarked. The model using container A and B is free configurable to the Business Model and demands of the Content Distributor.

3.13.4 Security

Security features:

- Content encrypted with standard encryption algorithms (RSA 128)
- Content encrypted with unique session key
- Containers protected against hacking with signing algorithm
- License tied to user's private keys
- Multiple key handling
- Playback only possible if the given private keys are in place and valid
- Reverse engineering prevented by different obfuscation techniques
- Personalised watermarking for tracking purposes

3.13.5 SDC DRM Solutions

Channel	Devices	Type of Network	Type of Contents	Distributors	License Models
Wireless	Mobile Phones PDA Car Handsets Other	GPRS UMTS W-LAN Blue Tooth Etc.	Music Video Pictures Games	Mobile Carrier E-Tailer Retailer Online Services	OMA Compliant Licence Models plus Secure Superdistribution Secure Transfer of Content
Fix Line	Set-top Boxes PC Game Console Digital Home Stereo	CATV ADSL LAN	Music Video Pictures Games	Cable Network Providers Telcos E-Tailer Retailer Online Services	MHP/Ocap Compliant Licence Models Plus Secure Superdistribution Secure Transfer of Content

3.13.6 Applications

SDC Java DRM is currently in use in different mobile data services projects in Europe:

- MmO2 Plc (United Kingdom, Germany, Ireland and Netherlands): SDC Java DRM is the chosen DRM System for the "O2 Music to mobile" service. The following functionalities will be provided:
    - Music streams over the air to GPRS devices
    - Music download over the air to GPRS devices
    - Music streams/download over the air to GPRS devices
    - Music download over the air to UMTS devices
    - SDC Music Client Package for mobile headsets
- SFR (France): Functionalities provided:

  - Music streams over the air to GPRS devices
  - Music download over the air to GPRS devices
  - Music streams/download over the air to GPRS devices
  - Music download over the air to UMTS devices
  - SDC Music Client Package for mobile headsets
- Amena (Spain): Functionalities provided:
  - Music streams over the air to GPRS devices
  - Music download over the air to GPRS devices
  - Music streams/download over the air to GPRS devices
  - Music download over the air to UMTS devices
  - SDC Music Client Package for mobile headsets

In the USA an initiative with Sun Microsystems is launched to address the Cable Network and Broadband Market with services like:

- Music download to Set-top Boxes
- Video download to Set-top Boxes
- Video streaming to Set-top Boxes

3.14 Internet Digital Rights Management

Internet Digital Rights Management (IDRM) [56] was an IRTF (Internet Research Task Force) Research Group formed to research issue and technologies relating to Digital Rights Management (DRM) on the Internet. The IRTF was a sister organisation of the Internet Engineering Task Force (IETF). Currently, this group has been closed.

IDRM investigated DRM technologies and the problems related to them, with a focus on the IP network infrastructure issues. The group was mostly concerned with delivery of content from content providers to service providers and from service providers to end-users. But it also investigated new delivery relationships that might become possible by wider adoption of DRM technologies on the net.

The IDRM group co-ordinated its work with other IRTF and IETF (Internet Engineering Task Force) activities as well as W3C efforts in DRM, e.g. XML-based rights languages. IDRM group only published three drafts, mainly about the handle system. The Handle System is a general-purpose global name service that allows secured name resolution and administration over the public Internet. The Handle System manages handles, which are unique names for digital objects and other Internet resources. This document provides an overview of the Handle System in terms of its namespace and service architecture, as well as its relationship to other Internet services such as DNS, LDAP/X.500, and URN.

3.15 OeBF

The Open eBook Forum (OeBF) [57] is trade and standards Group for eBook Industry. More than 70 members Worldwide form it, this independent organisation is guided by board of directors and membership.

The Rights and Rules Working Group [58] was proposed in 2001. The mission of the Rights and Rules Working Group (“group”) was to create an open and commercially viable standard for interoperability of digital rights management (DRM) systems, providing trusted exchange of electronic publications (ePublications) among rights holders, intermediaries, and users.

Several members of the OeBF proposed this group to attempt to converge quickly on a practical standard for interoperable DRM for eBooks, acting within the OeBF and following its rules and procedures.

This group was attempting to produce a useful standard in a relatively short time. The resulting DRM specification would make specific provision for extensions, versioning, and upward compatibility.

The scope of this Working Group will be to gather, analyze, prioritise, and coordinate requirements into the development and completion of an OeBF DRM specification.

- Glossary of terms and definitions and descriptions of stakeholders and of roles in an interoperating commercial network. The group will contribute additional terms to the Framework document as needed.

- Determining a balance between privacy, as required by law and consumer preference, and usage tracking, as desired by publishers.
- Selection and description of requirements addressed by the specification, including how the potential specification may interact with existing international standards.
- Design assumptions.
- General description of a DRM system.
- Data definition (format and meaning) of rights-defining object.
- Use cases addressed by the specification.
- Definition of "trust" needed between clients and servers.
- Provisions for upward compatibility.
- Definitions of trust levels and processes for rating vendors and interoperating products.
- Required trust services.
- Definition of mutual authentication and trust negotiation by clients and servers.
- Consideration of "superdistribution" techniques: peer-to-peer distribution of encrypted content with separate distribution of rights, temporary lending, and other peer-to-peer applications.
- Processing, rules, and interfaces, for software manager ("engine") handling rights objects.
- Metadata format and elements needed by current version of specification, including the relevant identifier and identifier system; provision for later versions.
- Data definitions for client and server credentials and for certificates.
- Applicable laws and regulations.
- General requirements and assumptions about container files.
- Implementation notes: status and details of various implementations, to help implementers build interoperable products.

The Rights and Rules group is working on a specification for a Rights Grammar, taking as a baseline the MPEG-21 Rights Expression Language. The specification will provide the publishing community with a means to express business rules by granting unambiguous access permissions.

There was only one public document Requirements on 2003.

3.16 PRISM

The Publishing Requirements for Industry Standard Metadata (PRISM) [59] Working Group was established in 1999 by a group of companies primarily involved in the production of serial and web-based editorial content that recognised the value of content standards. This group included publishers, other rights holders, systems integrators, software developers and content aggregators who faced common content application challenges such as re-use of content in multiple media types, rights and contract management, better access to content archives, and faster, less expensive exchange and integration of disparate sets of content across the enterprise and with outside business partners. The representatives of these companies believed that developing and adopting a standard set of XML metadata would assist them in managing and automating their labour-intensive content workflow processes.
The PRISM specification [60] defines an XML metadata vocabulary for managing, aggregating, post-processing, multi-purposing and aggregating magazine, news, catalogue, book, and mainstream journal content. PRISM recommends the use of certain existing standards, such as XML, RDF, the Dublin Core, and various ISO specifications for locations, languages, and date/time formats. In addition PRISM provides a framework for the interchange and preservation of content and metadata, a collection of elements to describe that content, and a set of controlled vocabularies listing the values for those elements.

Metadata is an exceedingly broad category of information covering everything from an article's country of origin to the fonts used in its layout. PRISM's scope is driven by the needs of publishers to receive, track, and deliver multi-part content. The focus is on additional uses for the content, so metadata concerning the content's appearance is outside PRISM's scope. PRISM focused on metadata for:

- General-purpose description of resources as a whole

- Specification of a resource's relationships to other resources
- Definition of intellectual property rights and permissions
- Expressing inline metadata (that is, mark-up within the resource itself).

Today PRISM consists of two specifications. The PRISM Specification, itself, provides definition for the overall PRISM framework. A second specification, the PRISM Aggregator DTD is a new standard format for publishers to use for delivery of content to web sites and to aggregators and syndicators. It is an XML DTD that provides a simple, flexible model for transmitting content and PRISM metadata.

The PRISM specification deliberately does not address security issues. The working group decided that the metadata descriptions could be secured by whatever security provisions might be applied to the resource(s) being described. PRISM implementations can achieve necessary security using a variety of methods, including:

- Encryption at the transport level, e.g., via SSL, PGP, or S/MIME.
- Sending digitally signed content as items within the PRISM interchange format, with verification performed at the application level (above PRISM).

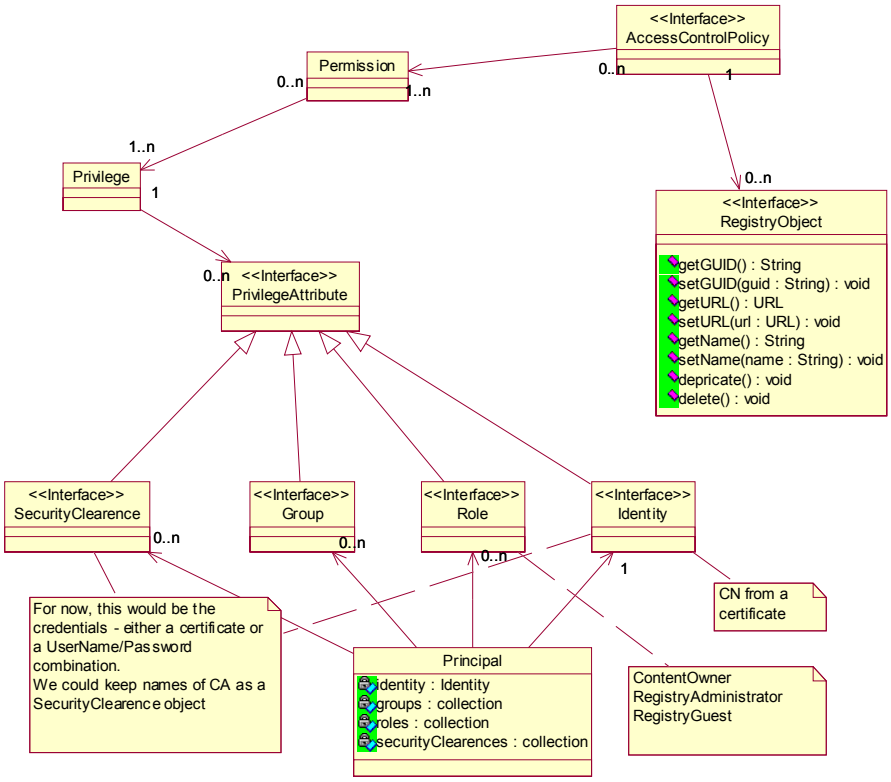
The PRISM specification does not address the issue of rights enforcement mechanisms. The working group decided that the most important usage scenarios at this time involved parties with an existing contractual relationship. This implied that the most important functionality required from PRISM's rights elements was to reduce the costs associated with clearing rights, not to enable secure commerce between unknown parties. Therefore the PRISM specification provides mechanisms to describe the most common rights and permissions associated with content, it does not specify the means to enforce compliance with those descriptions. Essentially, the goal is to make it less expensive for honest parties to remain honest, and to let the courts serve their current enforcement role.

3.17 OASIS

The Organisation for the Advancement of Structured Information Standards (OASIS) [61] is a not-for-profit, global consortium contributing to the development, convergence and adoption of e-business standards. OASIS produces worldwide standards for security, Web services, XML conformance, business transactions, electronic publishing, topic maps and interoperability within and between marketplaces. OASIS has more than 500 corporate and individual members in 100 countries around the world. OASIS and the United Nations jointly sponsor ebXML [62], a global framework for e-business data exchange.
One of the current OASIS technical committees is the OASIS Rights Language Technical Committee (RLTC). The purpose of the RLTC is to define the industry standard for a digital rights language that supports a wide variety of business models and has an architecture that provides the flexibility to address the needs of the diverse communities that have recognised the need for a rights language. OASIS RLTC uses XrML as the basis in defining the industry standard rights language in order to maximise continuity with ongoing standards efforts.

3.17.1 Security Info Model

The security model is based on two goals – simplicity from a client's point of view and extensibility for future enhancements.
The following figure shows the info model, which contains the security related objects.



The AccessControlPolicy is the top-level security object. It ties together the permission object with an instance of a Registry object. The permission object also contains the methods (of the RegistryObject), which the privilege object can access.
A privilege object contains many Privilege Attributes. A Privilege Attribute can be a Security Clearance, a group, a role, or an identity. This association enables one, the flexibility to have object access control policies based on a role, an identity or a group or a security clearance or even better all of the above.
While privileges deal with groups, roles et al, the permissions deal with the methods of an object and tie them to privileges. The permission is an “and” operation (or a cumulative) i.e. an entity can access the method of a RegistryObject only if it has all the privileges as detailed by the privilege object.
On the other hand, the AccessPolicy is an “or” operation. If an entity has “any” of the permissions, it can perform the method as detailed by the permission object.
An Identity usually is the DN in a certificate. It could be username/password as well.
The SecurityClearance object could keep the CA names, root certificates, et al. A SecurityClearance could be the traditional operations like Read, Create, Update, and Delete.
The Principal object is an entity, which has an identity, and optionally a set of role memberships, group memberships or security clearances. The authenticator will work against a principal.

3.18 cXML

Commerce XML (cXML) [63] is an open Internet-based standard for e-commerce. cXML reduces on-line business trading costs by facilitating the exchange of content and transactions over the Internet. Developed in concert with more than 40 leading companies, cXML is a set of lightweight XML DTDs based on the World Wide Web Consortium's XML standard with their associated request/response processes.
cXML provides an infrastructure that will streamline the process of digitally exchanging catalog content and transactions in a secure manner. cXML supports all supplier content and catalogue models, including buyer-managed, supplier-managed, content management services, electronic marketplaces, and web-based sourcing

organisations. This will allow suppliers to provide customers with selective access to personalised catalogue content while maintaining their unique branding and competitive differentiation.
Additionally, cXML defines a request/response process for the exchange of transaction information. These business processes include purchase orders, change orders, acknowledgments, status updates, ship notifications and payment transactions.
cXML allows buying organisations, suppliers, service providers, and intermediaries to communicate using a single, standard, open language.
Successful business-to-business electronic commerce (B2B e-commerce) portals depend upon a flexible, widely adopted protocol. cXML is a well-defined, robust language designed specifically for B2B e-commerce, and it is the choice of high volume buying organisations and suppliers.
cXML transactions consist of documents, which are simple text files containing values enclosed by predefined tags. Most types of cXML documents are analogous to hardcopy documents traditionally used in business.
The most commonly used types of cXML documents are:

- Catalogues
- PunchOut
- Purchase Orders

3.19 Apple iPod DRM

No public specifications available.

3.20 XrML

The eXtensible rights Markup Language [64] is the rights expression language developed by ContentGuard. It has been defined as the Digital Rights Language for Trusted Content and Services that provides a universal method for securely specifying and managing rights and conditions associated with all kinds of resources including digital content as well as services.
XrML is based on DPRL [65] that is intended to support commerce in digital works and specification of access for secure digital documents in cases where financial exchange is not part of the terms of use.
The design goals for DPRL are to describe rights, fees and conditions for commerce models, to provide standard terms for usage rights specifications, to provide operational definitions of specifications for vendors of trusted systems and to provide a basis of extensibility to new language features in a manner that does not compromise the other goals
XrML is an XML-based specification grammar for expressing rights and conditions associated with digital content, resources, and services
The XrML specification defines a general-purpose language in XML used to describe the rights and conditions for using digital resources. It also provides mechanisms to ensure message integrity and entity authentication within XrML documents. The specification consists of the following parts:

- XrML Core Schema: Provides normative technical details regarding the core of the XrML design and architecture
- Standard Extension Schema: Provides normative technical details regarding the XrML standard extension. This extension to the language defines types and elements common to many XrML usage scenarios but which do not form part of the core language.
- Content Extension Schema: Provides normative technical details regarding the XrML content extension. This extension to the language defines types and elements to describe rights, conditions, and metadata for digital works, allowing trusted systems to exchange digital works and interoperate

The most important concept in XrML is a license. An XrML license contains two elements a grant that conveys to an identified party (principal) the right to use a resource subject to certain conditions and an issuer that digitally signs the license. In addition, the issuer may provide additional information about the issuance of the license.

Next figure illustrates the structure of an XrML license.

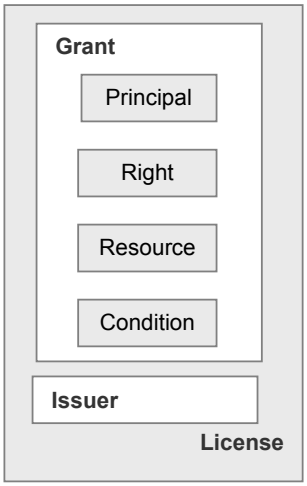


Figure XrML license

XrML was chosen as the basis for the development of the MPEG Rights Expression Language.

3.21 ODRL

The Open Digital Rights Language (ODRL) [66] is a proposed language for the Digital Rights Management community for expressing rights information over the digital content. It intends to provide flexible and interoperable mechanisms to support transparent use of digital resources in distributing or consuming of creations in digital form. ODRL is focused on the semantics of expressing rights languages and definitions of elements in the data dictionary and it can be used within trusted or untrusted systems for both digital and physical resources.

The models for the ODRL language and data dictionary contain the structure and core semantics for the expressions. These models provide the overall framework for the expressions into which elements can be applied.

ODRL is based on an extensible model for rights expressions, which involves three core entities and their relationships. The core entities are assets that include any physical or digital content, rights that include permissions that are the usages or activities allowed over the users. The Permissions can contain constrains, requirements and conditions. Constraints are limits to these permissions, requirements are obligations needed to exercise the permission and conditions specify exceptions and parties that include end users and Rights Holders.

An ODRL license is formed by the elements shown in the following figure.

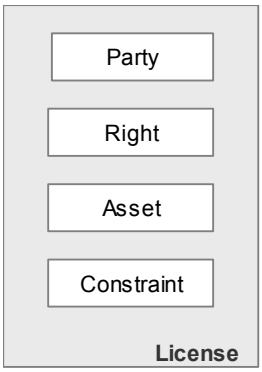


Figure. ODRL License

4 Copyright and IPR issues

4.1 European legal framework

4.1.1 Introduction

A) WIPO Treaties overview
Based on existing international treaties, namely the Berne Convention for the Protection of Literary and Artistic Works as revised in Paris on July 24, 1971, and the Rome Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations of October 26 1961, a WIPO Conference in Geneva adopted the WIPO Copyright Treaty (WCT) and the WIPO Performances and Phonograms Treaty on December 1996 (WPPT) Those treaties demonstrated the increasingly need for a strong harmonisation with respect to IP legislation on international level. The Directive 2001/29/EC on "the harmonisation of certain aspects of copyright and related rights in the information society" obliges MS to transpose into national law the main international obligations arising from the two treaties on copyright and related rights adopted within the framework of the World Intellectual Property Organisation (WIPO).
The WIPO Copyright Treaties aim to provide solutions to the questions raised by new technologies and new form of exploitation of IPR. The key provisions can be summarised as follows.

WCT and WPPT key provisions

New set of rights:

- **Right of communication to the public:** Art. 8 of the WCT Treaty

This article grants right holders with a new exclusive **right of communication to the public.** The language of the article is such that the communication of a work to the public by the means of the new technologies will be subject to the authorisation of authors of literary and artistic works.

- **Right of Making Available of fixed performances and of phonograms:** Art 10 and 14 WPPT

The introduction of this provision states that producers of phonograms and Performers have the exclusive right of authorising the making available to the public respectively of their performances fixed in phonograms and of their phonograms, by wire or wireless means, in such a way that members of the public may access them from a place and at a time individually chosen by them.
The "making available right is one of the most important innovation of the WIPO Treaty allowing phonographic producers and performers to have control of the exploitation of their works.

- **Reproduction right**

The WPPT clearly defines the right of reproduction of Performers and Producers respectively in Art 7 and Art 11 which has to be applied in the digital environment as stated in the ***Agreed statement concerning Articles 7, 11 and "****The reproduction right, as set out in Articles 7 and 11, and the exceptions permitted hereunder through Article 16, fully apply in the digital environment, in particular to the use of performances and phonograms in digital form."*

In the WTC Treaty there is not a specific article on the **right of reproduction** but it has been included in the agreed statement concerning article 1 of the Treaty: "*The reproduction right, as set out in Article 9 of the Berne Convention, and the exceptions permitted hereunder, fully apply in the digital environment, in particular to the use of works in digital form"*

- **Right of distribution** Art. 6 of the WTC - Art 8 and art 12 of WPPT

The principles of this article are an improvement for right holders. However the agreed Statement concerning these articles is of notable importance as they restrain the right of distribution to "fixed copies that can be put into circulation as tangible objects".

Limitations and exceptions

WTC Art. 10 and art 16 of WPPT concern the limitation and exceptions. They allow Contracting States to provide for limitations and exceptions to the rights provided for in the new Treaties under the strict conditions of the so called **3-steps-test.**

• the limitations or exceptions are confined to "special cases";
• the limitations or exceptions do not conflict with the normal exploitation of the work;
• the legitimate interests of the author are not unreasonably prejudiced.

Technological measures

WTC Art. 11 and art 18 WPPT provide for important obligations for Contracting States concerning the protection of technological measures: at national level, Contracting States should therefore provide for civil and criminal remedies against any action intended to circumvent technological measures. In short Member states should prohibit hacking the encryption used by right holders to prevent unauthorised copying of or access to works

Rights Management Information

WTC art 12 and art 19 WPPT Member countries must provide adequate and effective legal remedies against the removal or altering of "rights management information" knowing that it will enable or induce infringement of copyright, and the distribution of copyrighted works knowing the RMI has been removed or altered.

WTC art 12 As used in this Article, "rights management information" means information which identifies the work, the author of the work, the owner of any right in the work, or information about the terms and conditions of use of the work, and any numbers or codes that represent such information, when any of these items of information is attached to a copy of a work or appears in connection with the communication of a work to the public.

WPPT art 19 as used in this Article, "rights management information" means information which identifies the performer, the performance of the performer, the producer of the phonogram, the phonogram, the owner of any right in the performance or phonogram, or information about the terms and conditions of use of the performance or phonogram, and any numbers or codes that represent such information, when any of these items of information is attached to a copy of a fixed performance or a phonogram or appears in connection with the communication or making available of a fixed performance or a phonogram to the public.

Term of Protection

Art. 9 of the WTC extends the protection of photographic works in the territories of Contracting States from 25 to 50 years.

Art 17 WPPT:

1. The term of protection to be granted to performers under this Treaty shall last, at least, until the end of a period of 50 years computed from the end of the year in which the performance was fixed in a phonogram.
2. The term of protection to be granted to producers of phonograms under this Treaty shall last, at least, until the end of a period of 50 years computed from the end of the year in which the phonogram was published, or failing such publication within 50 years from fixation of the phonogram, 50 years from the end of the year in which the fixation was made.

WPPT: some important considerations

- **New Definition of phonographic producer**

"producer of a phonogram" means the person, or the legal entity, who or which takes the initiative and has the responsibility for the first fixation of the sounds of a performance or other sounds, or the representations of sounds;

Previous definition (Rome international Convention 1961): "producer of phonograms" means the person who, or the legal entity, which, first fixes the sounds of a performance or other sounds;

It's worth to mention that following this new definition, the right owner with respect to the "phonograms" has not to be confused with the record label when the record label does not take the responsibility for the first fixation. Even if the system for the identification of the right owner (and therefore the collection and distribution of revenues) still follows "record label" parameters, the reference to the record itself is not feasible in the new digital environment.

- **Moral right of performers**

Before the WIPO Treaties, neither the Rome Convention nor any other international treaty granted moral rights to performers, whereas Article 6bis of the Berne Convention confers such rights on authors. Under the WPPT Treaty, a performer may, as far as is reasonably applicable, claim to be identified as the performer of his performances, and may object to any distortion, mutilation or other modification of his performances that would be prejudicial to his reputation.

- **Right of remuneration**

Performers and producers are both entitled to an equitable remuneration for any use of phonograms for commercial purposes or for broadcasting or communication to the public, including the playing of a phonogram to the public present in the same place

WIPO Treaties summary

1996 WTC 48 contracting states

Major provisions:

1) introduction of the right of distributions with international exhaustion
2) introduction of the right of communication to the public in general (including "interactive transmission")
3) expansion of the term of protection of photographic work
4) provisions for "technological measures"
5) provisions for "right management information"

1996 WPPT 44 contracting states

Major provisions

1) New definition of producer of phonogram
2) Moral rights of performers

3) Introduction of the right of making available
4) economic rights of performers and phonogram producers with respect to phonograms
5) provisions for "technological measures"
6) provisions for "rights management information"

B) The EUCD Directive

The Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on " the harmonisation of certain aspects of copyright and related rights in the information society" commonly known as the EU Copyright Directive (EUCD) aims to bring IP legislation in line with the Information Society and technological developments by structuring copyright protection in the new environment The purpose of this section is to provide an overview on the ways in which EU members states have transposed the EUCD most controversial provisions such as those related to the exceptions and to the protection of technological measures into national laws
Scheme representing the current status of EU Members implementation:

AUSTRIA July 2003
BELGIUM no
DENMARK December 2002
FINLAND no
FRANCE no
GERMANY September 2003
GREECE October 2002
ITALY April 2003
SPAIN no
UK October 2003

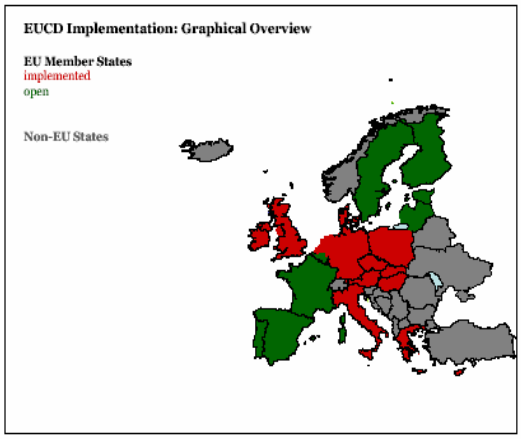


Figure EUCD Implementation: Graphical Overview

Rights definitions

- **Reproduction right**

As for the specific rights contained in the EUCD, Article 2 obliges MS to grant the creator of a copyright protected work the exclusive right to authorise or prohibit any **reproduction**. Article 2 also specifies the acts of reproduction covered by exclusive rights as to comprise direct or indirect, temporary or permanent reproduction by any means and in any form, in whole or in part

- **Right of communication to the public of works**

With respect to the **right of communication**, Article 3 states that right holders have an exclusive right to authorise or prohibit any communication to the public of the originals and copies of their works. This right entails the making available to the public of their works in such a way the public may access them from a place and at a time individually chosen by them (e.g. Internet). This provision also covers the on-line demand services but it does not cover private communications.
Both rights are granted to:
authors, **performers** for the fixed performances, **phonogram producers** on the phonograms, **producers** of the first fixations **of films** and **broadcasting organisations**, of fixations of their broadcasts

Exceptions

The EUCD introduces exhaustive list of 'exceptions and limitations' to the exclusive rights of the right owners. The exceptions granting uses that are considered as non infringing are stated by all the copyright laws of the different member states. Article 5 of the EUCD gives each member state the option to include any or all of the exceptions in their national version of the legislation. Crucially, the Directive in Article 5 lays down a number of exceptions to the right of reproduction and the right of communication.

- **Exceptions to the right of reproduction**

ART 5.1 Only Mandatory exception:

Exception to the right of reproduction in respect of certain temporary acts of reproduction, which are integral to a technological process and have *no economic significance* (e.g. caching during transmission, web browsing).

ART 5.2 exceptions

a) copying on paper (not sheet music), fair compensation
b) analogue and digital copying on any medium, by a natural person for private use (fair compensation)
c) specific acts of reproduction by libraries, educational establishments, museums and archives, which are not for direct or indirect economic or commercial advantage
d) ephemeral recordings of works made by broadcasting organisations by means of their own facilities and for their own broadcasts the preservation
e) reproductions of broadcasts made by social institutions pursuing non-commercial purposes, such as hospitals or prisons (fair compensation).

- **Exceptions to the right of reproduction and right of communication to the public**

a) illustration for teaching or scientific research (source to be indicated i.e. author name)
b) uses for the benefit of the disabled people to the extent required by specific disability
c) reproduction by the press, communication to the public or making available of published articles on current economic, political or religious topics (source to be indicated)
d) quotations for purposes such as criticism or review, related to a work which has already been lawfully made available to the public (source to be indicated)
e) use for the purposes of public security or reporting of administrative, parliamentary or judicial proceedings
f) use of political speeches and extracts of public lectures or similar works to the extent justified by the informative purpose (source to be included)
g) use during religious celebrations or official celebrations organised by a public authority
h) use of works, such as works of architecture or sculpture, made to be located permanently in public places
i) incidental inclusion of a work or other subject-matter in other material
j) use for the purpose of advertising the public exhibition or sale of artistic works, to the extent necessary to promote the event,
k) use for the purpose of caricature, parody or pastiche
l) use in connection with the demonstration or repair of equipment
m) use by dedicated terminals on-site for the purpose of research or private study, not of works nor subject to purchase or licensing terms
n) existing exceptions of minor importance

All exceptions must comply with the Berne Convention 3 step test and common to all of them is their non-economic nature.

However, in most cases, MS have to determine "**fair compensation**" and ensure that the right holders actually receive it. The Directive gives Member States certain flexibility in determining the form, detailed arrangements and level of *fair compensation*.

There are three important considerations which the Directive specifically exhorts Member States to take into account when determining the compensation level namely:
1. The harm, if any, caused to the right holder;
2. The availability, and degree of use of so-called 'technical protection measures'; and
3. Any other payments to the right holder, e.g. by way of a license fee, in which case no further compensation payment may be due

Exceptions: EU members' implementation

Looking at the current nationals' proposals for transposition or at the actual implementation of the Directive we have to underlines that in most cases, member States have chosen to keep existing exceptions without suppressing some or creating new ones; these exceptions reflect each country own cultural traditions and business practices.
Therefore the way member states comprise a closed list of exceptions are rather different as different are the content of such lists. In Europe, exceptions to copyright are largely diverse and not harmonised. The fact that Member States could choose to introduce – or not – such a wide range of exceptions does not bode well for a harmonised copyright framework, a framework which is intended to govern an information society with no territorial borders. However the following exceptions are generally recognised:
private copy or other private use, parody, quotation, use of a work for scientific or teaching purposes, news reporting, library privileges, needs of the administration of justice and public policy. But all these exceptions are not recognised in all countries: for instance, France does not know any exception for research or education, nor for libraries, while Germany do not have any exception for parody. Next to those broad categories of copyright exceptions, there are also very specific cases regarding particular situations. For example, there is the Greek exception, which allows the reproduction of Film (make copies of films) for purposes of restoration, or the German exception for public performance of beneficial events. The inconsistency arising from having different exceptions is more critical in the online environment and is potentially damaging for right holders.

AUSTRIA
- Private copy: copying for own private use – non commercial purposes
- disabled persons: non commercial ends
- copies for teaching purposes and copies on paper or a similar matter on any media may be produced only for non-commercial end and the following conditions must apply:
  - one single copy may be produced of own pieces of work; this copy may be exhibited, lent or used under same provisions as the original
  - like private persons, libraries and archives may produce single copies of works, which have not been published or are out of print; the same provisions on exhibiting, lending and using the work apply to these copies as to the original work.

BELGIUM
The proposed implementation text confirms the following 9 exceptions already provided in Belgian laws.
- Private copy: Reproduction in and for the family – the amendment proposal restricts the scope of the definition to non-commercial use.
- Citation for scientific, teaching and critics purposes
- For information purposes
- Use for reproduction and communication in a public place
- Use for free and private communication within the family
- Use of partial reproduction in a private or didactic place
- Caricature, parody and pastiche

- Use in connection with public exams
- Use for public loans organised by public authorities (prêt public)

DENMARK
For most part the exceptions listed in Article 5 of the Directive are identical to the exceptions that were a part of the existing Danish law.
The main differences are as follows:

- Private copy: is entitled to make or have made, for private purposes, single copies of works which have been made public if this is not done for commercial purposes. Such copies must not be used for any other purpose. The provision of subsection (1) does not confer a right to engage another person to make copies of (I) musical works; (ii) cinematographic works; (iii) works of applied art; or (iv) works of art if the copying is in the form of an artistic reproduction. (4) The provision of subsection (1) does not entitle the user to make copies of musical works and cinematographic works by using technical equipment made available to the public in libraries, on business premises, or in other places accessible to the public.
- Photocopying (Article 5.2(a) is not considered as an exception as it was in existing Danish law. Instead the law allowed for a legal licence that requires schools and universities to negotiate compensation with the authors' collective rights management organisation. This was kept unchanged in the new legislation.
- Exceptions for satire and in connection to with the repair of equipment are not included in the new legislation.

FINLAND
New law proposal (still under discussion)
The proposal intends to change exemptions fundamentally by requiring that for any copyright exemption to apply the user must first have obtained a legal copy of the whole work. Therefore to cite for didactic purpose any given work found on the Internet user should get the right owners authorisation or explicit consensus. The foreseen exceptions are:

- Private use
- Photocopying
- Internal publications
- Educational use (matriculation exam)
- TV and Radio in governmental facilities (hospitals, prisons etc)
- Museums, archives
- Disabled persons
- Composite works
- Showing a copy
- Quotations
- Reuse in newspapers
- Concert programs
- Recording news events
- Repeating public statements
- Document publicity, public security

FRANCE
Law project (not entered into force yet)

- Private copy: once a work has been disclosed, the author may not prohibit:
  - private and gratuitous performances carried out exclusively within the family circle;
  - copies or reproductions reserved strictly for the private use of the copier and not intended for collective use, with the exception of copies of works of art to be used for purposes identical

with those for which the original work was created with the condition that the name of the author and the source are clearly stated:

- analyses and short quotations justified by the critical, polemic, educational, scientific or informative nature of the work in which they are incorporated;
- press reviews;
- dissemination, even in their entirety, through the press or by broadcasting, as current news, of speeches intended for the public made in political, administrative, judicial or academic gatherings, as well as in public meetings of a political nature and at official ceremonies;
- complete or partial reproductions of works of graphic or three-dimensional art intended to appear in the catalogue of a judicial sale held in France, in the form of the copies of the said catalogue made available to the public prior to the sale for the sole purpose of describing the works of art offered for sale.
- parody, pastiche and caricature, observing the rules of the genre.
- acts necessary to access the contents of an electronic database for the purposes of and within the limits of the use provided by contract.
- act necessary for a lawful judicial or administrative procedure, or undertaken for the purpose of public safety.

GERMANY

The German law (http://www.fipr.org/copyright/guide/germany.htm#_ftn17) introduced a number of exceptions and limitations to the exclusive rights to reproduce, to communicate and to make available to the public a work. These exceptions (http://www.fipr.org/copyright/guide/germany.htm#_ftn18), oblige the rights holders to allow for copies of his work in the following cases:

- Private copy: exception for digital copies for personal use fully applies but has to deal with copy protection mechanisms. The limitation for private copying (§ 53 (1) German CA) may be enforced against technological protection measures, but only in respect of reproductions on paper or similar mediums by photographic techniques. Thus, the right holder is not obliged to support the user if he or she wants to make a digital private copy of the work.
- For the uses of law enforcement and the judiciary
- For persons with a disability, in order to gain access to a work. New provision
- For the use in schools and educational institutions, but only copies of small parts of a work or of small works. Copies of school books are not allowed at all for use in school broadcasts
- For public speeches, but not for publication in monographs
- Newspaper articles and radio commentaries for inclusion in press digests
- For use in reports on current-day events. This provision was extended to cover reports in all kinds of media, including the Internet
- Citations
- For public performance, if royalties are duly paid or in the scope of beneficial events
- It is permitted to make available to the public, as much as this is required for a certain purpose and justified by non-commercial ends, of small published parts of a work, works of small size and single contributions from newspapers and periodicals, for the purpose of illustration in education at schools, universities, non-commercial institutions of education and further education and institutions of vocational training, and exclusively for a delimited group of instruction participants, or published parts of a work, works of small size and single contributions from newspapers and periodicals, exclusively for a delimited group of persons for their own scientific research

GREECE

The Greek implementation text transposed into law the following exceptions:

- Private use: it shall be permissible for a person to make a reproduction of a lawfully published work for his own private use, without the consent of the author and without payment. The term "private use" shall not include use by an enterprise, a service or an organisation.
- Quotation of Extracts
- School Textbooks and Anthologies: lawfully published literary works of one or more writers… encompass only a small part of the total output of each of the writers.
- Reproduction for Teaching Purposes: articles lawfully published in a newspaper or periodical, short extracts of a work or parts of a short work or a lawfully published work of fine art work
- Reproduction by Libraries and Archives: for a non profit-making library or archive to reproduce one additional copy from a copy of the work already in their permanent collection,
- Reproduction of Cinematographic Works: only for the purpose of preserving it in the National Cinematographic Archive
- Reproduction for Judicial or Administrative purposes: reproduction and communication to public of political speeches, addresses, sermons, legal speeches or other works of the same nature, as well as of summaries or extracts of lectures, provided the said works are delivered in public.
- Use of Images of works sited in Public Places :occasional reproduction and communication by the mass media of images, photographs sited permanently in a public place
- Public Performance or Presentation on special occasions: official ceremonies and within the framework of staff and pupil or student activities at an educational establishment.
- Exhibition and Reproduction of Fine Art Works: for catalogues and is possible to exhibit those works to the public only on the museum premises, or during exhibitions organised in museums.
- New provision: Reproduction for the benefit of blinds and deaf-mute. The reproduction of the work is allowed for the benefit of blinds and deaf-mute, for uses which are directly related to the disability and are of a non-commercial nature, to the extent required by the specific disability

ITALY

Most of the exceptions indicated in Article 5 of the Directive have been fully implemented in the Italian law. Italian copyright law already provided many of them.

- Private copy: private copying for personal use of sound and video recordings on any kind of support is allowed, as long as the copy is intended for a purpose that is neither directly nor indirectly commercial and that it is made respecting the technological measures designed to restrict acts that are not authorised by the right holder
- Reproduction and communication to public of economical, political, religious articles
- Reproduction and communication to public of works for information purposes
- Political speeches in public premises
- Use for the purposes of public security or to ensure the proper performance or reporting of administrative, parliamentary or judicial proceedings;
- Reproduction on paper or any similar medium for private use
- Reproduction for libraries, public archives and museums.

(Last 2 are both limited to the 15% of the whole work)

- Quotations for purposes such as criticism or review are allowed, but they must not have commercial purposes when performed for scientific research and teaching
- People with disability: reproduction and utilisation for communication to public of works only for personal use and of non-commercial nature and to the extent required by the specific disability
- Free communication to individuals for research and private studies purposes by dedicated terminals located in public premises: museums, libraries, etc.
- Free broadcast of reproductions from public hospitals and prisons only for internal use.

SPAIN

The draft proposed by the Spanish Government, in sections 6 to 14, presents the changes and additions to the limitations and exceptions included in the law of intellectual property of 1996. The final result is that the

suggested modifications to the reformulated text of intellectual property law (LPI 1/1996) are mainly to include all the exceptions cases that the Directive allows

UK

The new law amended the Copyright, Designs and Patents Act 1988 ensuring that UK Law complies with European Law as set out in the Directive.

In UK the exceptions to copyright are limited by the expression of the "fair dealing" which is a doctrine on the limitations and exceptions to copyright, which is found in many of the common law jurisdictions of the Commonwealth of Nation [1]. The new law main innovation states the following:

- a copy of an extract made by or for an individual from a literary, dramatic, musical or artistic work (e.g. a book chapter or a journal article, a poem, an excerpt from a musical score, or a diagram or photograph) may be made under the defence of fair dealing for the purposes of research for a non-commercial purpose or private study

  Any copying which is to be undertaken in support of commercial research or private study which is directly or indirectly connected with a commercial purpose cannot be defended as fair dealing, and in the absence of the prior permission of the copyright owner or the prior grant of a license, is likely to constitute infringement of copyright.

EUCD Most controversial provisions

The EUCD contains a Chapter entitled *Protection of technological measures and rights-management information* that obliges MS to enact effective legislation against the circumvention of any technical protection measure, and the removal DRM protection. In this respect, the EUCD stresses the importance of compatibility but does not prescribe certain standards. Rather, is addresses the industries to develop open, interoperable and compatible standards for DRMS. Though the EUCD does not introduce DRMS standards, it supports the use of DRMS by protecting technical measures, and by requiring MS to take into account the application and non-application of technological measures when providing for "fair compensation" in the context of the private use exception for which fair compensation is required. The provisions included in this Chapter are the most controversial and have generated several issues most of them still under debate. As a result the different ways in which such provisions have been implemented in EU countries and the different interpretations of the most controversial aspects have generated a quite inhomogeneous and confusing landscape causing complex consequences that can affect the way DRM system could operate.

What are TPM?

EUCD Art 6 (3)

"the expression "technological measures" means any technology, device or component that, in the normal course of its operation, is designed to prevent or restrict acts, in respect of works or other subject-matter, which are not authorised by the right holder of any copyright or any right related to copyright as provided for by law or the sui generis right provided for in Chapter III of Directive 96/9/EC."

"*technological measures shall be deemed 'effective' where the use of a protected work or other subject-matter is controlled by the right holders through application of an access control or protection process, such as encryption, scrambling or other transformation of the work or other subject-matter or a copy control mechanism, which achieves the protection objective*."

KEY POINTS

This definition of TPMs outlines that are essentially two major requirements: i) that the measure be designed to prevent unauthorised use of work, and ii) that the measure be *effective.*

[1] http://en.wikipedia.org :Fair dealing is an enumerated set of possible defenses against an action for infringement of an exclusive right of copyright.. Fair dealing cannot apply to any act which does not fall within one of these categories. In practice, common law courts might rule that actions with a commercial character, which might be naively assumed to fall into one of these categories, were in fact infringements of copyright

However the Directive does not distinguish between access and copy –control, giving equal treatment to both types of technologies. Making a clear reference to a "copy control mechanism" could be interpreted as excluding any legal protection against circumvention of TPMs that would protect exclusive rights of the copyright owners other than the reproduction right (what a bout streaming?)
Another issue arises on the interpretation of the term "effective": one interpretation of this requirement could be that TPMs that can be circumvented too easily or by accident will not qualify as an "effective" measure and therefore will not be protected against circumvention.

EUCD ART 6(3) EU members' implementation

In this section we analyze definitions of the terms "technological measures" and "effective measures" as set fort in the implementation legislation of above EU states. The definitions of these terms lead to critical consequences and to different results.

AUSTRIA
Effective copy protection measures are: *all technologies, devices and components that, in the normal course of their operation, are designed to prevent or limit the breaches of right specified in subsection 1, and which ensure achieving this protection objective.*

BELGIUM
"the technological measures are technologies, devices or components which, in the normal course of their operation, are designed to prevent or restrict acts, in respect of works or other subject-matter, which are not authorised by the right holder of any copyright or any right related to copyright."
The provision covers the devices that aim at "protecting the copyright and related rights provided for by the law. Therefore circumventing a technological measure restricting the use of public domain material is legal.
The meaning of **effective** should be related to the act of circumvention: *anyone circumventing an effective technological measure, with the knowledge or with reasonable grounds to know that she is pursuing that objective, will be liable under Articles 81 and 83 to 86 of the Belgian Copyright Law.*

DENMARK
Effective technological protection measures are any effective technological measures that, in the normal course of their operation, are designed to protect works and performances and productions, etc. protected under this Act"
As a consequence for the Danish laws, only measures that are used to prevent copying are protected. The law does not protect systems that are designed to control the user's own use of the work.
Effectiveness: the term is not clearly defined. Accordingly to the explanatory memoranda, *copy control mechanisms and the like that are incorporated in works in digital form must achieve the protection objective, and measures which are not really effective will not qualify for protection*.
It remains with the courts to make the final decision as to whether a technological measure qualifies for protection in this respect

FINLAND
TPM are *technologies, devices or components, which in the normal course of their operation serve to prevent or restrict acts in respect to copyrighted works, which are not authorised by the author or subsequent right holders*.
The protection is given to effective TM protecting a "copyright protected work". Circumvention is thus allowed if the TM protects material that is not copyrightable or has fallen into the public domain.
Effectiveness: is not clearly defined. According to the explanatory memorandum a technological measure is usually not to be deemed effective if it can be circumvented by accident.

FRANCE Provision under new project law
Protected technical measures are technologies, devices or components which, in the normal course of their operation, prevent or restrict uses, in respect of works, performances, phonograms, videograms and broadcasting programs, which are not authorised by the holder of copyright or neighbouring rights.

Relevant both for blocking the reproduction or communication act, but also preventing or restricting any act, which is not authorised by right holders.
Effectiveness: the new bill states that technical measures shall be deemed effective where the use of a protected material is controlled* through application of an access control or protection process, such as encryption, scrambling or other transformation of this protected material or a copy control mechanism which achieves the protection objective.
*(Controlled by whom? the bill does not require technical measures to be controlled by right holders)

GREECE
Protected technical measures are technologies, devices or components which, in the normal course of their operation, prevent or restrict uses, in respect of works which are not authorised by the right holder of any copyright or any right related to copyright as well as the *sui generis* right of the data base maker.
Effectiveness: when rights owners control the use of protected work.

GERMANY
Technological measures *means any technology, device or component that, in the normal course of its operation, is designed to prevent and limit actions in respect of protected works or other subject-matter protected by this law, which are not authorised by the rights holder.*
Effectiveness: still confused: the content has to be controlled through application of a mechanism, which achieves the protection objective. But another paragraph states that the technological measures are effective if the use of protected work is controlled by right holders through application of an access control: therefore the "access control" is qualified as a technological measure.

ITALY and SPAIN
Technological measures are any technology, device and component that, in the normal course of its operation, are designed to prevent or limit act in respect to protected works that are not authorised by rights holders
This definition should include both technological measures that hinder activities covered by the exploitation rights (reproduction, distribution, public communication and transformation) and measures, which control access to a work
Effectiveness: means the use of protected works controlled by rights owners.

UK
Technological measures *are any technology, device or component, which is designed, in the normal course of its operation, to protect a copyright work other than a computer program.*
The term protection of work is clarified: prevention or restriction of acts that are not authorised by the copyright owners and are restricted by copyright; use of a work does not extend beyond the scope of the acts restricted by copyright.
Effectiveness: not limited to copy protection (also the access control) and if the copyright owner controls the use of the work

KEY POINTS:

Question 1) to what extent "access control" mechanism falls under the definition of technological measures and therefore protected by anti circumvention provision?
Minimal approach (Denmark) – cut out mere access control.
Maximal approach (Italy, UK and Germany) access control technologies fall in the scope of protection.

Question 2) How to deal with the different provisions of the required "effectiveness"?
Interpretation 1) "effective" in relation their possible circumvention: measures that can be circumvented are not effective (Belgium, Denmark and Finland)
Interpretation 2) effective in relation with the control: if rights holders control the use of works/acts (Italy, Spain, and UK) or if the use of the work is simply controlled (by whom?) (France)

Question 3) Who prevails? The rights holders' authorisation or the copyright laws?
As we have seen in some countries there is no explicit reference to a copyrighted/protected work (Greece and France)

EUCD art 6 (1) and (2) TPM Legal protection

1. *Member States shall provide adequate legal protection against the circumvention of any effective technological measures, which the person concerned carries out in the knowledge, or with reasonable grounds to know, that he or she is pursuing that objective.*

Therefore not under all circumstances must circumvention be considered illegal in national law. Only if a person knows or has reasonable grounds to know that an act leads to the circumvention of a technological measure, do the Member States have to declare that act unlawful.

2. Member States shall provide adequate legal protection against the manufacture, import, distribution, sale, rental, advertisement for sale or rental, or possession for commercial purposes of devices, products or components or the provision of services which:

(a) are promoted, advertised or marketed for the purpose of circumvention of, or

(b) have only a limited commercially significant purpose or use other than to circumvent, or

(c) are primarily designed, produced, adapted or performed for the purpose of enabling or facilitating the circumvention of, any effective technological measures.

The main purpose of these criteria is to make a difference between equipment and software which can be used for circumvention, but which is also capable of other uses, which are not related to circumvention.

KEY POINTS:

There is no clear interpretation of the "limited commercially significant purposes"
Question 1) When will a device have a "limited commercially significant purpose or use" other than circumvention?

Questions 2) If a technological measure is used to hinder the reproduction of non-original material or of material fallen into public domain shall a device circumventing this measure than be allowed?

EUCD Most controversial article: interaction between protection of TPM and the exceptions

Art. 6(4)
1 Notwithstanding the legal protection provided for in paragraph 1, in the absence of voluntary measures taken by right holders, including agreements between right holders and other parties concerned, Member States shall take appropriate measures to ensure that right holders make available to the beneficiary of an exception or limitation provided for in national law in accordance with Article 5(2)(a), (2)(c), (2)(d), (2)(e), (3)(a), (3)(b) or (3)(e) the means of benefiting from that exception or limitation, to the extent necessary to benefit from that exception or limitation and where that beneficiary has legal access to the protected work or subject-matter concerned.

2 A Member State may also take such measures in respect of a beneficiary of an exception or limitation provided for in accordance with Article 5(2)(b), unless reproduction for private use has already been made possible by right holders to the extent necessary to benefit from the exception or limitation concerned and in accordance with the provisions of Article 5(2)(b) and (5), without preventing right holders from adopting adequate measures regarding the number of reproductions in accordance with these provisions.

The technological measures applied voluntarily by right holders, including those applied in implementation of voluntary agreements, and technological measures applied in implementation of the measures taken by Member States, shall enjoy the legal protection provided for in paragraph 1.

The provisions of the first and second subparagraphs shall not apply to works or other subject-matter made available to the public on agreed contractual terms in such a way that members of the public may access them from a place and at a time individually chosen by them.

Article 6(4) of the Directive addresses the interaction between the legal protection of technological measures for protection of copyright and the need for users to be able to take advantage of certain exceptions, which are allowed by Article 5 of the Directive. The aim of the article is to balance the interest of the right holders using technologies on one hand and from other hand the right given to public.

The indicated exceptions can be divided in 2 categories:

Public policy exceptions: Photocopying, copy and archive purposes of educational facilities, broadcasting own ephemeral recording, broadcasting reproduction for non commercial purposes, teaching or scientific research use, use by disabled, public safety.

The reference to these exceptions is mandatory even if the article states that member states should take appropriate measures only in absence of voluntary measures taken by rights holders including agreements.

Private copy exception: in this case the intervention of the legislator is not mandatory, but optional. Here also, the initiative lies on the right holders.

KEY POINTS

Question 1) Why only these exceptions and not for example the exception for news reporting (which also involves the freedom of information and of the press)?

Questions 2) What happens when one of the exceptions listed in art 6 has not been included in a country law?
(i.e. France has no exceptions for educational and research purpose? France is not obliged to make educational institutions benefit of an exception that does not exists in law)
Member states should intervene only for the exceptions listed in this article, but as we have seen the list of exceptions listed in art. 5 of the Directive was optional.
One problem with this regime is that not all Member States apply the same exceptions. Therefore, what is legal in one Member State will not be legal in another

Question 3) Does this mean that the exceptions provided in copyright law can be denied? Will end-user contracts be used to replace copyright law?
In fact the provision invites interested parties, such as rights holders, users, and other interested third parties (e.g., producers of consumer electronic goods), to take “voluntary measures” in order to ensure that users can benefit from certain exceptions to copyright law. This approach seems to delegate to private parties the responsibility of safeguarding the public interest.
The technological measures can override the exceptions granted to users in law, and, so have the potential to distort the balance that the law tries to achieve. This is a conflict that is so far, unresolved in European law.
The problem is that it is possible to set the TPM to such a level that some of the copyright exceptions normally available to users can be inaccessible in the encrypted publication. Although the EUCD forbids the denial of certain of the exceptions, it also excludes from this, publications licensed to users under a voluntary contract.
DRM models and licensing can specify aspects such as whether the content can be read only on screen or printed out or whether the content is tied to one machine, or can be accessed on any number of terminals; and

lists of other things the reader can and can't do with the content. The user is required to click an 'I agree' button before opening the file and the TPM software then enforces the terms of this online contract. The contracts, enforced by the TPM, can enable the rights holders to control exactly how the work can be accessed. Because different countries have differing laws on this subject, a publication can be infringing under the law of one state or country, while being perfectly acceptable in another. This tension between contract and copyright law is under discussion but unresolved worldwide.
The challenge for legislators is to maintain the balance between the interests of rights holders that need to protect their content and users that need flexible access.
Technology and the law must come together to provide the solution.

Question 4) Does any on demand service will not have to comply with the obligation to safeguard the exceptions and could be completely locked up?
As we have seen the fourth indent of 6(4) says that the provisions of the first and second indents, shall not apply to works or other subject-matter made available to the public on agreed contractual terms in such a way that members of the public may access them from a place and at a time individually chosen by them.
The wording of this provision plainly refers to the definition of the right to make works available to the public, as laid down in the Directive. Since making available works on the Internet on demand could become the prevalent business model for distribution of works the exceptions to copyright law in the online environment may be frustrated

Private copy exception: TPM and fair compensation issues

As we have seen the private copy exception is a non mandatory exception. Many European countries introduced a levy scheme for private copying. In this case the right holders cannot prohibit home copying, but they are entitled to be remunerated for private copying. Today, most continental European countries have granted authors, publishers, performers and phonogram and video producers the remuneration right for the private use of their works (so called fair compensation)
The most complex debate concerns the relation between levies scheme for fair compensation to right holders and the DRM/TPM. Right holders organisations, collecting societies, IT industries, consumers organisations and all involved stakeholders are strongly supporting their positions which can be summarised as follows showing two separate approaches[2]:

- Levies scheme should be deleted because
    - DRM technology which include technical protection measures ("TPM") and permit the licensing, monitoring, payment and control of individual usage, even if for private use only are already in place. Thus the risk is that a consumer pay twice

- Levies scheme should be kept:
    - since DRM is still at an early stage of development, no phasing out scenario can be established on the basis of the existing DRM systems.

EUCD ART 6(4) EU members implementation

AUSTRIA: Adopted the so-called "wait and see strategy" (recital 51 Directive). Right owners and users should come to an understanding on the exempted uses concerned in a reasonable time. Before no intervention is foreseen. The Austrian law does not contain any exceptions to the ban on circumventing copy protection, even for those copies that are explicitly allowed.

[2] For an exhaustive overview on the different positions : HLG report in DRM consultation

BELGIUM: "Wait and see strategy". Circumventing a technological measure in order to make a private copy, or an educational use, or a parody under Belgian Copyright Law, will be unlawful

DENMARK: Firstly voluntary measures that means: if an agreement cannot be reached the Danish law gives the users and the rights holder a right to take the case to an administrative body. "*Copyright License Tribunal may, upon request, order a right holder who applies technological measures to make such means available to a user which are necessary for the latter to benefit from the exception.*" – not applied for exception of private copy

FINLAND: Firstly voluntary measures and in case this is not possible, the draft bill provides for an arbitration procedure. Circumvention for private purposes still not define

FRANCE: Firstly voluntary measures only for the private copying exemption and for the exemption for disabled people concerning copyright and neighbouring rights, where the beneficiaries of these exemptions have legal access to the protected work or subject matter concerned. The Bill then provides for a "Mediators Board to responsible for the settlement of litigation.

GERMANY: Right holder has to help the user by providing the necessary means to enable certain permissible uses. The class of limitation on copyright are listed in German CA. Only some of these limitations apply to the digital context where TPM are of practical relevance: administration of justice and public safety, people with disabilities, collections for school or instructional use, school broadcasts and for making works available for teaching and research, personal academic use, for the inclusion of the work in personal files, if and to the extent that reproduction for this purpose is necessary and not done for commercial purposes, for personal use in teaching or for examinations.

GREECE: For teaching purposes, by libraries and archives, for judicial or administrative purposes, as well as the use for the benefit of people with disability, *the right holders are under the obligation to give to the beneficiaries the means to enjoy the benefit of the exception to the extent necessary to the extent those beneficiaries have legal access to the protected work or subject-matter.*
Should the right holders fail then the right holders themselves as well as such third parties may ask for the assistance of one or more mediators selected from a list set up by the Copyright Organisation. Applied to private copy only for the reproduction for private use on paper or any similar medium.

ITALY: Rights holders are required to adopt suitable solutions and agreements, to allow people and institutions to obtain the exceptions they are entitled to (for example, to allow visually impaired people to reproduce a protected e-book using a different format, in order to process it with a speech synthesiser). Private copy: TPM should allow people to make one private copy (even if analogue) of the works they've had legal access to, as long as it doesn't interfere with the normal use of the works themselves, and doesn't cause unjustified prejudice to rights holders. Any dispute caused by TPMs must be evaluated by the Permanent Copyright Consulting Committee.

SPAIN: For judicial or administrative purposes; for disabled people; temporary copying by broadcasting organisations, for research and for conservation purposes by certain not-for-profit establishments. If right holders do not voluntarily facilitate the exercise of those exemptions, beneficiaries of them are not allowed to circumvent the technological measures themselves. Private copy exemptions can be blocked by using technological measures.

UK: Where the application of any effective technological measure to a copyright work prevents a person from carrying out a permitted act in relation to that work, that person may issue a notice of complaint to the Secretary of State

Summarising

Public policy exceptions
- Option 1: "Wait-and-see" (e.g. Austria, Belgium)
- Option 2: Intervene to ensure that exceptions are granted
  - Mediation (e.g. Greece)
  - Administrative complaints procedure (e.g. UK)

Private copying exception
- Option 1: not allowed (most incumbent EU states)
- Option 2: granting private copying exception in one form or another
  - One (also analogue) copy (e.g. Italy)
  - One copy provided that beneficiaries of these exemptions have legal access to the protected work (e.g. France)

Article 7 Obligations concerning rights-management information

Article 7 EUCD relates to obligations concerning rights-management information. The rights management of a protected work or other subject matter includes information relating to the work or subject matter and the protection scheme. The Directive lays down provisions protecting the scheme from any unauthorised alterations or distribution. More concretely, Art 7 (1) EUCD obliges MS to "*provide for adequate legal protection against any person knowingly performing without authority any of the following acts: (a) the removal or alteration of any electronic rights- management information; (b) the distribution, importation for distribution, broadcasting, communication or making available to the public of works or other subject-matter … from which electronic rights-management information has been removed or altered without authority, if such person knows, or has reasonable grounds to know, that by so doing he is inducing, enabling, facilitating or concealing an infringement of any copyright…"* as for the definition of "rights-management information", it "*means any information provided by right holders which identifies the work... the author or any other right holder, or information about the terms and conditions of use of the work or other subject-matter, and any numbers or codes that represent such information."*

Art 8 Sanctions and remedies

1. *Member States shall provide appropriate sanctions and remedies in respect of infringements of the rights and obligations set out in this Directive and shall take all the measures necessary to ensure that those sanctions and remedies are applied. The sanctions thus provided for shall be effective, proportionate and dissuasive.*

2. Each Member State shall take the measures necessary to ensure that right holders whose interests are affected by an infringing activity carried out on its territory can bring an action for damages and/or apply for an injunction and, where appropriate, for the seizure of infringing material as well as of devices, products or components referred to in Article 6(2).

Art 8 states that "Member States shall provide appropriate sanctions and remedies in respect of infringements of the rights and obligations set out in this Directive. In this context it is important to remark that the recent IP Enforcement Directive below analysed (Directive 2004/48/EC of the European Parliament and the Council of 29 April 2004 on the enforcement of intellectual property rights) creates a powerful new enforcement measures across Europe to ensure higher and harmonised level of protection of IP rights in European common market.
Even though the EUCD gave MS the possibility to introduce criminal action the majority of MS have mainly introduced civil actions. However the EUCD creates – at least – the means for rights holders to take civil action.

In following sections we propose a general analysis on the different regimes of sanction that mentioned states have put in place in order to comply with the EUCD art 8.

EUCD ART 8 EU members implementation

Austria: In concordance with Austrian legal tradition, the main effect of these provisions is in the field of civil law focussing on "*prevention and elimination of the circumstances in contradiction with the law"* .The new provisions protecting technological copy protection mechanisms and rights management information have been included in the catalogue of copyright infringements punishable with up to six months in jail or a fine.

Belgium: There is a penal sanction in the new proposed Belgian text dedicated to the circumvention of technical protection measures and the import, distribution etc. of circumvention devices.

Denmark In Denmark, the circumvention of TPMs as well as the trafficking in circumvention devices can be punished under civil and criminal law. The penalty for violation on effective technical measures and on rights management information is a fine. Imprisonment for these acts in Denmark is not possible

Finland: Both penal sanctions and civil remedies are available. New penal sanctions are introduced

France: The bill states that it is a copyright infringement to knowingly damage a technical measure while aiming at altering the protection provided by this measure

Germany: In addition to civil sanctions, German laws indicate some of the prohibited acts to be criminal offences, punishable with imprisonment. Germany makes a distinction between the circumvention of TPMs (imprisonment up to one year or a fine) and the trafficking in circumvention devices (imprisonment up to three years in case of professional purposes or a fine. However in Germany no criminal sanctions are applied in case the act has been exclusively performed for, or in relation, to private use by the offender or individuals personally connected with him.

Greece Activities in violation of the provisions related to the technological measures are punishable by imprisonment of at least one year and a fine of at least. In case the infringer commits the illicit actions on a professional basis or the circumstances under which such actions were committed show that the transgressor represents a particular danger to intellectual property rights, the penalties are further raised to a minimum 10 years of imprisonment, a fine of 14,673 € up to 58,694 € and revocation of the license of the enterprise through the medium of which the illicit acts were committed.
Punishment of the infringers requires criminal intent (of any degree) on the part of the transgressor, so that acts committed by negligence are not punishable under penal law.

Italy: The penalties for infringing copyrights and circumventing controls are provided in new law following Italian implementation. The penalties for commercial purposes are the same as the old Italian copyright law, but have been extended to the new felonies introduced by the Directive (the commercial manufacture, import, distribution, etc of devices, products or components or the commercial provision of services with the aim of facilitating the circumvention of TPM and the removal of rights-management information, when made for commercial non-personal purposes, and the commercial distribution, importation for distribution, broadcasting, communication or the act making available to the public works from which electronic rights-management information has been removed or altered). The implementation adds a new section introducing new sanctions (monetary) for some infringements made for personal and non-commercial purposes.

Spain: The Spanish draft does not propose any concrete penalties for infringing copyright or circumventing controls. It is establishes that the Commission on Intellectual Property as the legal body to intervene in cases

of property rights conflicts and technological protection measures. The Minister of Culture, upon a proposal of the Commission can legally impose sanctions and penalties.

UK: In the UK, there are no criminal sanctions for the circumvention of TPMs as long as it is conducted for private and non-commercial use. The UK also has a special Article in which is stated that the infringement that occurs in the course of business or "to an extent that prejudicially affects the right holder" can be qualified as a criminal offence

KEY POINT:

The short analysis reported above, shows that sanctions and remedies taken by EU member states have been interpreted in different ways. Significant differences seem to remain with regard to the interpretation of the MS obligation to provide "appropriate sanctions" (Art 8 (1)). While, except Greece, all countries imposed civil sanctions (but entity varies in each country), for the violation of anti circumvention provisions, differences remain with respect to the criminal sanctions. Main differences are below summarised:

Option 1: For any acts of circumvention (e.g. Greece), imprisonment and fines
Option 2: imprisonment and fines only for acts of circumvention for non-private and commercial uses (e.g. U.K. Germany)
Option 3: No imprisonment, only fines for acts of circumvention (e.g. Denmark)

The different approach of the UK and German laws could cause significant consequences. As an example and infringing entity would not have to fear in the case of violation for private use under, says UK laws, he would face a fine or even jail in Greece under the same scenario.

Overview of other relevant Directives

C) EU Directive 48/04 on the Enforcement of intellectual Property

The European Union directive on Measures and procedures to ensure the enforcement of intellectual property (Directive 2004/48/EC) adopted on April 2004. The Directive enforces that member states have to introduce measures which are normally only applied for counterfeiting of physical goods to all kinds of Intellectual Property Rights possibly even including secret information. These measures include very detailed requirements for third parties to provide information on possible infringements, raids undertaken by private companies without warning and freezing of bank accounts without warning The Directive proposes that almost all the enforcement measures available to IP owners in any member state must be available in all of them, and that the application of the criminal law to IP enforcement be made very much broader. The directive has been welcomed by the music and film industries but it divided computer industry and telecomm industry.

Directive aim:

This Directive is different respect previous European legal norms in the field of Intellectual Property Law, as the harmonisation is not limited to a branch of Intellectual Property Law like copyright. The Directive principally applies to any infringement of intellectual property rights as provided for by the Community legislation and/or by the national laws of the Member States (patent law[2], utility model law copyright law etc.) The objective of the Directive is to approximate the legislative systems so as to ensure a high, equivalent and homogeneous level of protection across the Internal Market (recital 10).
The Directive foresees **four main categories of civil measures** that can be sought by the beneficiaries in case of IP-infringements:

- measures for protecting evidence of IP infringements (Art. 6, 7)

This provision aims to solve the situation in IP infringement cases where decisive evidence is under the control of the infringer himself and/or is easy to remove. The Directive permits judicial authorities, on application by a claimant, to order that specific evidence, which is under the control of the opposing party, be produced by that opposing party (Art. 6). Additionally, and even before the commencement of proceedings, courts are able to take prompt and provisional measures to preserve relevant evidence for the enforcement of IPR rights (art 7)

- measure protecting the information right about the source and distribution channels of infringing goods and services (Art. 8)

This provision has been under discussion during the process of legislation by right holders, providers, users and their associations (http://www.ipr-helpdesk.org/newsletter/16/html/EN/IPRTDarticleN10AA2.html#n9). The right of information enables claimants to request an information order from the competent court against the infringer or other persons, who have demonstrably and on a commercial scale come into contact with the infringing goods and services or provided commercial services used in infringing activities (Art. 8(1)). This obliges the concerned persons to give information on the origin and distribution networks for the good and services

- provisional measures for the preventing infringements and for protecting the claims for damages (Art 9)

These measures, which can be ordered by the judicial authorities at the request of an involved person, are created to prevent further infringements of intellectual property rights and to secure the recovery of damages in advance of a final judgement.

- compensation and corrective measures following a judicially determined IP-infringement (Art.10 to 13), in particular regarding enforcement and the amount of civil damages.

The Enforcement-Directive clearly establishes that the infringer only has to pay civil damages appropriate to the actual prejudice suffered by him as a result of the infringement. The judicial authorities are allowed to set the damages by taking into account all appropriate aspects, such as negative economic consequences, including lost profits which the injured party has suffered etc or - in appropriate cases – they can fix damages as a lump sum on the basis of elements such as the amount of royalties or fees which would have been due if the infringer

Controversial issues:

Subject to controversial discussions has been the question of whether the measures and procedures provided by the Directive should also apply to infringements caused by consumers or private persons – which would include Internet file sharing and P2P (*). Following final version the procedures and measures provided for can, in principle, also be used against private persons and end-consumers.
(*) http://www.ipr-helpdesk.org/newsletter/16/html/EN/IPRTDarticleN10AA2.html#n6

Positions:
Telecoms operators and Internet companies fear that ordinary people could be prosecuted. “It inappropriately mixes civil and criminal enforcement measures together with new substantial law, causing the risk that individual Internet users are treated in an unjustified manner as pirates (ETNO position). They argue this could be intimidating to consumers and act as a deterrent for consumers to take up broadband Internet or third generation mobile phone services that are soon expected to become profitable.

Rights-holder organisations welcome the Directive and even underline that the IPR Directive is still not going far enough and push for tougher measures to fight against "piracy epidemic".

Major software companies such as Microsoft (Windows) who suffer from illegal copying have been backing the directive. But small and sometimes even bigger ones such as Sun Microsystems and the free software community have opposed it for fear that they might be driven out of the market.

Consumer organisations such as BEUC have given strong warnings that the *directive "would allow consumers to be prosecuted, judged and condemned as harshly as a person making and selling millions of copies of CDs"*.

The Directive has not been implemented already and Member States have until 29 April 2006 to bring their legislation in line with the directive's provisions.

D) The E-Commerce Directive

The EU Directive 31/2000 (the 'E-Commerce directive') adopted in June 2000, requires Member States to harmonise certain aspects of their laws on buying and selling online service and content.
The Directive has been implemented in 12 Member States (exceptions: France, the Netherlands and Portugal); the Directive applies to both businesses and consumers, and is intended to provide a coherent structure of rules to be observed by entities doing various online businesses and to ensure a high level of consumer protection.

The most discussed issue regards the **liability of online service providers**. The Directive establishes an exemption from liability for intermediaries where they play a passive role as a "*mere conduit"* of information from third parties and limits service providers' liability for other "intermediary" activities such as the storage of information.

The Directive also clarifies that the internal market principle of **mutual recognition of national laws** and the principle of the country of origin must be applied to information society services.

Other central issues:

- **Place of establishment**: The Directive defines the place of establishment as the place where an operator actually pursues an economic activity through a fixed establishment, irrespective of where web sites or servers are situated or where the operator may have a mailbox.
- **Transparency**: The Directive requires Member States to oblige information society service providers to make available to customers and competent authorities (in an easily accessible and permanent form) basic information about their activities (name, address, e-mail address, etc).
- **Online contracts**: The Directive requires Member States to remove any prohibitions or restrictions on the use of electronic contracts. In addition, it imposes certain information requirements for the conclusion of electronic contracts in particular in order to help consumers avoid technical errors.

In relation to contracts, the Directive aims to:

- require Member States to adapt their national laws to ensure that e-contracts have the same legal status as traditional contracts;
- ensure that all e-contracts are based the "*full and informed consent"* of the parties; and
- specify the information, which must be communicated by the provider of goods or services prior to conclusion of an e-contract.

The Directive states that, in the absence of contrary agreement by business parties, information must be provided that explains:

- the technical steps required to conclude the contract;
- whether the contract is filed and accessible;
- the technical means for correcting input errors prior to concluding the contract;
- Sigma the languages offered for contracting.

There is an important exception to the requirement to provide the information set out above: it does not apply to contracts concluded *by way of exchange of e-mail or "equivalent individual communications"*. It should also be noted that any standard terms provided to the recipient must be made available to allow for storage and copying.

The draft Directive had initially attempted to define when certain e-contracts had been concluded. The final version of the Directive has dropped this approach and this leaves open the possibility that different national laws approach this issue differently.

E) The Distance Selling Directive - governing B2C contracts

A special word or warning is due with regard to e-contracts where one party is a consumer. The Directive 7/97 on the protection of consumers in respect of distance contracts governs consumer agreements where the parties are not physically present and is therefore of direct relevance to e-contracts. An electronic supplier will, prior to concluding a contract, need to display specified information which includes:

- its name and postal address;
- the characteristics of the relevant goods/services and their price;
- any delivery costs and payment terms;
- an express right of withdrawal from the contract (normally 7 working days);
- a statement as to how long the offer/price remains valid;
- information on complaints and after-sales service.

Among others, the right of withdrawal may pose serious practical problems, as the provider will be obliged to reimburse sums received. Fortunately, the right does not apply in certain circumstances, such as where performance of the contract has begun or goods made to specification.

In addition requirements include that:

- the supplier confirms in writing information already given to the consumer and provides additional information, including the procedure for cancelling the contract;

- there be a contractual cooling off period enabling the consumer to cancel the contract by notice, and for restoration of goods on cancellation;

- contractual performance be rendered within 30 days, subject to agreement; and

- the consumer has a right to cancel payment where there is fraudulent use of the consumer's payment card in connection with a distance contract.

F) The Database Directive 96/9

The Directive "concerns the legal protection of databases in any form" (Article 1.1).

Article 1.2 defines the Directive's object of protection:
"'Database' shall mean a collection of independent works, data or other materials arranged in systematic or methodical way and individually accessible by electronic or other means".

Thus, a `database' is more than a mere collection of simple data. Which Databases Are Protected? A database, which will benefit from legal protection "*may include any type of information, such as text, sound, images, numbers, facts, or data.* It is for this reason that commentators have also referred to the Directive as the "Multimedia Directive. To be protected, the contents of the database must be "individually accessible." Electronic and print databases are covered. Electronic media specifically include CD-ROMs, CD-I, and

online services. The extension to print databases is a significant expansion from the earlier drafts of the Directive, which only covered electronic databases

.

The individual elements of the database must be "arranged in a systematic or methodical way" The Explanatory Memorandum excludes from the definition of a database "the mere storage of quantities of works or materials in electronic form".

However, according to Recital 21, "*it is not necessary for those materials to have been physically stored in an organized manner".* It follows that a collection of unassorted data fixed on a hard disk or other digital medium would qualify as a database if combined with database management software enabling retrieval of the stored data.

The elements collected in the database must be `individually accessible by electronic or other means'. In other words: the stored works, data or other materials must be retrievable. Not every collection of works, data or materials is a database within the meaning of the Directive. The collection of moving images together constituting a movie (film) is not a `database The Directive does not, however, protect the computer software driving the database as such (Article 1.3). The Software Directive of 1991 protects computer programs.

Databases enjoys copyright protection only if "by reason of the selection or arrangement of their contents, [they] constitute the author's own intellectual creation" (Article 3 .1).

Article 5 enumerates the rights protected under copyright: a broadly phrased right of reproduction (including "*temporary or permanent reproduction by any means and in any form, in whole or in part*"), rights of adaptation, distribution (subject to Community exhaustion), and communication to the public.

The Directive allows for all exemptions traditionally found in the copyright laws of the Member States (Article 6 .2 d). However, unauthorized copying for private purposes from *electronic* databases is not permitted. This is a very wide protection - for example simply searching a database electronically may involve the temporary copying of the database to another medium and thus may constitute a restricted act. Restricted acts are allowed where the user has been licensed to use the database or is otherwise a lawful user, when it is for teaching or scientific research but not commercial research and where it is for public security, administrative or judicial purposes. Thus copyright protects the author's own intellectually creative selection or arrangement of the contents of a database whereas the database right protects the investment of the database maker in the obtaining verification or presentation of the contents of a database.

Sui generis right

The EU Database Directive establishes an entirely new intellectual property right, called a "*sui generis" right.* The *sui generis right* is defined in Article 7 .1 as a right "*to prevent extraction and/or reutilization of the whole or of a substantial part, evaluated qualitatively and/or quantitatively, of the contents of that database. D*atabase makers can, for a period of 15 years from the completion of the database, prevent unauthorized extraction and re-utilization of the contents of the database. The *sui generis* right adds an extra layer of protection, which may cumulate with existing rights of intellectual property. The Directive defines the owner of the *sui generis right* as the "maker of a database" (Article 7 .1). Pursuant to Recital 41, the "*maker of a database is the person who takes the initiative and the risk of investing*."

Extraction is defined as "*the permanent or temporary transfer of all or a substantial part of the contents of a database to another medium by any means or in any form*". The right pertains to the downloading, copying, printing, or any other reproduction in whatever (permanent or temporary) form.

Reutilization is defined as "*any form of making available to the public all or a substantial part of the contents of a database by the distribution of copies, by renting, by on-line or other forms of transmission*." The Directive does not define a `substantial part', an omission that has been criticized. According to the Explanatory Memorandum "*no fixed limits can be placed in this Directive as to the volume of material which can be used".*

The taking of insubstantial parts of the database does not infringe the *sui generis right*, unless this is committed in a "*repeated and systematic*" manner to the detriment of the database producer (Article 7 .5).

Exceptions to the *sui generis right* are stipulated in Article 9. Member States may stipulate that lawful users of a database which is made available to the public in whatever manner may, without the authorization of its maker, extract or re-utilize a substantial part of its contents: (a) in the case of extraction for private purposes of the contents of a non-electronic database; (b) in the case of extraction for the purposes of illustration for teaching or scientific research, as long as the source is indicated and to the extent justified by the non-commercial purpose to be achieved; (c) in the case of extraction and/or re-utilization for the purposes of public security or an administrative or judicial procedure.

Duration

The duration of the extraction right is 15 years from the date of completion of the making of the database (Article 10 .1), or if later, the first making available to the public (Article 10.2). In practice, most databases will be protected for a much longer period. According to Article 10. 3, "*any substantial change, evaluated qualitatively or quantitatively, to the contents of the database, including any substantial change resulting from the accumulation of successive additions, deletions or alterations, which would result in the database being considered to be a substantial new investment, evaluated qualitatively or quantitatively, shall qualify the database resulting from that investment for its own terms of protection*". Thus, a regularly updated database is awarded *permanent* protection.

Implementation overview

Article 189 of the EC Treaty leaves Member States the freedom to choose the means of implementing a Directive. Member States have chosen to deal with the *sui generis right* either in a special section of the copyright law or in a special law. Member States were to implement the provisions of the Directive by 1 January 1998. Only a handful states have met this deadline. In some Member States implementation bills are still pending in national parliaments. The Database Directive has effect not only in the European Union, but also in the entire European Economic Area. Eventually, the Directive will be implemented in some 30 European states.

Deadline 1 January 1998
Met by Sweden, Germany, UK, Austria, France (partly)
Spain, Finland, Denmark, Belgium (1998)
Italy, Netherlands (1999)
Greece, Portugal (2000)
Iceland, Luxemburg (2001

Main differences:

Germany: original databases as subcategory of compilations; sui generic right is considered a neighbouring right
UK: databases are treated as a subset of the category of literary work; sui generis right, called a *database right*, is defined as a property right. Typically, many of the recitals of the Directive have been transposed into material provisions of the law
Nordic countries (Denmark, Finland, Iceland, Norway and Sweden): respective laws contain provisions expressly protecting non-original compilations of data, such as catalogues, tables and similar compilations, provided they comprise "a large number" of items. For the Nordic countries, therefore, the Database Directive is of only limited consequence.
Spain/Italy: the Database Directive was implemented amending the Law on Intellectual Property. The Act closely follows the wording of the Directive. The copyright provisions of the Directive are integrated in the copyright Law. The sui generis right is regulated together with existing neighbouring rights.

Exceptions copyright
Lawful user: only authorised by contract (FR), or also by law (BE)
Lawful use exception not transposed (FI, SE)
Exception for private use not limited to off-line (GR, LU)
Exception for education not transposed (FR, GR)

Exceptions Sui generic right
Lawful use not transposed (LU)
Lawful use not limited to insubstantial parts (Nordic countries)

Restricted acts copyright
Temporary reproduction not expressly mentioned (AT, BE, DK, FI, DE, ES, Nordic Countries)
Exhaustion not provided (FR, LU)
Exhaustion not limited to off-line distribution (DE, PT

Restricted acts sui generis right
"extraction" and "reutilisation" not used (DE, Nordic countries)
Temporary transfer not covered (AT, DE)
Exhaustion not limited to off-line distribution (PT)
SG right on insubstantial parts not transposed (FI, SE)

Main issues

- Overlapping of laws: the two rights, copyright and database right, protect different or potentially different people - the 'maker' of the database can claim the protection of the database right whereas the 'author' (a term which acknowledges creativity) may be able to claim the protection of copyright. There is no need to register either right. The two rights also run for different periods of time. Copyright runs for 70 years from the end of the year of the author's death whereas the database right runs for 15 years from the end of the year of completion of the database.
- The Directive has been the basis for the EC position in the WIPO talks and deliberations. Some critics of database protection claim that the new laws actually prevent access to some information, and this has led to a series of discussions with, in particular, the USA. The USA has several bills pending (HR 1858 and HR 354), but currently relies on copyright law and state laws regarding misappropriation to protect databases.
- The Directive explicitly excludes subcontractors from the definition of "database maker." It makes it clearer that EU companies which subcontract for data entry keying to companies located in places such as the Philippines, China, and India still are considered the database maker for purposes of the Directive. On the other hand, it makes it more difficult for companies located outside the EU to claim EU residence by subcontracting to companies located in the EU.
- One of the most controversial aspects of the Directive is that database makers must be nationals of a EU Member State, or have their habitual residence in the Union, in order to obtain the benefit of the sui generis right.
- The Directive leaves it to Member States to provide for exceptions to this right member since the exceptions to the sui generis right are somewhat narrower than the "fair use" defences to copyright infringement, the sui generis right provides more protection to database makers than the copyright regime does for copyrightable materials.

In Article 7.3 of the Directive it is mentioned that the sui generis right can be transferred, assigned or granted under contractual licence. This Article has given the excuse to say that this Directive leads to the introduction of the concept that contract law is stronger than copyright law. In the EU, only the UK copyright law (common law) provides for the possibility where contracts can override copyright law. Copyright laws, which are based on the concept of droit d'auteur, provide for a stronger protection to copyright law above contract law.

4.1.2 IPR management aspects and issues

a) Copyright and Exclusive Rights

Copyright is the right to which the creator of a literary, scientific or artistic work is entitled in his or her immaterial, i.e. intangible work; the catalogue of works ranges from text via sounds and images to embrace computer programs and databases. Comparable with a property right in a material object, copyright has been structured by the legislature as a so-called exclusive right. Hence, it is solely for the creator of a work to decide whether - and if then in which manner - he or she wishes to exploit the work and who should be excluded from such exploitation.
In addition to authors, other natural and legal persons who engage in activities within the culture business also enjoy legal protection. Specific protections have been set up to protect the rights of performers in their performances, the rights of producers of sound recordings in their sound recordings and the rights of broadcasters in their signals. These rights are said to be "neighbouring rights" to copyrights, because the three categories of beneficiaries do not create works; rather, they use the works of others as raw material for the purpose of communicating by various means. These related (or neighbouring) rights must also be taken into consideration when analyzing the implications of digital technology for the exploitation of protected works and achievements.

The following table shows the categories and examples of works of authorship. The granting of copyright has nothing to do with the artistic value or fineness to be found in them. If they express original thoughts or sentiments of the creator without copying those of others, such things are also protected as works of authorship.

Categories and examples of works of authorship

Literary Works:	speech, treatise, essay, novel, scenario, poem, lecture, etc.
Musical Works:	musical composition, lyric with music, etc.
Choreographic Works & Pantomimes:	choreography of dance, ballet, pantomime, etc.
Artistic Works:	painting, engraving, sculpture, cartoon, calligraphy, stage setting, etc. including industrial arts
Architectural Works:	architecture (Blueprint belongs to figurative works.)
Map and Figurative Works:	plan, chart, model, etc. of scientific nature and map
Cinematographic Work:	movie, fixed TV program, video, etc.
Photographic Work:	photo, gravure, etc.
Program Works:	computer program

Other categories of works made from original works

Derivative Work:	a work created by translating, musically arranging, cinematizing, transforming, or otherwise adapting a pre-existing work
Compilation:	collection of works and/or data such as encyclopaedia, dictionary, newspaper, journal and anthology
Database:	collection of works and/or data the information in which can be searched for and read with the aid of a computer

What Rights Are Granted to Authors?

Moral rights: exclusively personal to the author, (the "inalienability" of moral rights). As moral rights are of personal nature and non transferable, they are exhausted at the death of the author, however, moral interests of the late author are protected to some extent by the Copyright Laws even after his/her death.

Economic rights: can be transferred by sale, assignment, succession, etc. partly or totally. Therefore, if an economic right is assigned to someone, the assignee will become the "copyright owner" although the original author continues to be the "author" with moral rights.

Moral rights

Right for authorship:	the right to control the act of indicating the name of the author in terms of whether any name should be indicated, whether the name should be the true name or pseudonym, etc.
Right for integrity:	the right to control the act of distorting, mutilating or modifying a work

Economic rights:

Right of reproduction:	the right to authorise or prohibit the act of making copies of a work by any means: printing, photography, reprography, sound recording, visual recording, downloading, etc.
Right of communication	the rights to authorise or prohibit any communication to the public of the originals and copies of their works It includes the right to making available to the public their works in such a way the public may access them from a place and at a time individually chosen by them (e.g. Internet, public performance, broadcasting, interactive on-demand)
Right of distribution	the exclusive right of distribution to the public of their works or copies. This distribution right is exhausted where the first sale or other transfer of ownership in the Community of a copy is made by the right holder or with his consent. This provision does not apply to on-line (i.e. relevant only to tangible objects).
Right of adaptation:	the right to control the act of adapting or transforming a work by such means as translation, musical arrangement, transformation, dramatisation, etc.

Neighbouring Rights of performers and producers of phonograms

Moral rights of performers (introduced by WPPT)
Economic rights to both categories.

Moral rights of performers

Right of authorship:	the right to control the act of indicating the name of the performer
Right of integrity:	the right to control the act of distorting, mutilating or modifying performances in a manner prejudicial to the performer's reputation

Economic Rights of Performers and Producer of Phonogram

Live Performance (only performers)

Right of fixation:	the right to control the act of recording live performances
Right of making available	the right to control the act of making available live performances (Internet broadcasting, webcasting, etc.)

Fixed Performances/phonogram

Right of reproduction:	the right to control the act of making copies of fixed performances /phonograms
Right of making available:	the right to control the act of making available fixed performances/phonograms
Right of transfer of ownership:	the right to control the act of publicly transferring ownership of fixed performances/of phonograms (with exhaustion)
Remuneration right for communication to public	the right to receive equitable remuneration for any commercial use of fixed performances/phonograms (i.e. broadcasting or communication to the public).

Rights of broadcasters

Right of fixation:	the right to control the act of fixing transmitted programs whether broadcasts are transmitted by wire or over the air, including by cable or satellite.
Right of reproduction:	The right to control the act of making copies of fixed programs whether broadcasts are transmitted by wire or over the air, including by cable or satellite.
Right of making available:	the right to authorize or permit the making available to the public, by wire or wireless means, in such a way that members of the public may access them from a place and at a time individually chosen by them
Right of retransmission:	the right to control the act of re broadcasting or diffusion

Rights expiration

Authors (artistic, literary, music, dramatic, film, etc)	o 70 years after the death of the author; o work of joint authorship, 70 years after the death of the last surviving author o In the case of anonymous or pseudonymous works, 70 years after the work is lawfully published.
Performance:	50 years from the end of the year in which the performance was fixed in a phonogram.
Phonogram:	50 years after the first fixation 50 years from the date of the first lawful publication 50 form the first lawful communication to the public USA: term of protection of phonographic producers has

	been extended to 95 years
Database collections	Full term of other relevant copyrights in the material protected. In addition, there is a database right for 15 years.
Program of broadcasting	50 years after the transmission

Issues of rights expiration

The length of copyright protection varies according to factors including:

- Different national legislation;
- The type of creative work;
- Whether it has been published or not
- The date of publication.

As reported above the duration of authors rights (life plus 70 years) has become the global benchmark since it was adopted by the European Union. However also in Europe there are some exceptions: France uniquely extends the EU period with provision for the *annees de guerre*: extra time for the First World War (considered to have lasted from 1914 to 1919) and the Second World War (1939 to 1948). France also adds a further thirty years for an author who "died for France".Outside the EU former USSR states often have a similar provision: for the works of authors active during the Great Patriotic War (1941-45) the protection in Russia is for example prolonged by four years.

The below table demonstrates that for example the law of copyright duration in the U.S. is in unduly complex. One can identify categories of works that might clearly be in the public domain, but other categories of works will depend on individual investigation of the circumstances of their creation, publication, and compliance with notice and registration requirements. Further, this addresses only U.S. copyright law. Some works may be subject to other legal conditions to their use, such as a person's right of privacy, or a business's trademark interests. Uses of works outside the jurisdiction of the United States will also implicate other countries laws.

Copyright Term and the Public Domain in the United States 1 January 2005[3]

UNPUBLISHED WORKS

Type of Work	Copyright Term	What was in the public domain in the U.S. as of 1 January 2005
Unpublished works	Life of the author + 70 years	Works from authors who died before 1935.
Unpublished anonymous and pseudonymous works, and works made for hire (corporate authorship)	120 years from date of creation	Works created before 1885.
Unpublished works created before 1978 that were published after 1977 but before 2003	Life of the author + 70 years or 31 December 2047, whichever is greater	Nothing. The soonest the works can enter the public domain is 1 January 2048
Unpublished works created before 1978 that were published after 31 December 2002	Life of the author + 70 years	Works of authors who died before 1935.
Unpublished works when the death date of the author is not known	120 years from date of creation	Works created before 1885.

[3] This chart was first published in published in Peter B. Hirtle, "Recent Changes To The Copyright Law: Copyright Term Extension," *Archival Outlook,* January/February 1999. This version is current as of 1 January 2005. The most recent version is found at http://www.copyright.cornell.edu/training/Hirtle_Public_Domain.htm

WORKS PUBLISHED IN THE US

Date of Publication	Conditions	Copyright Term
Before 1923	None	In the public domain
1923 through 1977	Published without a copyright notice	In the public domain
1978 to 1 March 1989	Published without notice, and without subsequent registration	In the public domain
1978 to 1 March 1989	Published without notice, but with subsequent registration	70 years after the death of author, or if work of corporate authorship, the shorter of 95 years from publication, or 120 years from creation
1923 through 1963	Published with notice but copyright was not renewed	In the public domain
1923 through 1963	Published with notice and the copyright was renewed	95 years after publication date
1964 through 1977	Published with notice	95 years after publication date
1978 to 1 March 1989	Published with notice	70 years after death of author; if work of corporate authorship, 95 years from publication, or 120 years from creation
After 1 March 1989	None	70 years after death of author, or if work of corporate authorship, the shorter of 95 years from publication, or 120 years from creation

In U.S. all terms of copyright run through the end of the calendar year in which they would otherwise expire, so a work enters the public domain on the first of the year following the expiration of its copyright term. For example, a book published on 15 March 1923 will enter the public domain on 1 January 2019, not 16 March 2018 (1923+95=2018).

Identity of Rights Owners

AUDIO

Possible owners of audio assets include:

- Author/Composer
- Phonographic Producer
- Performer(s)
- Licensee (licensed in various markets)
- Sub publisher (in various markets)

FILM/TELEVISION/VIDEO

Possible owners include:

- Producer
- Production Company
- Performer(s)

- Composer/publisher of scores
- Distributors (of various markets)
- Actors
- Screenwriter
- Director
- Publishers of underlying text/book

STILL IMAGES
Possible owners include:

- Photographer
- Artist
- Publisher (if book cover)
- Person represented in image (rights to privacy/publicity)
- Company owning photo (Film studio/television station)
- Company with rights to license digital reproductions

TEXT
Possible owners include:

- Author
- Publishers
- Sub publisher

Multimedia content

The creation of a multimedia product such as an electronic book or interactive game can be a complex legal endeavour. Because multimedia products often embody a vast collage of written, audio and visual materials, in many cases created or controlled by third parties, the rights acquisition process can be an analytical and organizational challenge and a time- consuming, expensive component of the overall development project. Critical elements of the content acquisition process include:

- evaluating the product carefully and thoroughly to identify and classify all elements of content
- deciding systematically which of those elements may require third party licenses or releases
- tracking down the persons or entities with authority to grant the rights needed
- negotiating the necessary licenses and other agreements.

It is not at all uncommon for dozens of separate agreements, if not more, to be required for the development of a single multimedia product.
Since several categories of works can be incorporated into one new media product, the applicable protections could vary from one element to another.
Here are some examples:

A recent photograph of a very old painting. The photograph (artistic work) is protected, whereas the painting (another artistic work) is no longer protected. The rights in the photograph will have to be cleared.

The recording of a recent musical arrangement of a symphony from the last century. The new musical arrangement constitutes an adaptation protected by copyright (new musical work) of a work in the public domain. Performances by performers are also protected (rights of performers). The sound recording of the new work is also protected (rights of the producer of sound recordings). The rights will have to be cleared with the sound recording producer, and with the performers, if the contract between them does not transfer

relevant rights to the sound recording producer.

A sound recording made in 1945, incorporating songs by authors who are still alive. The sound recording is no longer protected (50 years after fixation); the songs, however, still are. Like the sound recording, the performances of the performers are no longer protected (50 years after fixation). Clearance will therefore have to be obtained from the owners of the rights in the music.

A magazine page that contains photographs, text and drawings. Separate rights adhere to the magazine page as a whole (compilation of various works), the photographs (artistic works), the drawings (artistic works) and the text (literary works). It will be necessary to contact the owner of the rights in the magazine to find out what rights he acquired in each of the components from their respective owners and whether he is in a position to grant the relevant clearances. If not, it will be necessary to contact each owner directly or other rights holders.

B) Rights management overview

The management of intellectual property rights can involve a menu of rights, a variety of administrative devices, and many kinds of parties–both individual and organisational. While the menu of rights and the range of administrative devices are relatively similar between countries, the diversity of parties potentially involved in the management of intellectual property rights can differ from one country to another as can the particular function or set of functions that these management organisations perform. In the digital era, the ubiquity and worldwide scope of electronic distribution networks, the increasing production of multi-media works, the ease and speed of technologically assisted reproduction, and the overall financial stakes involved have increased both the complexity of and the necessity for effective rights management.

Rights management elements

Rights management involves many elements and tasks. These elements include:

- the type of rights involved
- the range of management tasks

Type of Right

Depending upon the type of creative work involved, the bundle of rights might not only include reproduction rights (including derivative works), but also performance rights, mechanical rights, and synchronisation rights. Many of these rights are managed by collecting societies.

The range of management tasks

The collective rights management involves a number of tasks ranging from public registration, to licensing, monitoring use, fee collections, royalty distribution, application service provision, policy advocacy, policy and standard development, etc. Usually no one collective rights management organisation performs all these tasks. For example only with regards to music IPR there are different types of organisations having different functions:

- Authors and publishers collecting societies which both license mechanical and performance rights (such as SIAE in Italy)
- or two separate collecting such as in UK for the two different licenses
- Performing rights organisation (for licensing public performance rights of copyright owners)
- Mechanical rights organisations (for licensing mechanical rights of copyright owners)
- Phonographic producers rights collecting societies (in some countries more than one such as in Italy SCF and AFI)
- Performers rights collecting societies

Furthermore, the management tasks vary from one country to another, as does the complement of various types of organisations.

European Music Authors Composers and Publishers collecting societies

• Austria AKM	http://www.akm.co.at/
• Belgium SABAM	http://www.sabam.be/
• Bulgaria MUSICAUTOR	
• Croatia HDS	http://www.hds.hr/main/default_en.htm
• Czech Republic OSA	http://www.osa.cz/titul.php?jazyk=en
• Denmark KODA*	http://www.koda.dk/
• Estonia EAU	
• Finland TEOSTO*	http://www.teosto.fi/
• France SACEM	http://www.sacem.fr/
• Germany GEMA	http://www.gema.de/
• Greece AEPI	
• Hungary ARTISJUS	
• Ireland IMRO	http://www.imro.ie/
• Israel ACUM	http://www.acum.org.il/
• Italy SIAE	http://www.siae.it/
• Lithuania LATGA	http://www.latga.lt/
• Netherlands BUMA *	http://www.bumastemra.nl/
• Norway TONO *	http://www.tono.no/
• Poland ZAIKS	http://www.zaiks.org.pl/
• Portugal SPA	http://www.spautores.pt/
• Romania UCMR	http://www.ucmr-ada.ro/
• Slovakia SOZA	http://www.soza.sk/
• Spain SGAE	http://www.sgae.es/
• Switzerland SUISA	http://www.suisa.ch/
• Sweden STIM*	
• U.K. PRS *	http://www.prs.co.uk/

***only performing rights**

European Music Publishers Mechanical Rights Organisations

• Netherlands STEMRA	http://www.bumastemra.nl/
• Scandinavia Nordisk Copyright Bureau (NCB) - Denmark, Finland, Norway and Sweden-	http://www.ncb.dk/
• U.K. MCPS	http://www.mcps.co.uk/

Music producers and performers rights collecting societies

Austria IFPI Austria (International Federation of the Phonographic Industry)
Austria VDFS
Belgium IFPI Belgium
Belgium URADEX performers rights
Croatia IFPI
Croatia HUZIP performers rights
Czech Republic – IFPI
Czech Republic INTERGRAM performers rights
Denmark GRAMEX performers and producers rights
Finland GRAMEX performers and producers rights

France SCPP producers rights (mainly majors)
France SPPF producers rights (SMEs and independent producers)
France ADAMI performers rights
Greece IFPI
Greece APOLLON performers rights
Germany IFPI
Germany GVL performers rights
Hungary IFPI
Hungary EJI performers rights
Ireland IRMA Irish Recorded Music Association
Ireland PPL Phonographic Performance Ireland
Ireland RAAP performers rights
Italy SCF producers rights (mainly majors)
Italy AFI producers rights (SMEs and independent)
Italy IMAIE performers rights
Netherlands SENA performers rights
Netherlands IFPI
Norway FONO independent producers rights
Norway GRAMO producers and performers rights
Poland ZPAV producers rights
Poland STOART performers rights
Portugal AFP producers rights
Portugal GDA performers rights
Spain AFYVE producers rights
Spain AIE performers rights
Sweden IFPI
Sweden SAMI performers rights
UK PPL Producers and performers rights
UK PAMRA Performing Artists Media Rights Association

Reproduction rights organisations:
Members of IFRRO, The International Federation of Reproduction Rights Organizations (RROs). These organisations are set up jointly by authors and publishers and represent them both equally. Most RROs (68%) administer reprographic rights for all types of works. Only a few, such as Germany, have three different bodies, which handle reproduction rights for texts, visual material and musical works separately. Around half of the RROs analyzed have been granted the right to administer public lending rights (52%). Sixty percent of the RROs administer digital rights. Less than half (48%) of the RROs deal additionally with other rights, like rental rights, cable retransmission rights, broadcasting rights and communication to the public rights.
All European RROs are non-profit organizations. The formation of an RRO usually be approved by a public body (86%).
Authors and publishers grant and withdraw mandate (permission) to RROs individually to administer their reprographic rights. Generally, the RRO is granted either a non-exclusive mandate (32%), or an exclusive mandate (68%) that provides the rights holders with an opportunity to withhold works or rights from the mandate. In 35% of the countries RROs are also granted rights by law. However, most frequently an exclusive right is granted to the RRO by the individual rights holders themselves (53%).

Foreign rights holders are represented by all RROs through bilateral agreements. RROs treat national and foreign rights holders equally. RROs conclude both Type A and Type B reciprocal agreements. The former is more frequently used (65% concluded more Type A agreements than Type B agreements). Type A implies exchange of both rights and revenues collected, while Type B agreements are an exchange of repertoire, but no transfer of collected revenue.

In six countries an extended collective license – or obligatory collective management of the reproduction rights – has been established, and in thirteen countries there are legal licenses to support at least part of the RROs activities. In nine countries (41%) the user is offered both transactional and blanket licenses. However, in most countries (54%) licenses are limited to blanket licensing. Tariffs are usually fixed by negotiations. In some countries, approval of the tariffs by the authorities is needed (35%). In 25% of the countries the tariffs are fixed by the legislation.

In some countries, rights holders have decided against collecting data on photocopying directly from users, and thus, a distribution method has been developed based on the availability of the material in the market. The rights holders report to the collecting society when their works have been published and are compensated for probable copying of the work. There are also countries where rights holders have opted for non-title specific distribution of remuneration. Surveys are designed to collect generic, non-title-specific information regarding the volume of copying of the type of material and categories of publications, rather than identifying the specific publication, author and publisher that have been photocopied.
Levies on reprographic equipment and/or an operator levy are covered by legislation in 16 EU countries (70%) and one country outside the EU. The equipment levy generally applies to all photocopiers (76%). In many countries faxes, scanners and multifunction machines are also levied. The standard use covered by the levy is private use (80%). Moreover, in nearly half of the countries research use, educational use and library use are also covered.[4]

IFRRO European members:
AIDRO, Associazione Italiana per i Diritti di Riproduzione delle Opere dell'ingegno Italy
Bonus Presskopia Sweden
CEDRO, Centro Español de Derechos Reprográficos Spain
CFC, Centre Français d'exploitation du droit de Copie France
CLA, The Copyright Licensing Agency Ltd. United Kingdom
COPY-DAN Writing Denmark
CopyRo Societate de Gestiune Colectiva a Dreptunior de Autor Romania
CopyRus – Russian Rightsholders' Society on Collective Management of Reprographic Reproduction Rights Russian Federation
HARR, Hungarian Alliance of Reprographic Rights Hungary
ICLA, The Irish Copyright Licensing Agency Ireland
KOPINOR Norway
KOPIOSTO Finland
Literar-Mechana Austria
LUXORR, Luxembourg
OSDEL, Greek Collecting Society for Literary Works Greece
ProLitteris Switzerland
REPROBEL bcvba- scrl, Belgium Belgium
Stichting Reprorecht Netherlands
VG Bild-Kunst, Verwertungsgesellschaft Bild-Kunst Germany VG WORT, Verwertungsgesellschaft WORT Germany

Collective Licensing Terms

- Rights holder Agreement – an agreement between an individual rights holder and a collecting society (usually only under voluntary licensing) for a collecting society to represent that rights holder works for collective licensing
- Mandate – the authority of a collecting society to represent rights holders and their works for collective licensing given by law, by the rights holders individually or as a whole, or by rights holders' organisations

[4] http://www.ifrro.org/show.aspx?pageid=home

- Repertoire – Complete list of works managed by a collecting society and owned by its members .The repertoire of a collecting society also includes the complete list of works of every other collecting society (of same category) based on which a bilateral agreement has been signed
- Blanket/Repertory license – Authorisation granted to user that may use any or all the works within the "repertoire" or collection of many works according to the conditions and terms of the license.
- Non-voluntary licensing – Licensing that is obtained through national legislation, in which the consent of the rights holder is not required but for which the rights holders have a right to remuneration.
- Legal license/Obligatory Collective License – non-voluntary license in which permission of the use is granted by law. These legal licenses can be divided in two categories:
    a) Compulsory license – a non-voluntary license or legal license in which the royalty rate is determined through negotiations between the rights holders (or their representatives) and the users
    b) Statutory license – a non-voluntary license or legal license in which the royalty rate is determined by the legislation

Examples of music compulsory license is the "mechanical license" (explained below) that covers songs recorded for a record written by someone else and the "blanket license" for the public performing rights (see below public performance rights)

Extended collective license

The essence of such a system is that, if there is an organisation which is authorised to manage certain rights by a large number of owners of rights and, if it is sufficiently representative in the given field, the effect of such collective management is extended by the law also to the rights of those owners of rights who have not entrusted the organisation to manage their rights

c) Licensing and rights clearance of Musical works and Sound Recording

At the outset it is important to distinguish between **publishing rights in a song,** and **rights in a sound recording** that may embody the song. When we hear a song on the radio, two separate and distinct intellectual properties are involved that need to be identified and understood. The first property is the music composition, itself (the lyrics and music composed by the songwriters). The second property is the sound recording—the physical embodiment of sounds resulting from the recorded performance of that musical composition. In most cases, a user will have to consider obtaining separate rights for both the use of the music composition and the sound recording.

MUSICAL WORKS

Music Publishing rights

In order to facilitate the exploitation of music, the songwriter/composer generally transfers the publishing rights to the publisher pursuant to a music **publishing agreement** that assigns the copyright to the music publisher, which then shares publishing income with the songwriter and composer as stipulated in the agreement. To assign this copyright to a third party music publisher it is essential in most countries that such a music publishing agreement has to be written. However not all music publishing agreements involve a transfer of copyright. Some contracts are 'administration deals' only where the publisher will receive a percentage of the income generated by the song catalogue for undertaking certain necessary tasks (administration, registration, monitoring and royalty collection).

(It has to be notice that the actual term 'music publishing' is derived from the traditional business of printing sheet music. Before sound carriers were even invented music publishers were already active in the mass production of sheet music. The generic expression 'music publishing' has continued through to the present day although, in practice, printing sheet music is now only one smaller aspect of the work of the modern music publisher. Nowadays music publishing encompasses the whole area of administering and exploiting musical works, not just print rights.)

Mechanical Rights

The right to reproduce and distribute to the public a copyrighted musical composition on phonograms (in any material object in which sounds are fixed, except those accompanying audiovisual works and motion pictures (see "synchronisation rights," in next section) is **called the mechanical right**.

Licenses granted to the user to exploit the mechanical rights are called mechanical licenses. Once the copyright owner of a musical composition authorises the public distribution of phonograms embodying the composition for the first time, anyone else may then also record that musical composition and distribute phonograms of that new recording by following the procedure established by national legislation, that require paying a statutory royalty for each record manufactured and distributed. This is called a compulsory license. Publishers utilise collecting societies to handle mechanical license grants on their behalf. In short, mechanical right allows the owners of the copyright in music works to claim royalties when their works are *recorded*. The word "mechanical" comes from the use of a mechanical device to play the music works.

In the United States mechanical royalties are paid at the statutory rate (statutory license). In Europe and other countries of the world, mechanical royalties are calculated differently

Synchronisation Rights

The **right to record a musical work** in synchronised relation to the frames or pictures in an audiovisual production, such as a motion picture, television program, television commercial, or video production, is called the **synchronisation (or "synch") right**. There is no compulsory license for this right; it is subject to the licensor and licensee reaching mutual agreement as to terms. In addition to mechanical rights, some European collecting societies are starting to represent many music publishers in handling synchronisation licensing.

Public Performance Rights

Performance and broadcasting income is a key source of income for the songwriter and publisher. Every time a copyrighted work is broadcast, or performed in public, it should (theoretically) generate income. Public performance licenses, not surprisingly, allow the licensee to publicly perform musical compositions. Because of the tremendous demand to play music publicly and the difficulty that would be involved in entering into separate agreements each and every time a particular work is performed, copyright owners almost universally delegate the right to grant public performance licenses to "performance rights organisations" (collecting societies)

Small performance rights include concert and other so-called "live" performances, incidental and background music on television programs and radio airplay. A grand right covers performance of music in a dramatic setting or, in any way, it directly advances the plot of the production in which it is included.

Collecting societies offer so-called "blanket" licenses of their entire catalogue, licenses for a particular production or so-called "per-program" licenses and individual licenses. Public places that play music must pay for this performing right (in this case 'blanket' licenses are therefore issued for this purpose). Internet sites, which play copyrighted music also require performing rights licenses.

SOUND RECORDING

The term Master owner refers to owner of the original, produced recording of a song (on a tape or other storage form) from which a record company makes CD's or tapes which it sells to the public.

Because the Master embodies creative material from a number of different persons, it can be complicated to obtain the proper clearances

Whether the songs included on the Master are written by the by a songwriter/composer a **mechanical license** is required to reproduce the songs.

If the song is written by the recording artist (or musical group), that license is either included in the **recording agreement** or the rate(s) at which such license must be issued is specified.

Reproduction Rights
"Master recording rights" or "master use rights" are required to reproduce and distribute a sound recording embodying the specific performance of a musical composition by a specific artist.

Synchronisation rights:
You may want to use a particular recording of a musical work — that is, to dub directly from an existing sound recording. In this case there are two copyrights to consider, and two copyright owners — copyright in the musical work and copyright in the recording/phonogram.
If the owner of the Master does not also own the copyright in the musical work embodied in the recording, then while the Master owner would have the right to license the Master to be used as part of a movie or television soundtrack, such license does not include synchronisation rights of the musical work, and the licensee must obtain the consent of the publisher. Thus, in order to synchronise Frank Sinatra's recording of "Strangers in the night" in a film soundtrack, the film company would need **two synchronisation licenses** from both the music publisher of the song and the owner of that specific Sinatra sound recording. The synchronisation license for the use of recorded music is granted by individual sound recording owners.

The neighbouring rights of performers and producers of phonograms to obtain remuneration for broadcasting or the communication to the public of phonograms
Sound recording producers and performers enjoy the right to remuneration when sound recordings/fixed performances are communicated to the public (including played on radio or on the Internet). This right to remuneration is administered by collecting societies who undertake the collection of these royalties and their distribution to their members.

USA: in United States sound recording copyright owners historically had not enjoyed a public performance right. In 1995 Congress passed the **Digital Performance Rights in Sound Recordings Act** (amended later by the Digital Millennium Copyright Act), which provides sound recording copyright owners with the exclusive right to "perform their works publicly by means of a digital-audio transmission." That means sound recording copyright owners finally can be compensated, in the form of a freely negotiated license, for public performances of their recordings under certain conditions. However this right applies only to digital transmissions publicly performed (it does not cover live performances or CDs played in public nor analogue transmissions such as AM or FM radio)

Fair compensation for private copying
Private copying levies were introduced in the 1960s and have been since established in different ways in many European countries. They were introduced to compensate right holders for reproductions made for private use ('private copying').
Private copying is a limitation to the exclusive reproduction rights of authors, performers and producers. The Copyright Directive (2001/29/EC) to some extent harmonises the scope of the private copying limitation across Europe, where no commercial aims are pursued and fair compensation is provided to the right holders.
The EUCD 29/01 Directive private copying (Art. 5.2(b)),
Berne Three-step test: Private copying must be compatible with the so-called *Three Step Test*. (in particular private copy exception cannot prejudice the normal exploitation of the work or the phonogram or videogram)
Fair compensation: In certain cases of exceptions or limitations, right holders should receive fair compensation to compensate them adequately for the use made of their protected works or other subject-matter. The Directive leaves open to Member States to introduce or maintain a levy system, but does not oblige them to do so
Relation with TPM: The level of fair compensation should take full account of the degree of use of technological protection measures referred to in this Directive.
***De minimis* rule:** in certain situations where the prejudice to the right holders would be minimal, no obligation for payment may arise. For example time shifting' (i.e. the recording of radio or television broadcasts for later consumption) would qualify as such a situation.

DRAMATIC WORK:
Choreography, pantomimes, plays, treatments, and scripts prepared for cinema, radio and television. Generally, dramatic works such as plays and radio or television scripts are works intended to be performed including spoken text, plot and directions for action.

Collective management societies administer rights in dramatic works by negotiating a general contract with the bodies representing theatres. In the dramatic field and although there are exceptions, the collective management organisation acts more as an agent representing authors. Collecting societies negotiate with representatives of theatres on the terms for the exploitation of dramatic works. This contract specifies the minimum terms for the exploitation of particular works The author authorizes the performance of each play through an individual contract containing the author's specific conditions. The collective management organization then notifies the user of the authorization and collects the royalties on behalf of the author.

LITERARY /TEXT

Collecting societies also administer the right of reprographic reproduction of literary and text including music scores and lyrics. With regards books, magazines, newspapers, or the lyrics of songs, collective administration mainly involves the grant of the right of reprographic reproduction, by which institutions such as libraries, public organisations, universities and schools are allowed to photocopy protected material. Authors' societies tend to administer this right.
The collective management of reprographic reproduction rights is usually done under the non-voluntary licensing arrangements. Under such arrangements, institutions such as libraries, public organizations, universities, schools and consumer associations, are allowed to photocopy printed works such as books, newspapers, magazines, reports and the lyrics of songs against the payment of equitable remuneration. The collective management organization collects and distributes this remuneration.

AUDIOVISUAL WORKS

The rights management of audio-visual works - feature films, short films, TV films, serials, cartoons and works involving multimedia and still images – can be compared to that of music.
On behalf of audio-visual creators, the collective management society negotiates general representation contracts with broadcasters like television stations, cable networks and satellite packages.
Societies may also assist individual authors negotiate production contracts for cinema, TV, radio and multimedia, providing them with standard contracts, for instance.

MULTIMEDIA WORKS

On account of growing popularity of "multimedia" productions, there is a growing tendency to set up new agencies. These agencies are a sort of coalition of separate collective management organisations, offering a centralised source where authorisations can be obtained easily and quickly. This to suit users in the multimedia field, where the majority of productions are composed of, or created from, several types of work, which require a wide variety of authorisations.

D) Impact of new technologies on collective rights management

The basic idea behind the development of DRM is to facilitate the licensing and acquisition of copyright or neighbouring rights through technical means, while also preventing by such means premium content from being used without authorisation. Nowadays many rights are directly licensed by right holders to the users (as distributors) but as we have seen certain categories of rights or mass use of protected matter, e.g. for multi-repertoire licensing in the area of music, are authorised and remunerated through collective management organisations.

Today, the management of intellectual property rights are in flux and the stakes involved are much greater than ever before. Among significant changes we can include the expanding scope of the rights management task and the complexity of rights management organisations
Technologies have contributed significantly to expand the scope of rights management in two ways. First, as they generate a new category of intellectual property rights--digital rights. These digital rights not only exhibit aspects of long-established rights (e.g., to copy, to perform, or to use in derivative works), but also constitute a new phenomenon in which the very essence of these activities takes on different meaning. Today with digital technology, virtually anyone can easily make unauthorised but perfect and low cost copies of recordings, films, books, and other intellectual property. Thus, the right to control and collect the rewards of reproducing the first--or original--copy has been radically transformed. Secondly, the tasks of licensing and monitoring all types of intellectual property rights has become more complex as the variety of legitimate uses has multiplied, as technology has made it both easier to monitor use and to exercise unauthorised use, while the value of intellectual property increases. Another key issue is related to the growing number and complexity of collecting societies as for their different role and categories of rights owners represented. So the question is how all the actors involved in the digital environment and the DRM proposed systems would be integrated into a coherent management rights system?
The Santiago Agreement: publishers collecting societies have signed a supplementary agreement to the existing agreements of reciprocal representation, the so-called "Santiago Agreement" (CISAC Congress 2000 in Santiago de Chile), and on the basis of this the collecting societies can grant licenses also for works of their sister societies for the use of music on the Internet even beyond their respective administrative areas (i.e., to avoid any doubt worldwide) Therefore content provider intending to offer its services worldwide on the Internet should not be expected to conclude licensing agreements with every collecting society in every country where its musical services are offered or presented online The Santiago Agreement contains the following five important principles: (1) licensing to the content provider. (2) The license is to be granted by the collecting society of the country in which the content provider has its usual place of business. 3) The content provider is granted the license worldwide on a non-exclusive basis.

KEY POINTS

Multiplicity of right holders
As we have seen simply for the use of sound recording many rights are involved and as a consequence several different licenses are to be issued (individual licenses as well as non-voluntary license with different collecting societies). This issue is more complicated in the case of a multimedia content where many rights holders may be involved. In addition, copyright rights are routinely transferred (e.g. from an author to a publisher, or from one publisher to another). It is a must for copyright-management system to know who owns the right to authorise the use of a work in whole or part at a particular point in time and then possibly also who may be entitled to a share of the royalties.

The new dimension of the rights involved

In the digital environment both moral rights and economic rights are involved.
Moral right issue: How should moral rights, be managed once a work is exploited throughout the digital cross media domain?
It is important to remember that, when copyright holders license or assign their copyright, they still retain the moral rights. In terms of the right of paternity, the creator (s) is not always guaranteed that the work will be credited to her or him. For example, in an interactive CD-ROM, the multiplicity of works included means that crediting creators becomes problematic as well. With respect to the right that allows the creator to prevent the mutilation, destruction or modification of an existing work, given the ease with which works can be modified with digital technology, moral rights could become crucial in new media to an extent that they were not in non-digital media.

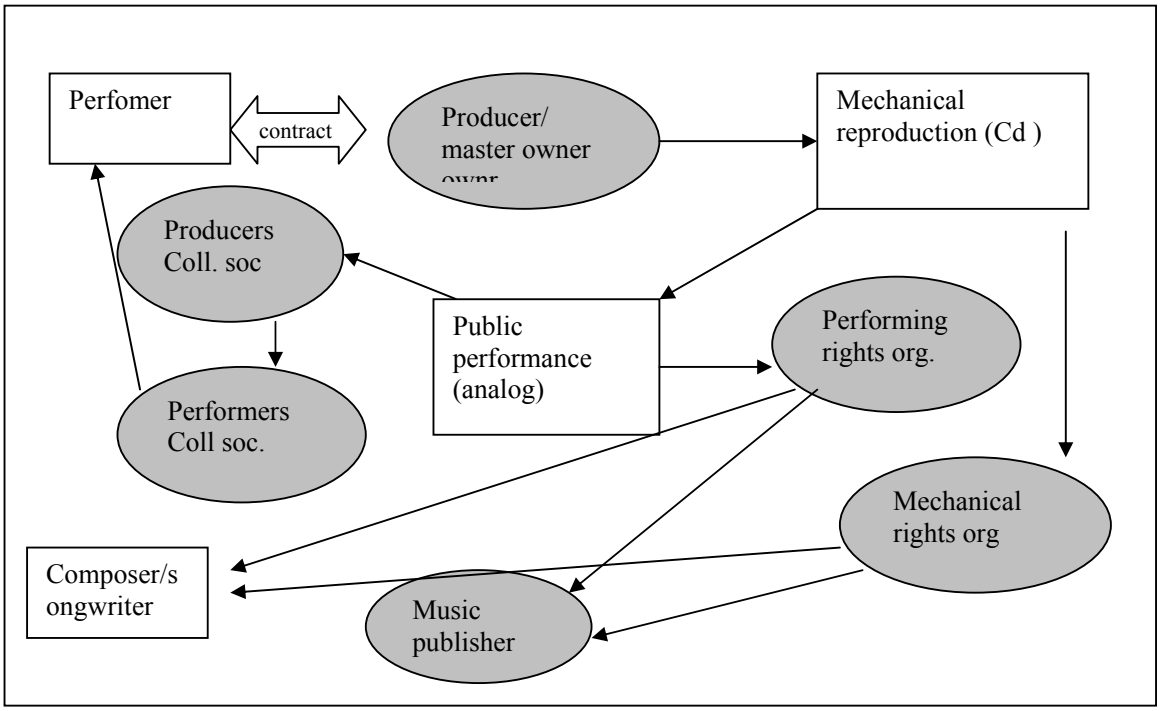
Economic rights
Before the digital distribution of music over the Internet, the difference between a reproduction and a performance of music was usually clear. Now the music transmitted over the Internet does not always fit

within these distinct categories. Often, both rights are involved when music is transmitted digitally through new media. Thus, the distinction between listening to and purchasing music becomes difficult in the digital environment.
Again, this is a quite relevant issue because, as we have seen rights holders are not necessarily the same regarding the performing rights and mechanical rights, and in some cases it is not even the same collecting society that administer the two categories of rights.
For the most part, online music is still separated into two categories: streaming and downloadable files
Streaming. Analysis here is problematic not only because of the law's complexity but also because of interpretation issues and the pace at which technology evolves**. Two streaming types** are common on the Internet: **Webcasting, which is essentially Internet radio**, and **posting,** which lets Web site visitors hear a posted audio file by opening it (i.e. to preview music for promotional purposes)

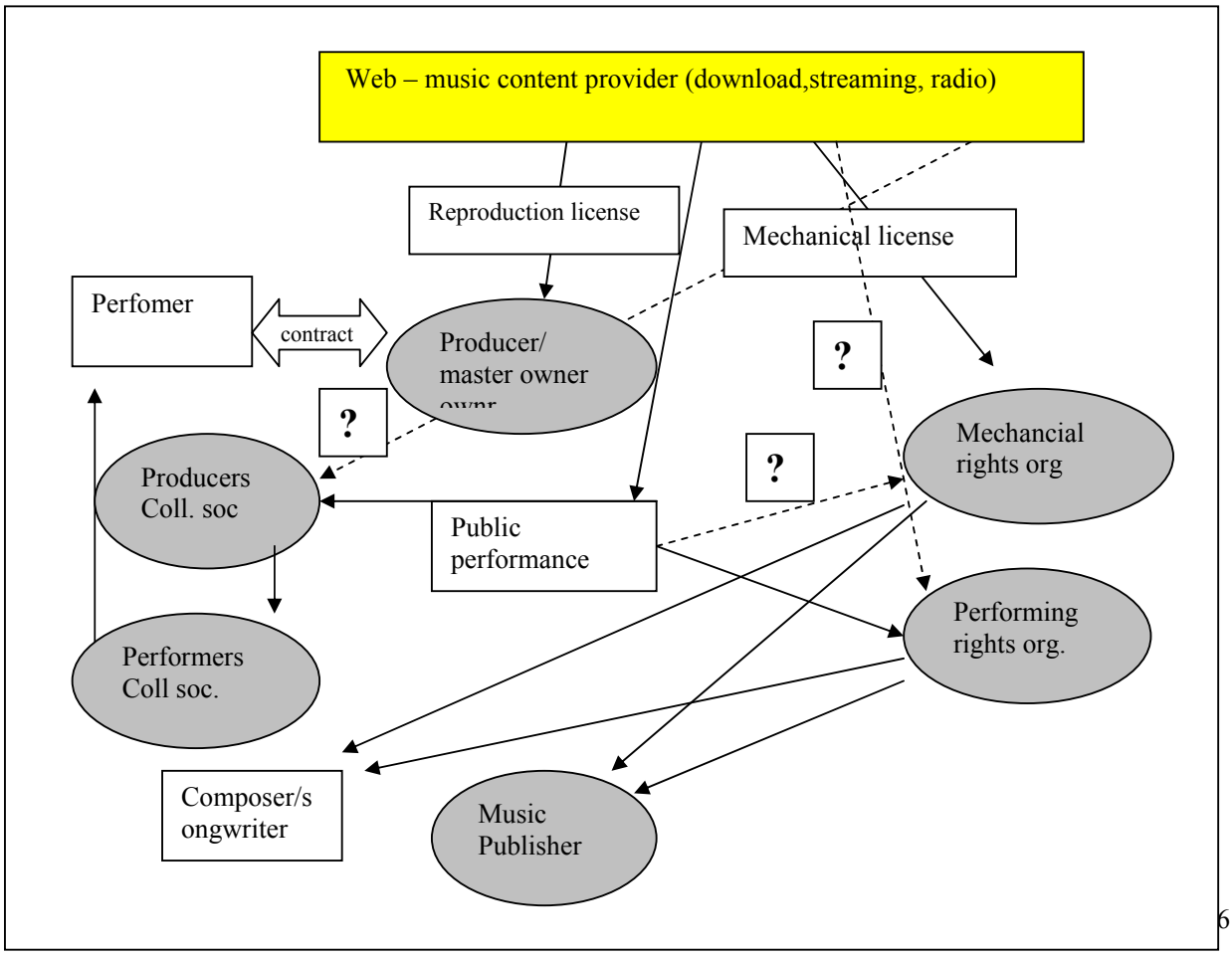
Reproduction/mechanical rights: Regarding on-line delivery and other kinds of downloading of music, the mechanical right is involved as digital copies, are to be considered as "mechanical reproductions (EUCD Directive reproduction act comprise direct or indirect, temporary or permanent reproduction by any means and in any form in whole or in part). License for the digital downloads of copyrighted musical works contained on a digital sound recording is issued by mechanical rights organisation (collecting societies). License for the reproduction of sound recordings are obtained directly from the owners of the sound recording. However many collecting societies believe that all kind of transmissions also constitute public performances. Therefore the performing right is also involved in case of on-line delivery, but this is not necessarily the case all over the world. In this context, producers, collecting societies and record companies have not yet taken a clear position on the necessity of obtaining a license for the right to reproduce a sound recording in connection with Internet streaming

Public performance rights; for the on-line radio and television and other kinds of streaming, the performing right seems to be involved. (However there is a distinction between web casting and posting).
Many collecting societies request the need to obtain a mechanical license for any copying that occurs through the process of transmitting a musical composition (such as from a server computer, as well as for any subsequent permanent and/or temporary copies made in the process of transmitting the audio from the host website to the end use).
The result is that a website wanting to make music available by digital transmission over the Internet has to obtain several separate licenses.
Still the clearance of producers and performers rights in connection with the on line public performance of sound recording is a complex task.
Example: You want to use Franks Sinatra's version of the Beatles' "something" on your web site. You should get the **public performance licence of the composition (i.e. by PRS in UK).** You then have to get the MCPS license for the **mechanical rights** (the download and distribution of the composition over the internet). You still need to obtain **reproduction licensing** from the master owner (record company xxx), which owns the rights to the sound recording itself. Lastly you should obtain licensing for **public performance of the sound recording** (i.e. **PPL**). These are the rights that must be obtained before using the tune on your website.

Current music licensing structure- non digital (simplified on delivery and reproduction)



Music licensing structure in the digital context: a confused scenario



The licensing parties

In the on line environment most rights holders today agree that the licensee must be the content provider who has the highest degree of control over the contents of the web site. It has to be noticed that under the Santiago Agreement a national based provider would have to be classified as a content provider and the foreign subsidiary as a service provide. From the point of view of the collecting societies in the interest of their members, the relevant definition in the Santiago
Agreement about the content provider must not be interpreted other than objectively, nor must they be at the users' disposal. The users would otherwise be able to transfer the function of content provider for a certain music offer to another company just as they pleased and in whatever country they liked. However it has to be noticed that some collecting societies (i.e. in US) have, on the other side, chosen to focus on the service or access providers who have the subscription agreements with the Internet end-users.

The applicable law

This question is rather complex and difficult. Which country's copyright law applies to an on-line transmission between two countries? Is it the law of the country from where the transmission originates, i.e. the country of origin or is it the law of the countries in which the transmission is received, i.e. the country of reception? There are arguments for both options, and there is yet no agreed international solution. The laws that take precedence are those of the country where the user is located. But that location is not always evident .As we have seen in the music field, the collecting societies representing authors and publishers disagree among themselves. US societies want to license in the country where the server is located, while their European counterparts prefer to license in the country of the content provider, which may or may not be in the same country as the server.

The applicable laws and the exceptions

The way member states comprise a closed list of exceptions are rather different as different are the content of such lists. In Europe, exceptions to copyright are largely diverse and not harmonised Depending on which law applies, an act may or may not require an authorisation or may or may not be covered by a compulsory license or equitable remuneration scheme.

4.1.2.1 License/standard contracts analysis

The voluntary licensing framework

The assignment of copyright.
Assignment is essentially a transfer of rights. It is just like a sale of the rights. Thus, one should always beware of assigning one's rights as it means ownership of them (and usually control as well) is transferred (i.e. composer/publishers contracts and artists/ producer contracts)

Licensing structure and elements

When a rights holder grants a license, he or she permits another to use the right but retains ownership and thus a certain control over that right. Licenses allow the usage to be limited to the real needs of the licensee. It also means that right holders don't lose total control of its rights.
In the case of copyrighted material, it must be remembered that one party has exclusive right (s) over the work and the other party requires access to the work in order to fulfil its mission.
The following list identifies the principal elements that may be covered by the contract:
Generally, a license agreement consists of clauses that deal with:

The Parties
Recitals
Definitions
The Agreement's purpose
The Rights granted under the License
Usage Restrictions
Territory
Term
Exclusivity
Delivery and Access to the Licensed Materials
License Fee
Licensee's Undertakings
Warranties Indemnities
Force Majeure
Assignment and sub contracting
Jurisdiction
Signatures

After giving details of the parties, there is usually a set of paragraphs called recitals. The recitals summarise what is intended to be achieved by the contract. Recitals are not part of the contract itself. Their aim is to give a brief overview of the objectives of the parties and to give the context in which the contract was originally written. They may be used of the contract requires interpretation as a result of a dispute.

Definitions

Legal contracts require the use of precise wording. Thus, where concepts are complex or it might take some time to explain a short phrase, a word is chosen as shorthand to signify them. A subtle change in the meaning of a definition can have a significant impact through the whole contract.

The Agreement's purpose

This is the heart of the contract and summarises what is being provided for the price. Anything that is not included won't be provided in the price and may have to be negotiated for an extra fee.

Scope of the user license / the Rights granted under the License

The contract will stipulate whether an assignment or a user licence is sought. It should be noted that the owner of the rights is not able to transfer more rights than he owns. If the licensee wishes to obtain certain rights, he must clear them with the owner of those rights. Therefore this clause determines what licensee is allowed to do with the Licensed Materials. Anything that is not mentioned here will not be allowed, unless re-negotiation or acquisition of extra rights under a further license. The list of activities can be long or short depending on the aims for which the license is required- (for example, the right to reproduce and adapt an extract with a view to incorporating it in an interactive CD-ROM, communicating it to the public by telecommunication, distributing it and making derivative products). It is important to underline that statutory rights already granted by national copyright laws or by international treaties are not negotiable. Therefore these rights should not be listed in the license, but many parties prefer to include them for convenience.

Usage Restrictions

These clauses define what is not allowed to do with the Licensed Materials. The most common usage restrictions are:

- substantial or systematic reproduction
- re-distribution, re-selling, loan or sub-licensing
- systematic supply or distribution in any form to anyone other than to Members of the institution

Territory
You can license someone to use your right in a particular territory but retain the rights to certain other territories. The license should specify the territory where the licensed material will be exploited - for example, the world, North America, Europe, etc.

Term
The term of a contract refers to the duration of the contract. The term of the assignment or the user license should be stated, as well as the renewal conditions, as the case may be. In this regard, it is of course a good idea to take into account the term of the protection that remains until the work falls into the public domain. The license can only be "cancelled" before the end of the term if there is a fundamental breach of the license or there is some other provision allowing for earlier termination (such as insolvency). Licenses can be as long or as short as the parties decide. Under the general law, a contract may be terminated at any time if other party defaults by failing to perform any obligations on its part.

Exclusivity – non-exclusivity
In practice, an exclusive license is very similar to an assignment. The granting of non-exclusive licenses makes it possible for several people to exercise the same rights simultaneously within the same territories.

Delivery and Access to the Licensed Materials
It is important to be as precise as possible about the date of delivery of the Licensed Materials, their frequency, the format and media. To avoid the risk of later dispute the license should specify clearly what these are. .

License Fee
Depending on the circumstances, the financial consideration could be paid in a lump sum, an outright fee or a royalty representing a percentage (i.e. on gross revenue or net revenue on the retail price if copies of the licensed material are to be sold), in can also be a combination of fee and royalties. Eligible deductions should be specified. Payment of royalties must include a reporting. In many cases, there is a provision for an advance but it has to be negotiated case by case. However the choice of the license fee (amount and condition) depends on what sort of deal in involved, who is the licensor and who is he dealing with.

Licensee Undertakings/obligations
When is included this provision states that licensee undertakes that neither it nor its users will infringe copyright or any other proprietary rights by for example, modifying, adapting, transforming, translating and creating derivative works of the Licensed Materials or parts of it. The licensee also undertakes that it will use or allow its users to use the Licensed Materials in accordance with the terms and conditions of the license.

Warranties and Indemnities
A warranty is a statement or representation that certain facts are true. Important warranties include that the goods and/or services will perform as promised in the agreement .The warranty provision for example states that the licensor has the rights and the authority to grant the license. If a license has no warranty clause or a warranty clause that is ambiguous. An indemnity is one party's agreement to insure or compensate the other party against losses and expenses resulting from failures in performance under the contract.

Force Majeure
A force majeure is a condition beyond the control of the parties such as war, strikes, destruction of network facilities, etc. not foreseen by the parties and which prevented performance under the contract. Most licenses states that failure to perform term or condition by any party under the license due to a force majeure will be excused and will not be deemed a breach of the Agreement.

Assignment and sub-contracting
This provision gives the licensee the right to assign its rights under the contract to third parties. In most jurisdictions, commercial contracts are not easily assignable. The case law on assignment is complex and not always certain. In many licenses is clearly indicated that the license may not be assigned to any other natural or legal person without the prior written consent of the other party.

Jurisdiction & Venue:
Since state law governs contracts, they will normally provide that any disputes under the contract are governed by a specific state's laws. A fundamental clause in this section is the national law chosen for the interpretation of the license and the court chosen for submitting a claim. Most licenses choose the national law most suitable to the licensor.

4.1.2.1.1 Licensing in the music sector

The below tables summarise some types of the music contracts analyzed respectively issued with the music publisher and with the master owner.

Contracts can be short or long depending on various aspects and on the chosen form. However in all circumstances, the rights holder and licensee must agree on some fundamental contractual conditions:

- Which rights are transferred?
- Is the license exclusive or non-exclusive?
- To which extent are the rights transferred, for instance how many copies can be made?
- What are the time limits of the contract?
- For which territory does the license apply?
- What remuneration shall the licensee pay to the rights holder?

Table Scheme of contracts elements - Licensor = music publisher

LICENSEE	Purpose	GRANTED RIGHTS	EXCLUSIVITY		TERM	TERRITORY
			YES	NO		
DISTRIBUTOR	SELL the lyrics/sheets	Print, publish, sell	X		3 YEARS	ONE
SUB-PUBLISHER	FOREIGN COUNTRY MARKET exploitation	Print, publish, sell; all rights under copyrights	X		3 YEARS	ONE/MORE
AGGREGATOR	DIGITAL MARKET DISTR.	sell, copy, sublicense, distribute		X	5/7 YEARS	WORLD
CD ROM/ DVD	Use of the text OF SHEET/LYRIC	Manufacture, sell, distribute		X	3/5 YEARS	ONE
ON-LINE RETAILER	SELL	sell, copy, sublicense, distribute, transmit		X	1/3 YEARS	WORLD
FILM PRODUCER	SYNCRO *	syncro with film and related uses		X	PERPETUITY	WORLD
ADVERTISING	SYNCRO *	syncro connect only with the spot		X	1 YEAR	ONE
MULTIMEDIA CD ROM	SYNCRO *	syncro connect with other media		X	PERPETUITY	ONE
MERCHANDISING	SELL	Utilise lyric/sheet music for manufacturing, advertise, distribution, sell	X		1/MORE YEARS	ONE/WORLD
PUBLISHER	USE of the text of lyric/sheets in a book	Print lyric/sheet in a book or magazine, sell, distribution		X	PERPETUITY	ONE/WORLD
	* for sound recorded, a master use license from the master owner is needed					

a) Music publishers licenses analysis

1) the granted rights

DISTRIBUTOR:
- To print, publish, and sell the music composition in the licensed Territory
- Print for any possible exploitation (sheets, album);
- Licensee can grant licensing to third parties (compilation of sheets music requested by other publisher)

SUB-PUBLISHER:
- To print, publish, and sell in the licensed Territory
- Performing right, synchronisation right, mechanical right are assigned
- Arrange, adapt and translate.

AGGREGATOR:
- Distribute for any possible exploitation in all digital means and media (whether now known or existing in the future)
- Licensee can grant licensing to third parties (compilation of sheets music requested by other publisher)
- The right to transmit, perform, distribute, promote and make commercial use via the internet and via other forms of digital dissemination

CD ROM / DVD PRODUCER: (use of text of lyrics and/or sheets)
- Manufacture, sell, and distribute in connection whit the release.
- The license cannot be assigned or transferred to third parties

ON-LINE RETAILER:
- To sell, copy, sublicense, distribute.
- Licensee can grant licensing to third parties

FILM PRODUCER:
- Record and synchronise the composition in relation with the film and not otherwise.
- To copy, print, distribute, perform exhibit by means of theatres, television including payTV, subscription TV
- To fix, sell, license and distribute through audiovisual media (video tape, DVD…)
- The license cannot be assigned or transferred to third parties

ADVERTISING:
- Synchronise the composition in relation with the advertising and not otherwise
- The license cannot be assigned or transferred to third parties

MULTIMEDIA CD ROM:
- Record and synchronise the composition in relation with CD Rom production and not otherwise.
- Copy, print, distribute, and sell.
- The license cannot be assigned or transferred to third parties

MERCHANDISING:
- Manufacture, advertising, distribution and sell in connection with a specified article

PUBLISHER: (use of text of lyrics or sheet in magazine, book, …)
- To print, sell, distribute in connection whit the release.
- The license cannot be assigned or transferred to third parties

Table Scheme of contracts elements Licensor = Master owner

LICENSEE	Purposes	GRANTED RIGHTS	EXCLUSIVITY		TERM	TERRITORY
			YES	NO		
RECORD COMPANY	FOREIGN COUNTRY MARKET exploitation	Manufacture, sell, distribute, perform	X		3/5 YEARS	SOME
RECORD COMPANY	COMPILATION	Manufacture, sell, distribute		x	3 YEARS	ONE
RECORD COMPANY	CLEARING OF SAMPLING			X	PERPETUITY	WORLD
DVD (MUSIC) PROD	VIDEOCOMPILATION	Manufacture, sell, distribute		X	3/5 YEARS	ONE
DISTRIBUTOR	SELL	Manufacture, sell, distribute	X		3/5 YEARS	ONE/WORLD
AGGREGATOR	DIGITAL MARKET DISTR/PERFORM.	Sell, copy, sublicense, distribute, transmit, perform…		X	5/7 YEARS	WORLD
ON-LINE RETAILER	SELL/PERFORM	Sell, copy, distribuite, transmit		X	1/3 YEARS	WORLD
MOBILE	SELL/PERFORM	Sell, copy, distribuite, transmit…		X	1/3 YEARS	ONE
FILM PRODUCER	Master use/SYNCRO * publisher license also needed	Syncro with film and related uses		X	PERPETUITY	WORLD
ADVERTISING PROD.	Master use/SYNCRO * publisher license also needed	Syncro connect only with the spot		X	1 YEAR	ONE
MULTIMEDIA CD ROM	Master use/SYNCRO * publisher license also needed	Syncro connect with other media		X	PERPETUITY	ONE

b) Master owner licenses analysis

1) the granted rights

RECORD COMPANY:

- manufacture, sell, use or otherwise distribute in the Licensed territory
- the exclusive right to perform publicly or to permit public performance including by radio and television broadcast
- the right to use and the right to allow others to use the name, likeness and biography of the artist whose performance is embodied in the said masters for the purpose of advertising and publicising the sale of phonograph records manufactured
- the possibility to grant to third parties in the licensed territory sub-licenses to exercise any or all rights granted to Licensee in this agreement, after a written approval of the Licensor
- the possibility to couple the phonograph records with other recordings for the distribution of TV albums after a written authorisation of the LICENSOR;
- the exclusive right to distribute phonograph records manufactured from the masters, through book and record clubs, mail order distribution plans or devices to sell phonograph records at budget prices;
- a first option for the sale and exclusive right to synchronise on film, video tape or other visual media now or hereinafter known

RECORD COMPANY 2: (compilation)

- the non-exclusive right to couple the phonograph records with other recordings
- the non-exclusive right to, use or otherwise distribute in the Licensed territory
- the possibility to use the name, likeness and biography of the artist whose performance is embodied in the said masters for the purpose of advertising and publicising the sale of phonograph records manufactured

DVD (MUSIC) PROD:

- the non-exclusive to record, manufacture, sell, distribute, exploit the videogram in the Licensed territory
- the non-exclusive right to couple the phonograph records with other videogram
- the right to use and the right to allow others to use the name, likeness and biography of the artist whose performance is embodied in the said master for the purpose of advertising and publicising the sale of videogram manufactured

DISTRIBUTOR:

- the exclusive right to copy, manufacture, distribute and sell the record in the Licensed territory

AGGREGATOR: (digital market distributor)

- the non-exclusive right to sell, copy, sublicense, distribute and otherwise exploit the "Recordings" by all digital means and media (whether now known or existing in the future), including, without limitation, the right to transmit, perform, distribute, promote and make commercial use of the Recordings via the internet and via other forms of digital dissemination of music such as, without limitation, cell phones and mobile memory and hard drive devices, and use artists' and producers' name(s), photographs and likenesses, biographical and other information in connection with the Recordings

ON-LINE MUSIC RETAILER:

- the non-exclusive right to sell, copy, distribute, transmit (download and streaming)
- to display any cover artwork associated with the recording

MOBILE:

- the non-exclusive right to sell, copy, distribute, transmit, promote and make commercial use in the Licensed territory
- to display any cover artwork associated with the recording

FILM PRODUCER: * publisher license also needed

- Record and synchronise the master recording in relation with the film and not otherwise.
- copy, print, distribute, perform exhibit by means of theatres, television including payTV, subscription TV
- Fix, sell, license and distribute through audiovisual media (video tape, DVD…)
- the license cannot be assigned or transferred to third parties

ADVERTISING PROD. * publisher license also needed

- synchronise master recording in relation with the advertising and not otherwise
- the license cannot be assigned or transferred to third parties

MULTIMEDIA CD ROM: * publisher license also needed

Record and synchronise the master recording in relation with CD Rom production and not otherwise.

- copy, print, distribute, sell.
- the license cannot be assigned or transferred to third parties

c) Synchronisation contracts: overview

To use sound recording in a visual work the customer should request (needs) a synchronisation license which should be negotiated on an individual basis with the copyright owners: the music publisher and the master owner who respectively will share the received synchronisation fee with the authors/composers and with the artists.

The synch license is generally a grant from the publisher or his/her licensor to the producer of the visual work, which authorises the utilisation of the underlying musical composition. The "synch" license itself does not permit the use of any specific recording of the particular musical composition. A separate recording or master use license is required for such a use or, in the alternative a new recording of the work would have to be produced.

Therefore the IPR related to the synchronisation are directly managed between copyright/ masters owners and the final users. A license between a music user (such as a film/TV production company) and the right holder of the musical work (usually a publisher) to use that music in a film/TV production is called a SYNC LICENSE or synchronisation license. A license between a music user and the owner of a sound recording to use that particular recording is called a MASTER USE LICENSE (as well as synchronisation license)

Typically, the major customers of this music market segment are:

- TV programs producers (sitcom, documentaries, etc.)
- advertising companies
- film producers
- video games producers
- home video producers (documentaries, education products, etc)
- CD-ROM producers

The expansion of new digital solution and of new standard applied to music market foresee the extension of the “synchronisation”

- telecom companies (e.g. new GSM applications),

- e-book applications
- internet sites (i.e. music under commercial banner)
- any other multimedia product embodying sound/music content

Synchronisation contracts elements
There are many issues which may arise whenever a synchronisation license is being negotiated between a producer of a film, television show, commercial, or computer game, and the publishers who owns the underlying music content

The Term
1. Films: The term is generally for the "life of the copyright" (in other words, the license will last as long as the song is protected by copyright law)

2. TV program: Sometimes for 3, 5, or 7 years, or, currently much more common, for the life of copyright.

3. Advertising: Typically one year; sometimes it is included a provision giving the licensee's right to renew for another equal term upon payment of an additional licensing fee

4. Computer Games: The term is generally for the "life of the copyright," As a practical matter, there are computer games which won't have such a life time and so in most instances the user won't consider it all that important to obtain a long term license.

The Territory
1. Films: Typically the territory is "worldwide."

2. TV program. It used to be that the territory was usually limited to certain countries. Today, most often, "worldwide."

3. Advertising: Local, regional, national, certain countries, or worldwide, i.e., depending on what the parties negotiate.

4. Computer Games: Worldwide.

Exclusivity Versus Non-Exclusivity

1. Films and TV program Synchronisation licenses are almost always non-exclusive in regards to films and television shows.

2. Advertising: There may be exclusivity for a limited period of time. When there is exclusivity, it is most often limited exclusivity, limited either to the territory of the license and/or to particular products or industries.

3. Computer games: Usually non-exclusive, though sometimes the license agreement will prohibit the music publisher from licensing the music to be used in other computer games for however long the license agreement will be in effect.

Synchronisation License Fee

The synchronisation fee will be in any given situation will depend on many factors:

the prospective use (e.g. whether the song will be used as a title song of a movie or in a commercial)
the prominence of use (background music or featured performance),

the duration of the use (i.e. one minute, four minutes, 10 seconds)
the popularity of the song and/or the songwriter, artists etc
the media in which the song is to be used (e.g. television, motion pictures or a video game)
the budget of the potential licensee
the type of market in which it will be exploited

Master use license
Many of the issues mentioned above in regards to synchronisation licenses are also issues in negotiations over master use licenses.
In this case the licensor may be willing to get a lower fee

Additional income

When music is "publicly performed" -- as in, for example, the case of a movie broadcasted in TV, or publicly performed online, the right holders of the underlying song will be earning not only the synchronisation fee which they received through the Synchronisation license, but also the "public performance" income from their collecting societies.

d) The use of protected materials in multimedia projects

When developing multimedia content, who uses material from other media must be careful about obtaining clearances for the same. As a preliminary note, he should have the concept firmly in mind so that when approaching the rights owners, rights needed are known. Following section introduce the problem of the use of other previously created copyrighted content

Music
Music is, of course, an important part of many multimedia products. Obtaining rights to music-related content is still complicated, time consuming and confusing process. As we have seen, music-related rights are split among a diverse group of owners and collecting societies, and necessary licenses can take peculiar, industry-driven forms. To use music (sound recording) for a multimedia project many licenses are to be obtained (synchronization, mechanical and also public performance license if final products are intended to be utilized in public places)

Photos
Ito use photos, multimedia producer must obtain clearances from the owner of the photograph. This is most often the photographer. When you see a photograph in a magazine or book, it is unlikely that that magazine or book owns the copyright in the photo. What is more likely is that the magazine is merely a licensee for some limited use and that all other rights remain with the photographer. You may obtain clearances, if at all, only by negotiating with the photographer, the photographer's agent, or in some cases the clearance house.
In some cases the permission of the persons depicted in the photograph is requested ("right of publicity," deriving from the right of privacy). These rights apply to living persons and, under certain circumstances, those dead. Their likenesses and even names may not be used for commercial purposes without their consent, which consent, if it is given at all, usually comes at a price.
Even photographs of now public domain works of art, perhaps called "classic art" such as the Mona Lisa, may also be protected by copyright. While the underlying art may be free to use, a photographic depiction of that free artwork may be separately copyrighted and so a clearance must be obtained for using that photographic reproduction of the artwork.
Needless to say, if the underlying artwork is still covered by its own copyright, then permission to use it must also be obtained.

Text
This category covers text of all sorts such as from books, magazines or the like, which are protected under the copyright laws. Clearance to use the copyrighted material must be obtained from the owner thereof,

usually the publisher if it is a book, or the author or whoever now owns the same. If the book is currently in print, it is usually not difficult to find out who owns it. But if the book is no longer in print but is still copyrighted, then searching out the author or the author's estate can be somewhat difficult. But the difficulty does not eliminate the requirement. In case of translation of the text, separate rights are involved.

Film/TV and radio
Analyzing and obtaining motion picture and audiovisual content rights can be even more complex than the related process with respect to music content, as music is often just one piece of an integrated audiovisual work. Numerous rights, often held by a wide range of different parties, are frequently implicated. Once again, multimedia product developers should tread carefully, reviewing their content needs very closely, approaching the rights clearance process systematically, and engaging knowledgeable professionals and services where necessary.
If one plans to use movie clips or segments of television shows, newscasts, commercials or similar content in a multimedia product, it will be necessary to obtain permission from the applicable copyright holders, even where very short clips are to be used. In most instances, the copyright in the motion picture or other audiovisual work will be owned by the production company that financed the film or television program in question. If the copyright owner is not readily ascertainable, it can also be useful to contact the distribution company, which often has such information. In addition to obtaining permission to use the motion picture or other audiovisual work as a whole, it may be necessary to license separately copyrightable elements of the work that are included in the clip to be used. Such elements may include

Music or Soundtrack: It may be necessary to obtain a separate license or licenses to use music if the audiovisual work contains a pre-existing musical work with a separate copyright owner or if the composer of a work created for the audiovisual product retained all or part of the copyright. In addition, if the music or soundtrack to the audiovisual work has been recorded and sold separately, the multimedia developer may need to obtain a license or licenses for use of the sound recording

Screenplay and Teleplay: In most cases, rights to the television teleplay or motion picture screenplay are included in the copyright to the audiovisual work as a whole, but in some instances the writer may have reserved some rights to the script in his or her contract with the producer. If this is the case, the multimedia product developer may have to deal with the writer separately and obtain his or her permission to use the desired clip.

Underlying Literary Works: If the film or television program is based on a book or other literary work, it may be necessary to obtain the author's permission to adapt the work for multimedia purposes

In the area of film, television and radio, union organizations play an important part (as they do in music). Because of this, when licensing a clip, multimedia producer will most likely be required by the terms of the license to pay and be responsible for all fees due the unions and guilds for the use of the material. These are referred to as "re-use" fees.

Multimedia developers should also be aware that a work's public domain status under a country copyright law is no guarantee that there are no rights clearance issues associated with its use in a product. For example, a work that has entered the public domain under U.S. law may still be protected under the copyright laws of other countries, and therefore a multimedia developer could risk infringement under foreign law if a product incorporating such a work were distributed internationally

4.1.2.1.2 Contracts elements and issues

Following the analysis of the contracts actually in use (below reported in Annex A) this section aims at identifying the main aspects and issues related to contracts aspects that have to be taken into account for the contracts standardisation process.

Business-to-Business (**B2B**) is a type of e-commerce in which an organisation conducts electronic transactions with other organisations. In the digital environment all transactions include intangibles content involving sellers and buyers of products and/or services. Generally, the seller is any company that sells a product and/or and the buyer may be a not-for-profit organisation, for-profit company or a government organisation such as a municipality, a state, or a government.

B2B

In the business-to-business environment, the size of an average contract is frequently substantial and therefore requires even greater and more detailed attention. Electronic signatures are likely to be of greater significance in B2B contracting than in B2C transactions.

The role of business contracts is to reduce uncertainty associated with the interactions between organisations. This uncertainty can arise due to partial information that trading partners have about each other and/or due to circumstances that are beyond their control. A contract is an agreement whose purpose is to mitigate such uncertainty – by defining obligations of parties to each other - and to have this enforceable by law. Currently, business contracts are printed on paper and humans carry out the contractual operations and decision making.

B2C

Business-to-consumer sales online are usually technically simple, often only requiring the completion of an online form. The legal requirements should not be underestimated and it is important that, before a deal is concluded:

- the customer has seen, read and accepted the terms and conditions
- the customer has specified a delivery address
- the ordered goods and the price to be paid are clearly identified.

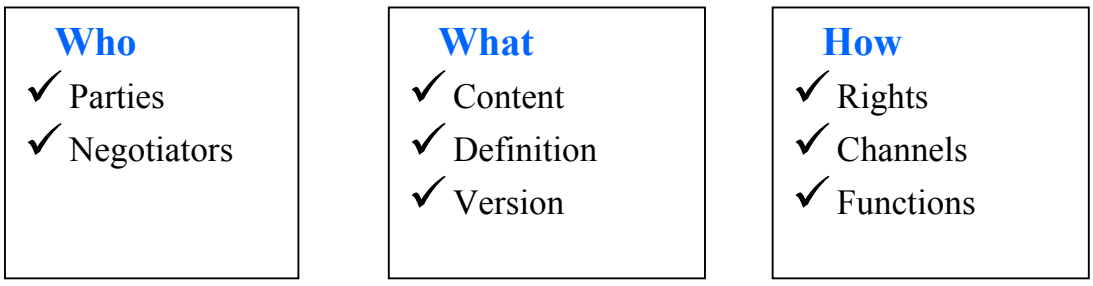
B2C contracts should comply with the EU Distance Selling Directive, consumer-specific provisions Companies selling over the Internet may also have to comply with the legislation in the customer's country.

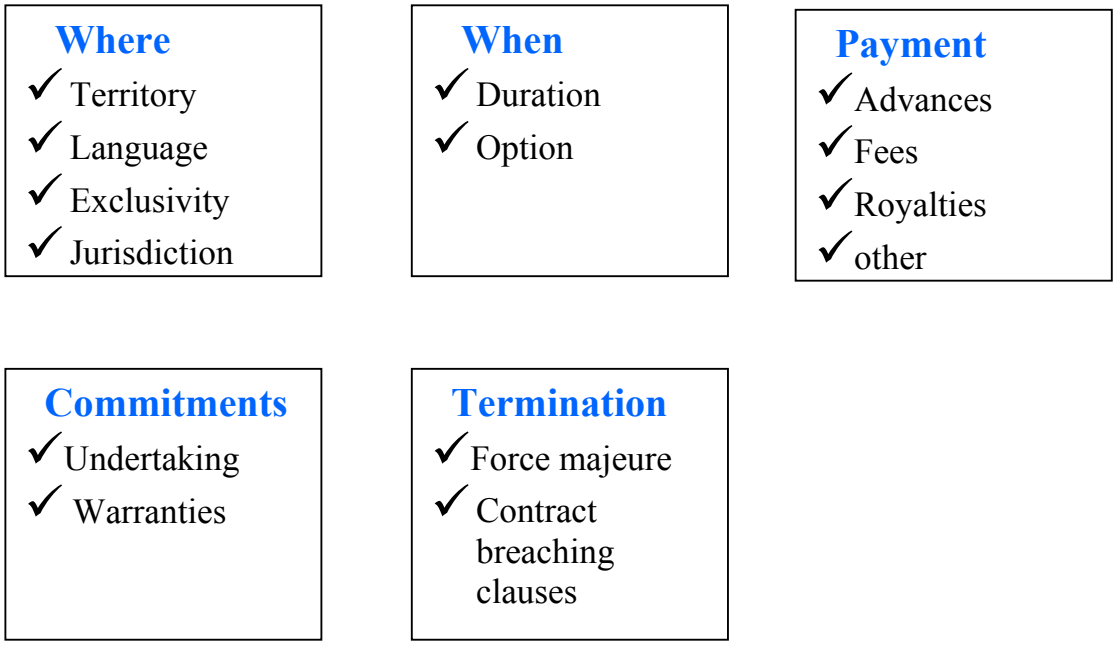
Elements of a Business Contract

There are fundamental elements needed to create a valid business contract:

- An *agreement* has to be reached on all essential conditions of the contract.
- The notion of *consideration*. Each party establishes the obligation to give something to each other. Consideration can take the form of money, services rendered, property or individual rights.
- The parties *competence*: ensuring that parties entering into the contract are lawfully capable of agreeing to contracts (e.g. whether an individual has the authority to represent their organisation).
- The *legal purpose* of the contract must be established. A contract cannot be enforced unless the actions agreed upon are legal in the jurisdiction where the contract is made.

As we have seen, in general, the following elements appear in a business contract as clauses covering:





In the context of B2B, many of the terms and conditions in the contract will form part of the requirements that specify behaviour of a B2B system. For example, terms and conditions associated with invoicing and payment will dictate what forms of invoices are acceptable, when they are to be received, and how the payment is to follow.
There will also be many terms and conditions that cannot be implemented (or are only partially automatable) and would require human actions and interventions.

A contract is a legally enforceable agreement in which two or more parties commit to certain obligations in return for certain rights [5]
In a B2B context this can range from a simple one-page contract to an extremely complex thousand-page document for a trade level agreement between multinational businesses. In general, most B2B contract formalisation follows several phases[6]:

- *Pre-contractual phase:* customers identify products or services and possible sources of supply;
- *Contractual phase:* creation of a formal relationship between buyer and seller, covering contract negotiation and validation operations;
- *Ordering phase:* delivery of content and services;
- *Settlement phase:* invoicing, payment authorisation and payment; and
- *Post-processing phase:* gathering information for management reports

B2B and B2C Deals and information Process

- Licensing originates in the business domain:
  - from content owner to content provider / or to distributor
  - from content provider to distributor
  - from distributor to retailer

[5] Reinecke et al., Introduction toBusiness - A Contemporary View, Allyn and Bacon, 1989.

[6] Clarke, R. "EDI is but one element of electronic commerce", 6th International EDI Conference, June 1993.

- from retailer to consumer

This value chain puts in evidence that the content owner can license its rights to a wide group of subjects whose activity needs to be evaluated to identify how many content transfers there are between the content owner himself and the consumer.
A content owner can grant its rights to an Internet services provider, a mobile company or to a satellite TV, which cares of making them available directly to the consumer.

A different option is represented by an intermediate phase consisting in the grant of the rights to a distributor or to a content provider, which in his turn grants them to the Internet service provider or to other operators charged of providing them to the consumer[7].

An explanatory description of the above process value chain is described below (Table 1 and Table 2)

[7] It should be taken notice of the fact that the number and the identity of the stakeholders in the TV sector has been influenced by the decisions taken by the European Commission to give an answer to some competition concerns in respect of the use of certain digital devices, for instance digital platforms.
Dominant positions have been limited, for example imposing an obligation to contract with sublicensees on a wholesale basis. Case COMP/M.2876 Newscorp/Telepiù, decision of 02.04.2003

Table 1

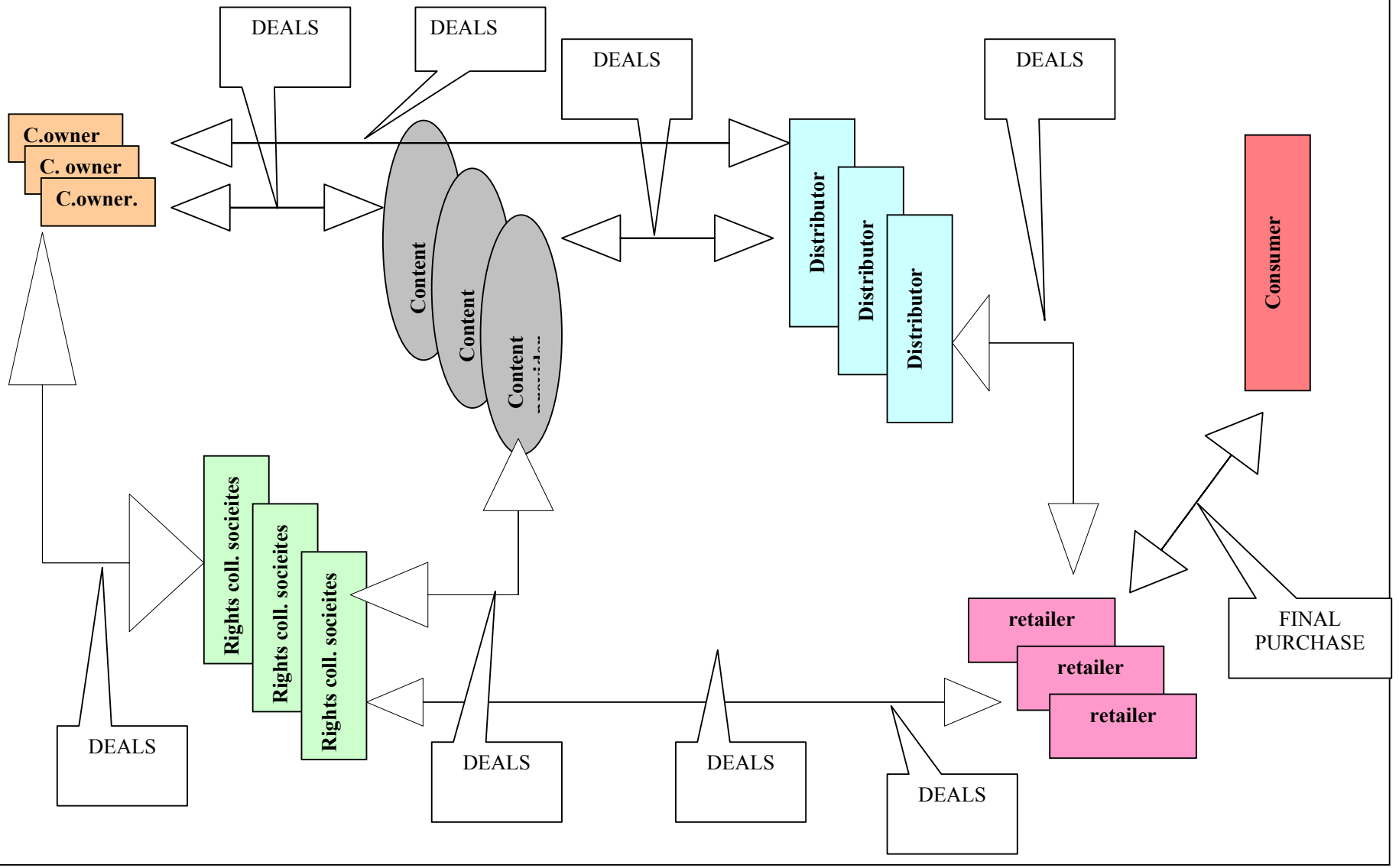
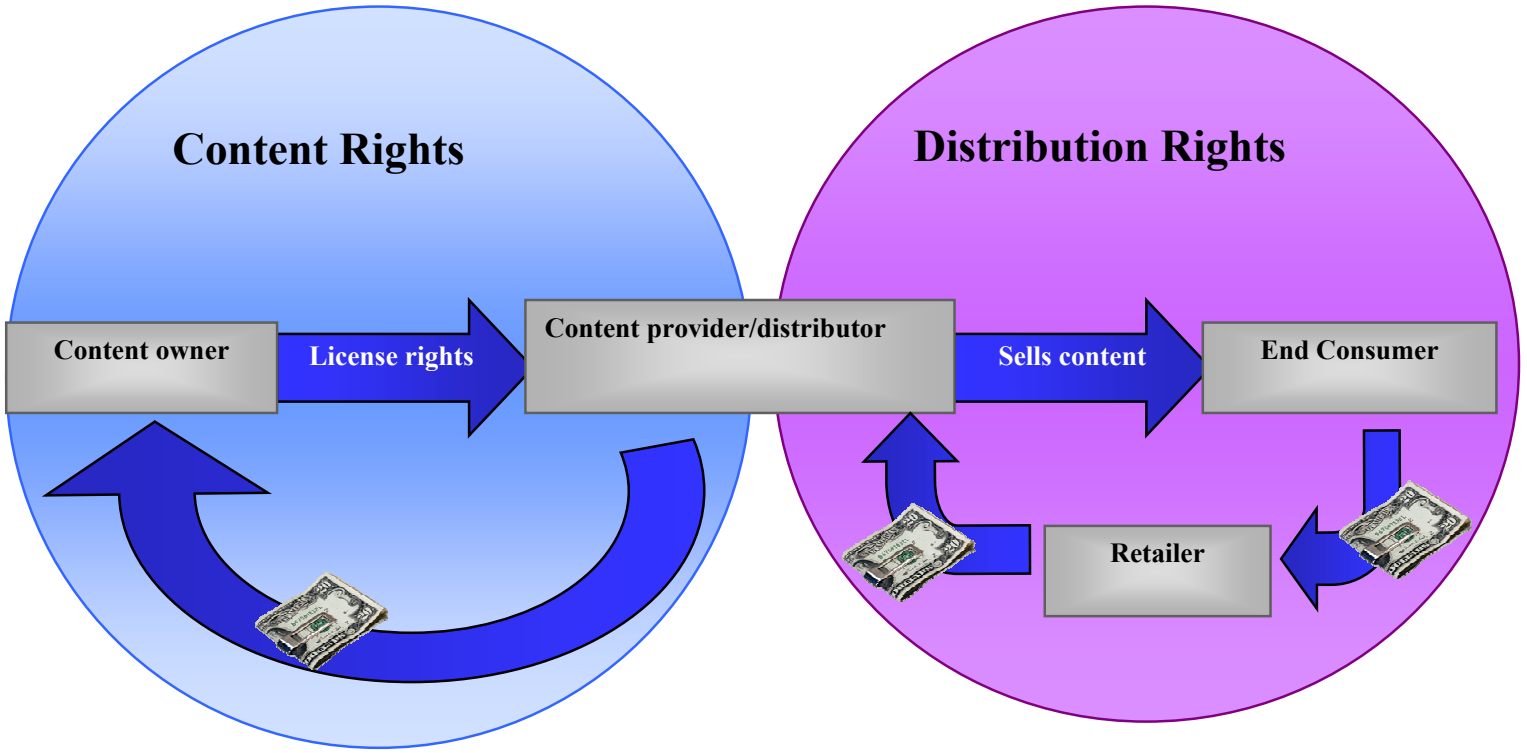
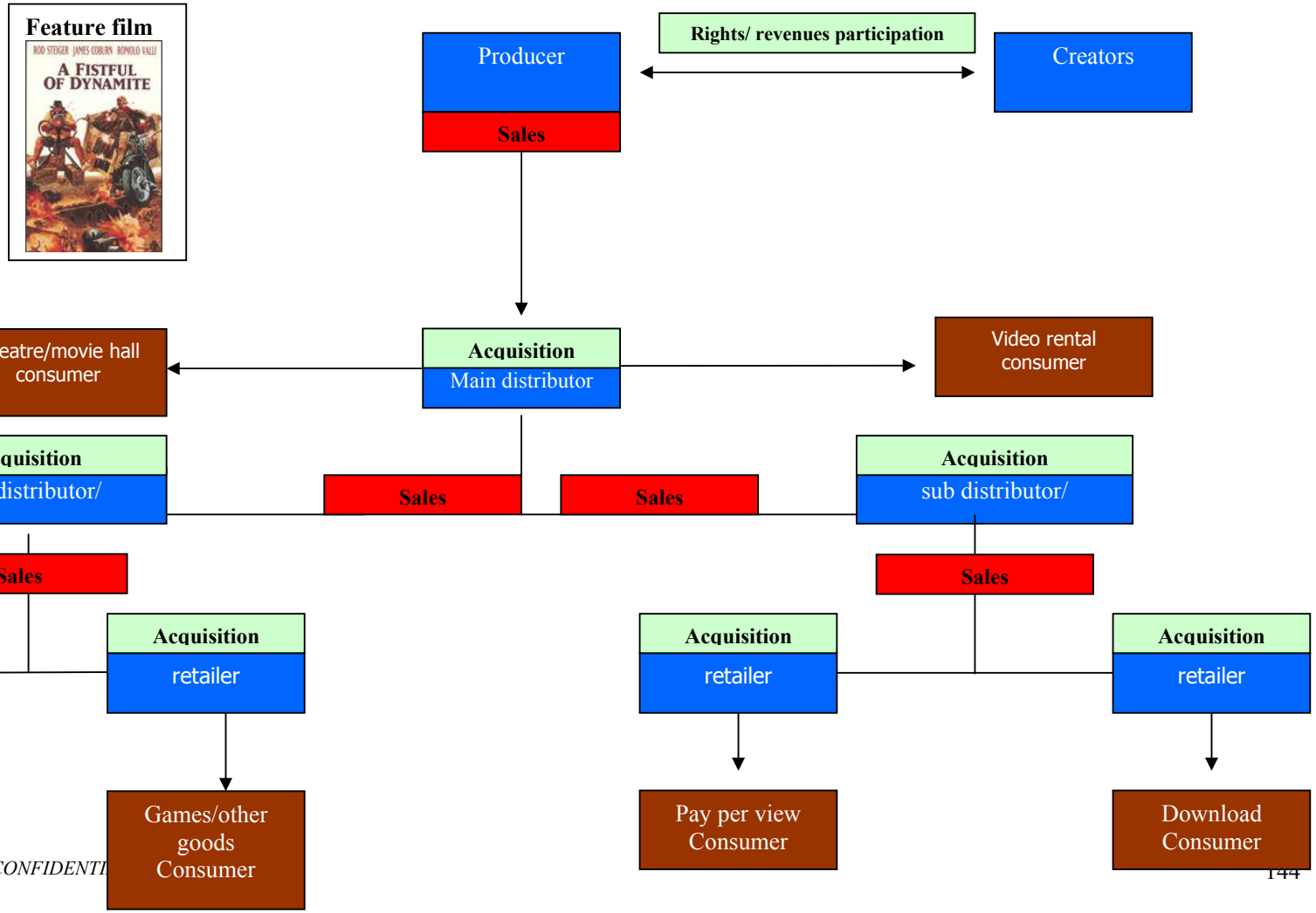
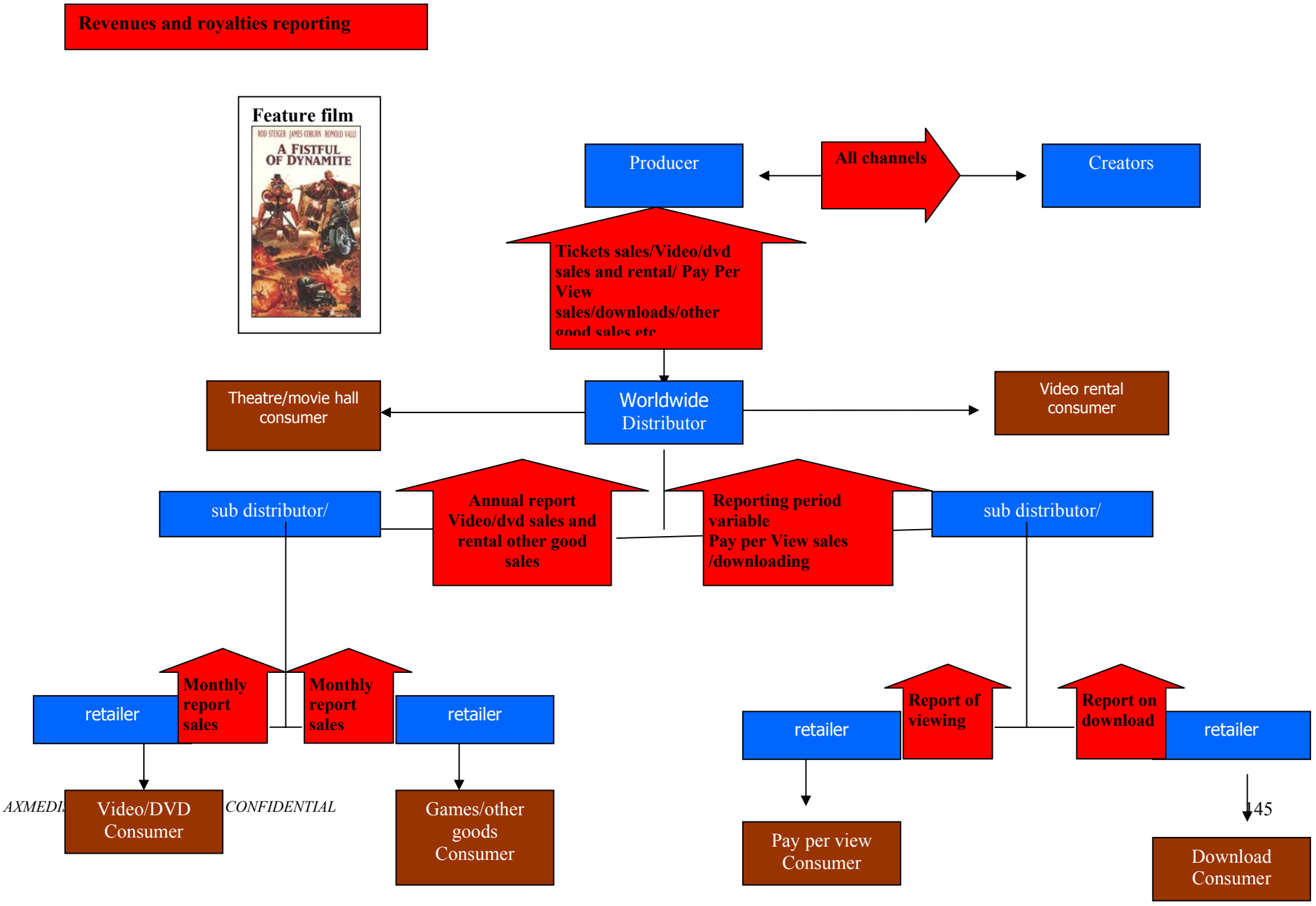

DEALS
DEALS
DEALS
DEALS
C.owner
C. owner
C.owner.
Content
Content
Content
Distributor
Distributor
Distributor
Consumer
Rights coll. socieites
Rights coll. socieites
Rights coll. socieites
retailer
retailer
retailer
FINAL PURCHASE
DEALS
DEALS
DEALS
DEALS

Table 2


Content Rights
Distribution Rights
Content owner
License rights
Content provider/distributor
Sells content
End Consumer
Retailer

Sometimes, business scenarios are more complex and are an aggregation of several of the above described simple scenarios.
The table below is an example of the more complex scenario that could concern the exploitation of a movie. In this case dealing process value chain involves for example the sub distributor as in-between actor.




Revenues and royalties reporting
Feature film
A FISTFUL OF DYNAMITE
Producer
All channels
Creators
Tickets sales/Video/dvd sales and rental/ Pay Per View sales/downloads/other good sales etc
Theatre/movie hall consumer
Worldwide Distributor
Video rental consumer
sub distributor/
Annual report Video/dvd sales and rental other good sales
Reporting period variable Pay per View sales /downloading
sub distributor/
retailer
Monthly report sales
Monthly report sales
retailer
retailer
Report of viewing
Report on download
retailer
Video/DVD Consumer
Games/other goods Consumer
Pay per view Consumer
Download Consumer

As an example to clarify the above scenarios, let's imagine the following cases:

The Movie producer: MR X

- Exclusive contract for worldwide exploitation of the movie with

A Main distributor: i.e. MIRAMAX

- Exclusive distribution contract – territory Italy

With a local Sub distributor (i.e. Italian De Agostini)

- Distribution contract with local retailers i.e. newspaper kiosks

The consumer buys the DVD

For the digital distribution reported on the rights side of the table, the case is the following:

Movie producer: MR X

- Contract for worldwide exploitation of the movie with

A Main distributor

- Non exclusive digital distribution contract

With a Sub distributor: i.e. on line distributor

- Non exclusive digital distribution contract (downloading or streaming of the movie)

With on line retailer

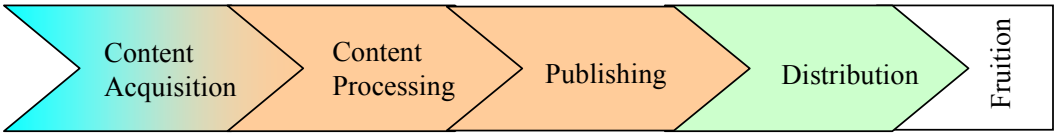
The Consumer pays for downloading the movie

The above scenarios can dramatically change depending on several circumstances. Sometimes the producers (mainly most powerful and important) directly manage their content with sub distributors or with the retailers; in other cases major distributors directly deal with retailer (for example in this case digital TV) or directly reach consumers and in other cases the sub distributors directly provide content to end consumer. The mentioned possibilities are variable.

4.1.3 Identification of value chain coming from the integration of the project partners

In the value chain each activity adds to the customer, value of the end product or service. The benefit of looking at the industry by using the value chain approach is that we are able to enlighten what activities have the most significance to the end customer value. It is also worth noting that the boundaries in the value chain do not necessarily form at the boundaries of different organisations, but at the boundaries of different activities. The key to understanding how the value chain boundaries are formed is in looking at the end product or service from the customer's point of view, and evaluating what features the customer values. The value chain, in its simplest form, is typically considered to be the independent businesses from different segments of an industry working together to help each member in the chain to meet their business goals. This report aims to map the value chain and strategic collaboration among AXMEDIS partners for the purpose of meeting the project's objectives for the mutual benefit and business opportunities. One of the most important aspects of successful value chain collaboration is the specific terms of arrangements between the players in the value chain who are responsible for getting content to the final consumer. Next section reports on the participating actors and their strategic objectives and relationship within the value chain.

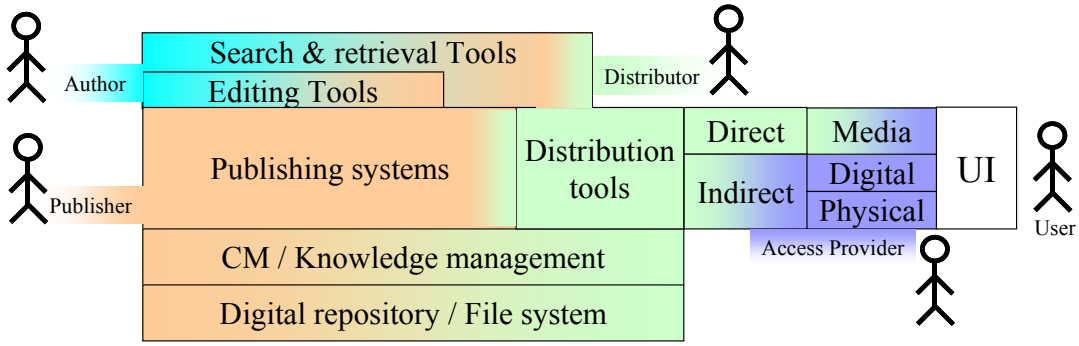
As a staring point for this is necessary to examine the overall value chain for content production and distribution that, with slight differences, is consistent regardless the media. At the origin of all there is a step that can be hardly defined or modelled as it consists of the "idea". Actually at the back of any content product there is an "idea" that could be political, scientific, artistic… anything that can stimulate someone to produce "content" (music, test, image, video…) and this could be the starting point of the process, yet could also be the end of it all as to turn the "idea" into a "product" (no matter if is will be a book, a magazine, a movie, a CD, an album…) it is necessary to find a "publisher/editor" willing to produce such content; this is the actual start of the value-chain. Originally the 1st source of added value was the possibility to replicate, via printing, the produced content. This step, actually made possible by Guttenberg, implicitly allowed also extensive distribution of replicated content. Therefore the original value chain of content production is related to paper publishing and looks like what reported hereafter:



The birth of new media, which could be used either in the processing or publishing phase, introduced new steps and actors in the value chain, which now looks like this:

The change is basically due to the insertion of an additional step: "quality assurance", and the modification from simple "distribution" to "personalisation and delivery". The first change is basically due to the fact that increasing the possible delivery media has also increased the complexity of the content production phase leading to more needs and additional actors involved in the process. If once the "proof reading" was a sub activity of the "publishing process", now this is often performed by professionals or even specialised agencies that check the "published media" prior to finalisation to provide a proper quality control and ensure both "correctness" and "usability". Given the sensitivity of the issue this activity is often ruled by very strict agreements binding the "controllers" to keep confidentiality on the accessed content. This is even more real when dealing with digital products (where SW plays a relevant role). Once stated this, it is necessary to take into account that the introduction of new media has also greatly changed the distribution scenario making new needs arise. In more detail while before the only real level of personalisation available was related to the "quality" of the object (hard-cover, paperback, rise paper, common paper, glossy pictures…) and therefore reflected in terms of prices; now the user requires a quite high level of personalisation that does not only cover the object aspect and cost but also (and this is becoming more and more frequent) even the content

(publishing on demand, customised delivery of news, tailored delivery and content format…). In all this is also comprised a new approach to content fruition (on-line) and payments (instalments, pay-pal, pre-paid cards, credit cards, certificates, coupons…). All this has also caused a change in the way "publishers" and "distributors" deal in business (delayed payments, anticipated stock acquisition, deferred payment, unsold stock return…) generating the need for further support tool spanning into knowledge management, data mining… In the following diagram is graphically presented how supportive tools (and therefore actors) work in cooperation with a publishing environment based on the reported value chain; it is worth noting that even when the context varies basically the publishing tools and supportive editorial tools are left unchanged (at least in terms of functional usage).



In all these diagrams we have used a colour-based code to express the areas of interaction of the various actors. It is also worth noting that each group of tool comprises a set of basic functionalities that are used by the various actors. In some cases access to certain functionalities is mediated via other tools and this is here expressed thanks to progressive shading. In more details we have that:

- Editing tools comprise facilities for design and composition;
- Search & Retrieval tools comprise gathering, sources management, metadata management and global knowledge management;
- Content / Knowledge management tools comprise content qualification, profiling approval, and local knowledge management;
- Delivery tools comprise profiling and personalisation support.

Most of the above mentioned functionalities are often used by more than a user (as already mentioned this is represented via progressive shading). This is obvious for tools like the search & retrieval one or for the editing one, yet is worth mentioning that often the usage of a specific set / class of tools is mediated through a specific system. For example in many publishing groups (typically related to newspapers or magazines) the editing environment is often integrated within the publishing system that may be configured to use one or several editing tools according to the internal needs of the various departments (e.g. composition needs are different from generic editing). What just mentioned is often achieved thanks to the support of WFM that may be embedded into the publishing / distribution system.

In order to simplify this complexity, we have grouped the different value-chain actors into major categories across a broad continuum from content owner, content provider including integrator and aggregators, distributors and access providers. Following table shows the group of partners participating to this business value chain. It is worth noting that given the specificity of the kiosk experimentation scenario, ILABS role will also span over chain segments that are not usually covered and more specifically: access provision.

<table>
<tr><td colspan="3"></td><td colspan="6">AXMEDIS technologies, DRM, tools</td></tr>
<tr><td colspan="3">Content owners</td><td>Content provider</td><td>Distributors/ Service provider</td><td>Access provider</td><td colspan="3">Customer interface</td></tr>
<tr><td>Producers</td><td>Publishers</td><td></td><td>ILABS</td><td rowspan="2">OD2
ILABS</td><td rowspan="3"></td><td colspan="3" rowspan="3">PC</td></tr>
<tr><td colspan="2" rowspan="2">AFI</td><td>SEJER</td></tr>
<tr><td>XIM integrator</td></tr>
<tr><td colspan="2">ANSC</td><td rowspan="4">TISCALI
ANSC
COMVERSE
ANSC</td><td rowspan="4">TISCALI
EUTELSAT
COMVERSE</td><td rowspan="3">TISCALI
EUTELSAT
COMVERSE</td><td colspan="2">PC</td><td>Mobile</td></tr>
<tr><td colspan="2">ILABS</td><td colspan="2">Mobile</td><td>Pda</td></tr>
<tr><td></td><td>SEJER</td><td rowspan="2">Mobile</td><td rowspan="2">PC</td><td rowspan="2">Pda</td><td rowspan="2">Kiosk</td></tr>
<tr><td colspan="2"></td><td>ILABS</td></tr>
</table>

Key roles:
Content owners
AFI: music audio, text and images
ANSC: music: text, audio, video and images
ILABS: publishing: educational content
SEJER: educational content

Content providers/aggregator
ILABS: e-learning content provider and aggregator
SEJER: educational content aggregator
XIM: interactive media content – content integrator

Distributor
OD2: music content provider to on line retailer/distributor
ILABS: e-learning content/solutions provider and distributor

Content provider/distributor and access providers
TISCALI: images, music and video content provider, distributor for PC and mobile, connectivity provider
COMVERSE: music content provider, mobile distribution, mobile technologies service providers
EUTELSAT: distributor of video content for broadcasting through satellite – satellite technology provider
ILABS: e-learning distributor and access provider for the kiosk local infrastructure

In this value chain each partner performs a well-defined role, taking inputs from upstream participants, adding value, and then delivering their output to a downstream contributor

Content owners:
These partners (or their members as in the AFI case) are those entitled to exploit their content by issuing agreements with content providers and distributors. They may share their revenues with other rights holders (authors, artists, etc.) accordingly to previously signed contracts. An important aspect in the contents is its ability to be virtualised, and thus be able to take advantage of the information network.

Content providers/aggregator:
This category includes content aggregators and organisations that provide digital content. They function as middleman between content owners and the distributors. Aggregators license content from the owners then package and format it for use by specific devices and networks. They provide value to the content owners by negotiating distribution deals with content distributors. Content aggregators combine content from numerous

sources and integrating it into a single interface. . In the aggregating process the delivery channel has to be taken into account for the content is dependent on the network used and the capabilities of the user interfaces

Distributor/service providers:
To generate revenues, content aggregators and content owners must deliver the content they provide through new distribution channels. Content distributors provide the aggregator and content owners with the ability to publish their content on different networks, devices, and operating systems.
Distributors support and develop applications for a wide variety of protocols.
Content distribution capabilities include synchronisation services that enable data transfers over unreliable networks and optimisation services, which compress data and thus speed the delivery to users in a bandwidth-constrained environment

Access providers:
Access providers are actors that provide connectivity and services through which customers access the content. They include wireless and mobile service providers like COMVERSE, Internet service providers like TISCALI and satellite technology provider like EUTELSAT.

Customer interface
The customer interface is the terminal equipment that the customer uses to consume contents. The software used is also an important aspect as is the usability and mobility features of the terminal equipment. Currently personal computers rule the market but smart phones, that have e-mail and Internet browsing capabilities, are still to make their breakthrough to the consumer market.

Who has to deal with?

Content owners/provider

<u>Publishers are connected with:</u>
Authors: Assignment agreement
Producers: Production contracts.
Performers: Performing contracts.
Co- Publishers: Agreements
Sub Publishers: Publishing contract for the identified territory
Aggregators: Contract agreement including distribution terms and conditions
Distributors: Distribution agreement (text, images)

<u>Producers are connected with:</u>
Performers: performing contract with terms and conditions for performing rights
Authors and Publishers Collecting societies: mechanical license for audio-video recording
Co -Producers: Co-production contract
Foreigner producer: license contract for the identified territory
Aggregators: license contract (including synchronisation contract) and distribution terms and conditions
Distributors: distribution agreement

<u>Aggregators are connected with:</u>
Producers: License contract
Publishers: Publishing contract
Rights Collecting Societies
Distributors: Distribution agreement

Distributors/service providers

Producers: Distribution agreement
Publishers: Distribution agreement

Aggregator: Distribution agreement
Authors and Publishers Collecting Societies: License
Rights Collecting Societies
Access providers

Access providers

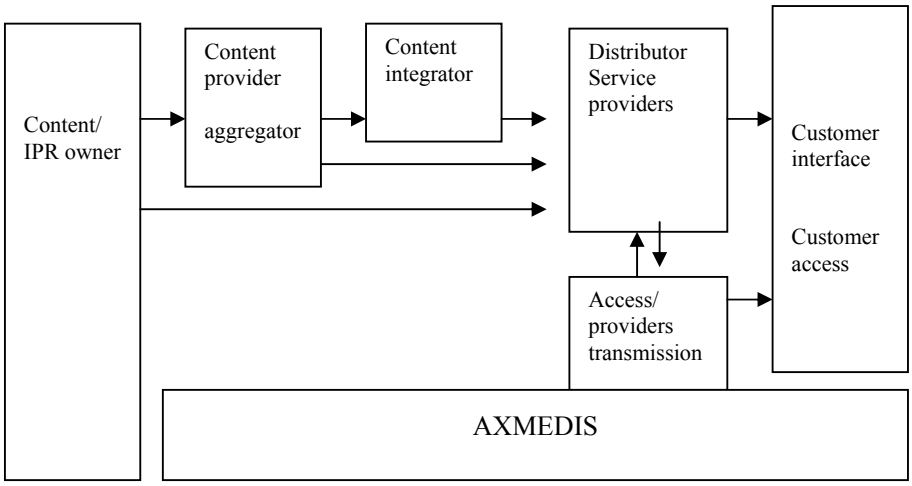
Network/ Internet service provider including broadcast television and radio services.
Connectivity providers: interoperability between connectivity between providers.
Distributors/Aggregators to deliver content
Software platform providers
Devices

4.1.4 Value and information flows

Next table is an example of the connections, value and financial flows that takes place among actors of the Internet on line music industry.

Actor	Type of flows	Inbound flows - from	Outbound flows - to
CONTENT PROVIDER ***CONTENT OWNER**	**Value flow**	Service provider (contract) Music creators (songs, music) Rights Coll. Soc. (rights)	Service providers (contract) Music content
	Financial Flow	Service Providers (share of revenues) *Rights Coll. Soc. (royalties)	Music creators (royalties) Rights Coll. Soc. (fees for licensing)
SERVICE PROVIDERS	**Value flow**	Content provider (contract, music content) ISP (hosting services) Providers of DRM systems, media platform, on line music application, etc. Affiliate services providers (Credit cards payments etc) Rights Coll. Soc. (licenses)	End user (on line music service) Content provider (request music content) Rights Coll. Soc (catalogue on music downloaded or streamed) Affiliate services Credit card clearing process
	Financial Flow	End user purchases (subscription fees, per track fees etc)	Content provider (revenue share according to contract) Provider of DRM system etc (revenue share according to contract) Rights Coll. Soc. (licenses fees) ISP (Hosting services) Credit card commission
ACCESS PROVIDER (ISP)	**Value flow**		Service provider (hosting services) music content to end user
	Financial Flow	Service provider (contract - hosting services) End user (subscription fees)	Affiliate services
END USER	**Value flow**	Service provider (on line music service)	Service provider (feedback) ISP access
	Financial Flow		Service provider (subscription fees, per track fees etc) ISP (subscription fees)

4.1.5 The multi-channel value chain



The increasing convergence of industry segments in the digital age and the complexity of industry structures, business models, and player relationships grow. Many players are moving into different or new areas of competence. New entrants are seeking areas of demand for their products, and ultimately, profitability.
Alliances and common strategies between the content owners/providers, distributors and access and technology providers that come up with new business models play a critical role in driving the adoption of licensed content services. As a consequence, a competitive and legal environment needs to ensure that technology providers benefit from content whereas content providers and owners benefit from delivery over the broadband infrastructures.
Business models need to be developed that respect the positions of content producers and that of the telecommunication operators. In the case of music, disagreements between the music industry (labels, collecting societies and authors associations), technology providers (PC and consumer electronics industry) and network operators are one of the main obstacles to the deployment of successful broadband content services.

To a better understanding of the value chain in a multimedia environment we have identified three areas within the converged market space and a number of roles within them, simplifying the value chain illustrated above.

These areas are:

- Content area – Digital content
- Service area – Service Provider
- Access area – Transmission

All areas and roles are defined in more detail below, with examples of activities undertaken in each area. It is important to underline that the inclusion of one supplier as an example player in one role does not exclude it from other roles.
These examples are indicative. Many organisations' brands fulfil activities in multiple segments and roles.

4.1.5.1 Content area

4.1.5.1.1 The ultimate content for which the customer is paying - either directly or indirectly

The Content area is concerned with those who create and provide content targeted at users, including any form of downloadable digital media (including music in any format, moving or still images, infotainment, textual content, etc.).
Taking content as one area, the key distinction (in a market framework model based on revenue flows) is whether the content has been created for profit or not.

4.1.5.1.2 Not-for-Profit role

Content created not-for-profit by users either as part of an enterprise, part of an online community, or purely for self-gratification. Examples of this are web-loggers (or 'Bloggers'), amateur musicians, etc.

4.1.5.1.3 Profit-Making role

Content created for profit – even if eventually supplied to users free of charge (e.g. adverts, sponsored downloads.)

4.1.5.1.4 Offline Products role

Offline products - physical products purchased or obtained online. They are included in this area as they cause revenue flow into the digital converged market. Examples of products in this category include DVDs and CDs.

4.1.5.1.5 Content area situation

CONTENT PROVIDER	SITUATION/ISSUES	OPPORTUNITIES
Content/IPR owners aggregator/integrator	• Copyright infringement worries • Weak understanding on how to optimise new or existing content • "Creativity" industry slows in the development of successful business models • Traditional business models and contractual procedures are applied in the digital environment • DRM, micro payment, etc., issues make this sector unstable • Major multinationals could undermine SMEs • Regulatory environment needs more harmonisation • End users not educated to pay • Progress across different IPR owners are not uniform (e.g. music vs. movie industry) • Clearance and licensing of digital rights is complex and inhomogeneous	• Customers want access to content • Much high-bandwidth infrastructure in place • Great opportunity to exploit content on a worldwide basis • Partnership with ITC industry are evolving • Mobile users are willing to pay for content, and number of customer recognising content value increases. • Devices more capable of displaying complex content • Europe has strong tradition of creativity

4.1.5.2 *Service area*

Service area includes the functions, which enable the user to access and interact with content and applications over digital channels.
In this area the market players mainly package, license content and market it to users. This activity may include Access - Marketing - Customer Relationship Transactional role.

Some players may fulfil multiple roles, as well as different kind of the roles to different users.

4.1.5.2.1 Access role

Enabling the use of a delivery mechanism to obtain content e.g. Tiscali.

4.1.5.2.2 Marketing role

Marketing services delivered over converged communications media include:

Internet
- direct – banner or pop-up adverts on websites
- access based – usage pop-ups
- search based

Mobile
- SMS marketing
- MMS marketing
- WAP site adverts
- Location based advertising

iTV
- Interactive adverts
- Sponsored interactive games

The Marketing role in this area is associated with the organisation planning and associated services surrounding the above examples.

4.1.5.2.3 Customer Relationship role

This action aims to assist customers in their interactions with a service or product and to ensure it service meets clients' requirements. Most online distributors offer some form of customer service, including email address to submit complaints or queries.

4.1.5.2.4 Transactional role

The provision of transactional services such as:
Payment or other transaction service to customer
Acquisition services
Hosting service – i.e. hosting Internet stores for others

SERVICE PROVIDERS	SITUATION/ISSUES	OPPORTUNITIES

Content distributors including content delivery network and streaming media players Retailers who sell their products through digital channels Advertising industry – using converged channels for marketing Portal/interactive platform gateways to content and transaction based services	• Lack of a clear business model and route to profitability is a concern • Integrating technology is expensive • Partnerships are emerging, but are still fragile • Risk of monopolistic action of big players • Risk of too much choice in some areas • DRM, copyright, micro • Payment, etc., issues make this sector unstable • Fixed Internet users still want content for free • Customer awareness of potential of multi-channel & high bandwidth opportunities to be addressed • Clearance and licensing of digital rights is complex and inhomogeneous	• Customers want access to content and services • Service area is the key segment in multi-channel space • Opportunity for innovation • Consumer trust is growing • Innovation will enable new business models and driving market growth • Content/push and delivery/pull will make service provider work • Increased customer recognition of content and services value • Devices more capable of displaying complex content • Much high-bandwidth infrastructure in place and more to come

4.1.5.3 Access area

Access area involves the technology and infrastructure required to transport content or service to the end customer, as well as providing a feedback channel for interactive communication.

4.1.5.3.1 Devices role

Devices encompass the provision of a customer end-point of delivery mechanism. This includes mobile handsets, cable modems, broadband modems etc.

4.1.5.3.2 Networks & Infrastructure role

Networks and infrastructure cover all elements of the delivery mechanism up to the end-point device. This includes all types of wireless and fixed networks, wires, repeaters, antennae, routers and so on used in the data delivery to the end-point device.

ACCESS PROVIDERS	SITUATION/ISSUES	OPPORTUNITIES
Network operator ISP Broadband/satellite Mobile service providers	• Access networks not widespread • Large firms may inhibit market development • Cross-platform services incorporating richer services needs standardisation • DRM, copyright, micro payment issues make this sector unstable • Devices much more complex than previously • Big players may smooth growth of smaller players	• Industry player are well known • Content is opportunity to fill networks • Plenty of network capacity • Potential of web based services • Access can expand into new services • Devices are much more capable and customisable • Wireless access now built-in to devices (e.g. new laptops)

4.1.6 AXMEDIS Value chain

To exploit valuable digital content and enhance their multi channels distribution, the AXMEDIS value chain structure and the applied DRM will be developed and implemented in order to grant new ways of creating and managing digital content and services. In particular addressing some of the following requirements which will enable capabilities for value content creation and distribution:

- **Information standards** to describe and compare available products and services. Excerpts, editorial reviews, customer reviews and ratings for example all provide ways for customers to further filter or qualify their interests.
- **Structured, organised profiles to describe customer needs**. Profiles include a customer's stated preferences, implied interests based on usage and immediate situation, such as location, time and access device.
- **Standards for agreeing on and applying commercial terms**. Personalised services that integrate the products and services of several providers require new business models. To be implemented, these models need to determine the detailed business terms that govern pricing and delivery responsibilities. In the music industry, for example, instead of selling an album for a fixed amount from one artist, the industry is looking to provide subscription services that allow the individual consumer to link multiple artists into a unique personal play list. However, to do this, the business terms along the value chain will be defined around new business models and automate them to support cost-effective business operations.
- **Technology to protect digitised content assets.** The ease of copying and reproducing content once it has been digitised is a major commercial threat to content owners. The average PC can copy music files, and faster connection bandwidth makes the illegal transfer of these files convenient. The entertainment industry must make the unauthorised copying and transfer of content more difficult and also make it attractive and convenient to adopt legal alternatives. However, copyright theft is not confined only to the entertainment sector. Many industries are concerned with protecting their intellectual output, including software developers, investment banks (proprietary research) and products companies (mobile phone designs), not to mention their marketing material and strategic plans. Digital containers require identification and knowledge of approved users before access is permitted.

5 Fingerprint and features estimation and data integrity

One solution to the present problems in authentication and verification of multimedia content is the embedding of a unique, fragile and imperceptible code, which is also called a fragile watermark. This was already addressed in other projects. The second solution, which is considered within the AXMEDIS scenario, is the efficient and effective usage of so-called fingerprinting or perceptual hashing techniques. Thus, the focus within AXMEDIS is on perceptual hashing. “Perceptual hashing” indicates the common aspects with cryptographic hash functions while considering perceptual similarity. In the following subsections cryptographic hash functions are explained. Their drawbacks – when they are applied to multimedia content – are described. The advantages of perceptual hash functions are motivated.

5.1 Cryptographic hash functions

A hash functions maps a larger input space to a smaller one. The output of a hash function is called digest. It serves as a unique digital fingerprint for the input data. According to Wikipedia [67] general prerequisites of cryptographic hash functions are:

- **Pre-image resistant**: given the hash h it should be hard to find the message m such that $h = hash(m)$ (one-way function).
- **Second pre-image resistant**: given an input m_1, it should be hard to find another input m_2 (not equal to m_1) such that $hash(m_1) = hash(m_2)$.
- **Collision-resistant**: it should be hard to find two different messages m_1 and m_2 such that $hash(m_1) = hash(m_2)$.

In [68] another property is given:

- **Random oracle property**: the hash function h behaves as a randomly chosen function.

These prerequisites cause any hash function to calculate a different digest if the original was altered even slightly. Thus, hash functions can be used to detect altered and forged documents. Hash functions can be used with a key. Among the common hash algorithms are MD-5 and SHA-1. For details on cryptographic hash functions suggested readings include [69], [70]. Also different RFCs (requests for comments) [71] provide valuable information about the usage of hash functions.

5.2 Drawbacks of cryptographic functions applied to multimedia data

Computers typically process digital data streams. In contrast to these data streams, humans perceive multimedia data. Obviously humans do not notice certain types of content modifications, e.g. the noise addition below the perceptual masking threshold. This property is exploited by lossy compression techniques, e.g. MP3 compression.

Cryptographic hash functions however are bit-sensitive. Thus, using cryptographic hash functions for authenticating multimedia data is restricted to application where content is not processed or not available in different formats: Even format conversions are critical as the content modifications result in different hash values.

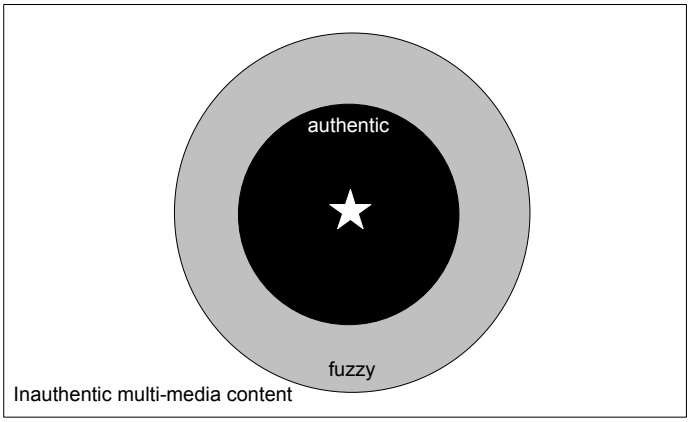


Figure The fuzzy boundary between authentic and non-authentic multimedia contents.

Perceptual hash functions are designed to overcome this drawback: Only manipulations, which change the content noticeably or considerably, should affect the calculated perceptual hash function. Unfortunately, there is no sharp boundary between authentic and inauthentic data. This is exemplified in the previous figure. For some processing operations it is difficult to decide if the result of the modifications is authentic. Besides perception issues this decision boundary is influenced by the application scenarios.

5.3 Perceptual hash functions

In contrast to watermarks perceptual hashing or fingerprinting techniques do not embed a message into a digital content. Instead, they directly calculate a content dependent identifier. This identifier ideally uniquely identifies the input data. Thus, their properties can be compared with cryptographic hash functions. A perceptual hash function (fingerprinting function) should also satisfy the previously described requirements on cryptographic hash functions:

- Pre-image resistant
- Second pre-image
- Collision-resistant
- Random oracle property

Additionally, a perceptual hash function has to fulfil a different requirement, which contradicts the prerequisites of the "second pre-image resistant" and the "collision-resistant":

- **Perceptual similarity**: If two given inputs m_1 and m_2 are perceptually equal (similar) their corresponding hash values should be equal: $hash(m_1) = hash(m_2)$ (rsp. similar: $hash(m_1) \approx hash(m_2)$).

Perceptual similarity requires fingerprinting methods to be individually developed for different content types (like watermarking technologies). A general scheme, as given in [72], is shown in the next figure and involves the following operations:

- **Feature extraction and processing**: Typically, the input signal is pre-processed, which depends on the data type. For audio typical pre-processing operations are down sampling, format conversion, and band-pass filtering. Similarly, pre-processing operations for image data includes resizing or colour conversion. In the case of audio or video the input data are segmented and so-called "sub-fingerprints" are calculated. Features are generally extracted from a transformation domain where redundancy is decreased (similar to compression). Within this transformation domain relevant features are extracted. In a post-processing specific relative measures can be derived.

- **Fingerprint modelling**: The multi-dimensional input vector sequence is mapped to a single vector to produce compact fingerprints. This can also include a binarisation.

- **Database lookup**: The first step in matching the calculated perceptual hash value(s) is to identify similar content. This is done by a database lookup. Obviously this database lookup includes a search in pre-calculated perceptual hash value(s). Different search strategies can be applied and must consider the chosen fingerprint model. Similarity is calculated by a suitable distance function.

- **Hypothesis testing**: Finally, the identified content item(s) are validated using a hypothesis test. A hypothesis testing involves a threshold. This threshold has to be chosen carefully. Different previously outlined issues influence this threshold.

These steps can be grouped in two functional blocks:

- **Fingerprint calculation**: Here, a secret key can be used for the calculation of the fingerprints. As this allows the calculation of key dependent fingerprints/perceptual hash values it increases the security of the fingerprinting calculation.

- **Fingerprint matching**: The previously described database and the following hypothesis testing are necessary for matching the calculated perceptual hash values with already stored ones. This potentially influences the following matching process, as perceptual distance metrics will not apply.

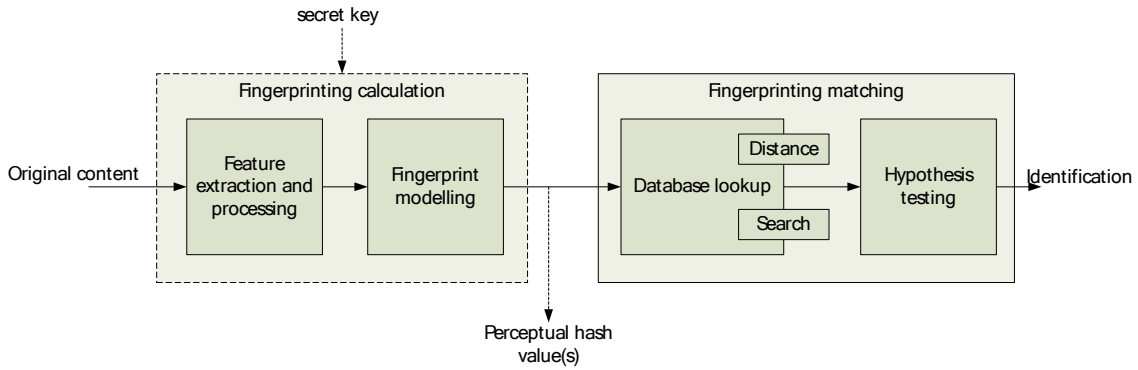


Figure The general identification based on fingerprints involves two functional blocks: First, the perceptual hash value (fingerprint) is calculated. Second, a database look-up retrieves one or more stored values. A following hypothesis testing verifies if content has been identified correctly. The results are returned.

Similar to watermarking we can identify two different classes of attacks:

- Attacks that influence the feature extraction, processing, and modelling operations. These attacks can be considered as attacks to the robustness of the fingerprinting. Like for watermarking robustness attacks, here a potential attacker is interested in identifying transformations that minimize the perceptual distortion while maximising the effects on the calculated perceptual hash values.

- Attacks can also try to gain knowledge about the secret key of the fingerprinting calculation. These attacks can be considered as attacks to the security.

5.4 General Requirements on fingerprinting technologies

5.4.1 Discrimination

The purpose of perceptual hashing technologies is the identification of content. In other words perceptual hashing technologies have to distinguish different content items. Thus, the discriminability of the perceptual hashing techniques is very important. The discriminability depends on the length of the calculated fingerprint. The used distance metric is another important factor influencing the discrimination.

5.4.2 Size

Perceptual hashing technologies must ideally also be able to uniquely identify each content. Thus, the size of the fingerprints should be large enough to address the different relevant content items.

5.4.3 Performance

Here, the complexity requirements also depend on the application. For example for broadcast monitoring the identification has to fulfil the same requirements on complexity and latency as the watermarking technologies.

5.4.4 Robustness

Perceptual hashing techniques also have to identify content items even after they were processed by a certain range of processing operations. These processing operations are specific to the application scenarios and the same that have to be considered for watermark. These manipulations increase the distance between the fingerprint of the original and the fingerprint of the modified content. The results are either false negatives (content is known, but cannot be identified) or in the worst case false identifications.

5.4.5 Searching

Depending on the content type and the fingerprint structure the search can range from a simple similarity search (e.g. in the case of images) to a more complex search. This complex search is typically the case for audio and video due to the time dependency of this data. Different operations can influence this time dependency. For examples, frames might be dropped out if a movie is converted into a different format.

5.4.6 Security

According to [68], only brute force methods are available for cryptographic hash functions if no analytic weaknesses are known.

- **Brute force attack**: If n is the size of the hash outputs around 2^n operations are needed to break the pre-image and the 2nd pre-image resistance.

- **Birthday attack**: If n is the size of the hash outputs around $2^{\frac{n}{2}}$ operations are needed to break the collision resistance.

However, if perceptual hashing functions fulfil perceptual similarity requirements the pre-image resistance, the 2nd pre-image resistance and the collusion resistance are potentially endangered.

- **Sensitivity attack**: The sensitivity attack against digital watermarks was first described in [73]. The assumption is that the watermark decoder is implemented in a tamperproof box. A potential attacker cannot reverse-engineer critical parameters or the detector's properties. Nevertheless, an attacker can experiment with the content and the detector.

6 DRM editor and viewer

The DRM editor and viewer is an application and it has been developed by using C++ MSVC7, the wxWidgets ver. 2.4.2 Mozilla and xerces libraries.

6.1 Technical Details

Reference to the AXFW location of the demonstrator	https://cvs.axmedis.org/repos/Applications/drmeditor/
List of libraries used	Wxwidgets 2.4.2 Xerces 2.6 (SAX)
References to other major components needed	License manager License model
Problems not solved	• Visualisation of some MPEG-21 REL licenses
Configuration and execution context	Windows
Programming language	C++

6.2 Description DRM editor and viewer

This module consists on a GUI application based on wxWidgets that currently provides visualisation functionalities for licenses expressed in MPEG-21 REL (Part 5 of the MPEG-21 standard that describes the syntax and semantics of a rights expression language).

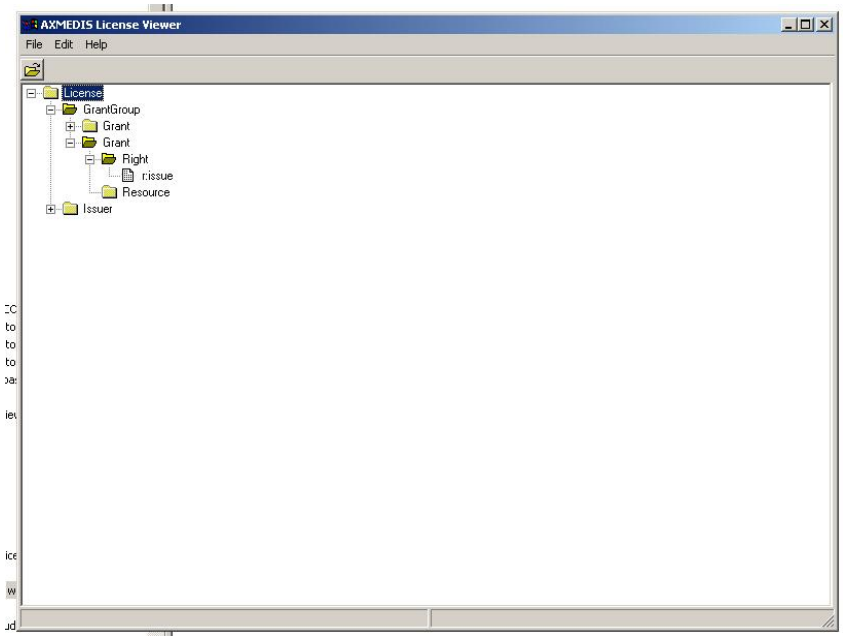


Figure DRM viewer snapshot

DRM viewer makes use of the license model specified in part E of specification deliverable, DE3.1.2. This model retrieves a license expressed in XML, according to the XML schemas that define MPEG-21 REL (there are three of them, r that is the core schema, sx that is the standard extension schema and mx that is the multimedia extension schema, as defined in [6]), and transforms it into an object model. The license model also provides functionalities for generating licenses in XML language and SQL instructions that permit the storage of the licenses into a relational database. The relational model supported was also specified in DE3.1.2.

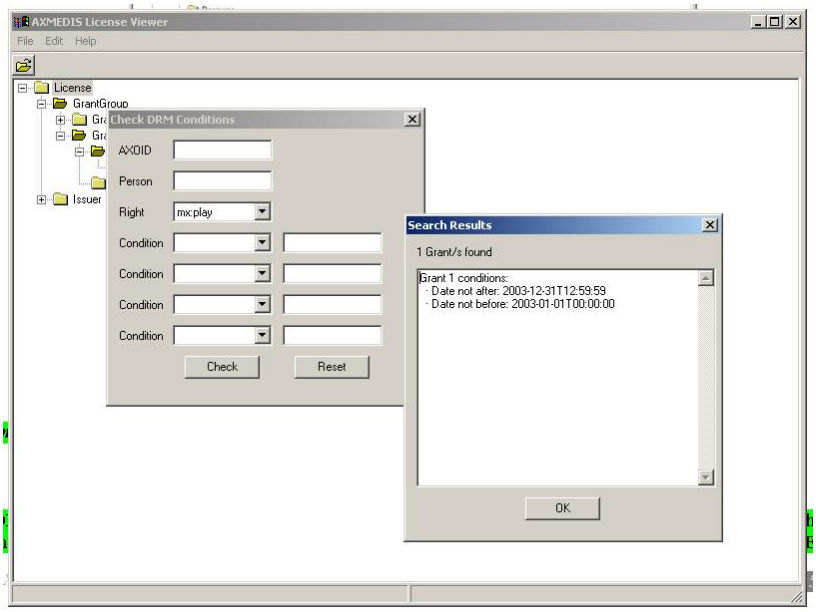


Figure Search functionality snapshot

Implemented features:

- License parsing using license model
- Visualisation of an MPEG-21 REL license in a tree format
- License checking according to available rights inside the license
  - A Check DRM conditions dialog is shown, only with the available rights in the license
    - AXOID
    - Person (principal)
    - Conditions Fee, territory, date, usage
    -
  - Given a license, ask if some rights are available under the license. As a response, the grants inside the license accomplishing the conditions are shown

Missing Features that will be implemented:

- Edition of licenses
- Improve license parsing support (related with license model)
- Improve license check, taking PAR and parent licenses into account (related with authorisation model)

7 Protection models for AXMEDIS objects repository

Protection models for AXMEDIS objects repository consists on the definition of a general framework for the creation and management of the licenses governing AXMEDIS objects. It currently makes use of other modules that will be described into this deliverable to provide its functionality, like the license model, the license database and the license generator.

The general protection model for AXMEDIS objects was specified in part E of specification deliverable, DE3.1.2. This model retrieves a license expressed in XML, according to the XML schemas that define MPEG-21 REL (there are three of them, r that is the core schema, sx that is the standard extension schema and mx that is the multimedia extension schema, as defined in [6]), and transforms it into an object model. The license model also provides functionalities for generating licenses in XML language and SQL

instructions that permit the storage of the licenses into a relational database. The relational model supported was also specified in DE3.1.2.

Nevertheless, this is not the only way of protecting AXMEDIS objects, as we have to take into account other active protection methods like encryption and decryption, key generation and secure communications. All these elements can be combined into AXMEDIS objects by using MPEG-21 IPMP (Intellectual property management and protection) and MPEG-21 REL (Rights Expression Language).

8 Automatic generation of contracts and licenses

In order to implement this module, we have to study current contracts structure and extract the more relevant information from them in order to create licenses expressed in MPEG-21 REL.

8.1 Technical Details

Reference to the AXFW location of the demonstrator	https://cvs.axmedis.org/repos/Applications/contractgen/
List of libraries used	wxWidgets xerces (SAX)
References to other major components needed	Licence model (https://cvs.axmedis.org/repos/Framework/source/licensemodel/)
Problems not solved	• Creation of complex contracts • Validation of fields introduced by the user • Dynamic creation of complex licenses
Configuration and execution context	Windows
Programming language	C++

8.2 Description Automatic generation of contracts and licenses

Contract generation is a stand-alone GUI application implemented using wxWidgets that makes use of the object oriented license model defined in specification document 3.1.2 part E. It provides the following functionality:

- Creation of final user licenses from contract information
- Creation of distributor licenses from contract information
- Creation of contracts

The extraction of information is currently done by the user of the application, who has to introduce the data in the text fields presented by the application. The result of the user operation can be stored as an XML file following MPEG-21 REL XML schema. The following figure shows a snippet of the Contract generator application interface:

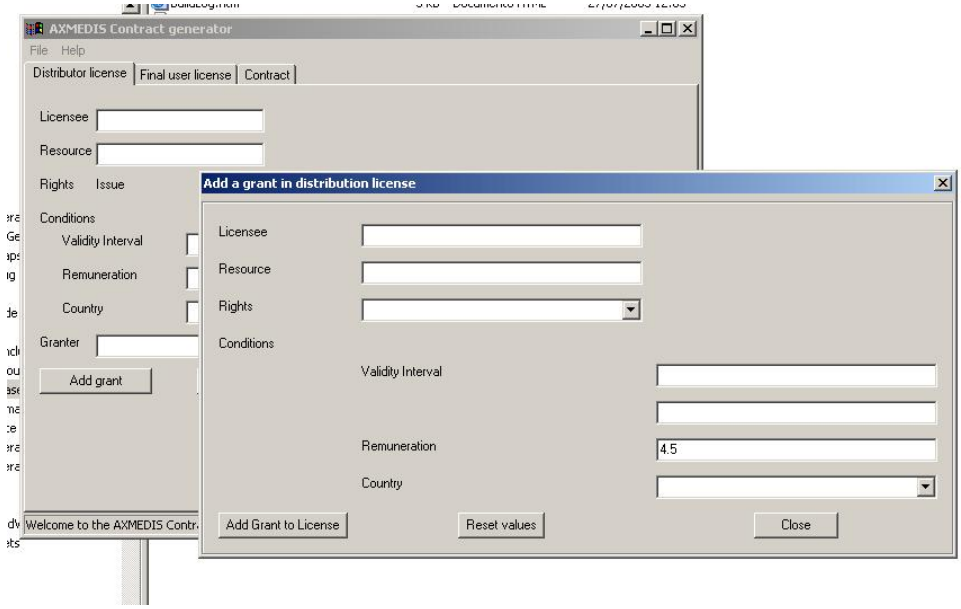


Figure Contract generator GUI

Implemented features:

- Basic creation of final user license using license model
  - ♣ Licenses are stored in MPEG-21 REL format
- Basic creation of distribution license using license model
  - ♣ Licenses are stored in MPEG-21 REL format
- Basic creation of contracts
  - ♣ Text format

Missing Features that will be implemented:

- Checking of format of input parameters
  - ♣ Dates, numbers
- Addition of conditions
  - ♣ Remuneration methods
  - ♣ Territory
- Automatic extraction of contract fields
- Construction of more complex contracts in text format

9 AXMEDIS Certification and Verification

AXMEDIS Certification and Verification consists of two different parts: one that will offer the AXCV functionalities and another one, which involves the Registration and Certification authorities of the AXMEDIS AXCS. Both of them are described in this section

9.1 Technical Details

Reference to the AXFW location of the demonstrator	https://cvs.axmedis.org/repos/Framework/source/axcs-axcv/
List of libraries used	Bouncy Castle cryptographic library JUnit (only for unit testing)
References to other major components needed	Axmedis Supervisor

	AXCS database AXCS database interface AXCS proxy
Problems not solved	• Adaptation to the implementation of the final AXCS database interface • Integration with AXMEDIS supervisor • Connection to the PMS Client AXCS proxy • Creation of the appropriate AXTID, according to standard ID syntax • Generation of tool enabling code (We must reach an agreement with the partner that implements the protection processor) • Generation of the appropriate (sequential) Certificate serial number • Implementation of PKCS Public Key integrity mode (no implementations found)
Configuration and execution context	Any platform
Programming language	Java

9.2 Description AXMEDIS Certification and Verification

The certification functionality of the AXCV involves, apart from some verification aspects, the creation of X.509 digital certificates for the AXMEDIS users. X.509 user certificates will be created at the user registration, through a Certification Authority platform. The issue of a user certificate may imply the need for manual verification of the user credentials, in particular when the user is a Business-to-Business user.

Once a user is registered in the system, if he installs and runs an AXMEDIS tool on a device, the creation of a certificate for the installed tool can be performed immediately, as all the information that must be checked is available in the system databases. To do so, a PKCS12 structure is created on the fly when a certification request is sent to the AXCV and returned back to the user.

Implemented features:

- Verification of users (in domain, if present)
- Certification of installed tools (tool, user and device)
- Verification of installed tools (tool, user and device)
- Generation of RSA key pairs for the creation of certificates
- Generation and storage of X.509v3 certificates:
  - AXCV self-signed certificate
  - Tool certificates
- Generation of password-protected PKCS12 for tool certificates and private keys
- Computation of enabling code according to the specification
- Base 64 encoding
- Web service interface

Missing Features that will be implemented:

- Adaptation to the implementation of the final AXCS database interface
- Integration with AXMEDIS supervisor
- Connection to the PMS Client AXCS proxy
- Creation of the appropriate AXTID, according to standard ID syntax
- Generation of tool enabling code (depends on protection processor)
- Implementation of PKCS Public Key integrity mode (no implementations found)

- Complete web service interface

9.3 Start-up of the Public Key Infrastructure

Registration and Certification authorities have been installed as part of the certification process needed by AXMEDIS. For the sack of simplicity, the Registration and Certification authorities have been installed in the same machine, but it is possible to separate their functionalities.

The Certification authority is currently available in the following URL: https://dmag.upf.edu:8443/pub. It uses OpenCA software and some adaptation will be needed in order to completely integrate it in AXMEDIS.

The functionalities available for the users (https://dmag.upf.edu:8443/pub) are the following:

- Get CA certificate – import it into the browser.
- Request a certificate – apply for Certification.
- Get requested certificate – import into the browser the signed certificate.
- Certificate requests list – view pending request.
- Valid certificates list – view currently valid certificate list.
- Export from PKCS#12 to PKCS#10 – export in a local file.
- Request the revocation of certificates.

The functionalities provided by the registration authority (https://dmag.upf.edu:8443/cgi-bin/ca/ca) are the following:

- Editing requests
- Approving requests
- Creating private keys with smart cards
- Deleting wrong requests
- Email users

The functionalities provided by the certification authority (https://dmag.upf.edu:8443/cgi-bin/ca/ca) are the following:

- Create certificates
- Create CRLs (Certificate Revocation Lists)

10 AXMEDIS Supervisor

This module provides the functionality needed to supervise user activity in the AXMEDIS system.

This module receives lists of action logs and supervisor input data information describing user activity over AXMEDIS objects, checks its correctness according to past actions and stores the information inside the AXMEDIS database.

10.1 Technical Details

Reference to the AXFW location of the demonstrator	https://cvs.axmedis.org/repos/Framework/source/axcs-axs/
List of libraries used	Bouncy Castle cryptographic library
References to other major components needed	AXCS database AXCS database interface AXCS proxy
Problems not solved	• Integration with database • Integration with AXMEDIS Certification and Verification

	• Connection to the PMS Client AXCS proxy
Configuration and execution context	Any platform
Programming language	Java

10.2 Description AXMEDIS Supervisor

It is implemented using the Java language and makes use of the Bouncy Castle cryptographic library to check the action log history provided by the user.

Implemented features:

- Verification of action logs list
- Insertion of action logs and supervisor input data in the database (although integration is missing)
- Generation of AXMEDIS object identifier
- Web Service Interface

Missing Features that will be implemented:

- Adaptation to the implementation of the final AXCS database interface
- Integration with AXMEDIS certification and verification
- Connection to the PMS Client AXCS proxy
- Complete Web Service interface for AXS module
- Perform the generation of object identifiers according to the specified format

11 Protection manager support

This module provides protection functionality to the AXMEDIS users inside the AXMEDIS system. It is a front end for the different modules inside it.

It currently provides the functionalities corresponding to the license manager and license generator modules.

11.1 Technical Details

Reference to the AXFW location of the demonstrator	https://cvs.axmedis.org/repos/Applications/pms/
List of libraries used	Xerces gSoap
References to other major components needed	License manager License generator
Problems not solved	• Provide different versions of PMS module • Connect different versions of PMS module
Configuration and execution context	
Programming language	C++

11.2 Description Protection manager support

It is implemented using the C++ language and it has been also integrated with gsoap library and initial web service functionality is provided, although it has to be completed with other modules that have to be integrated. The details of each module below PMS are provided in the corresponding section.

Implemented features:

- Creation of final user license and distributor license
- Storage of license
- Retrieval of license (if the license id is provided)

Missing Features that will be implemented:

- Integration of other modules below PMS (as specified in document DE3.1.2)
  - ♣ Key Generation
  - ♣ Secure caching
- Complete license creation and management

12 AXCS proxy

AXCSProxy is a module that sits between a client application and a server application. It receives all requests from the client application, and it forwards these requests to the server application. In this case the client application is the PMS module, and the server application is the AXCS module.

12.1 Technical Details

Reference to the AXFW location of the demonstrator	N.A.
List of libraries used	GSoap
References to other major components needed	PMS AXCS
Problems not solved	
Configuration and execution context	
Programming language	C++

12.2 Description AXCS Proxy

This module will be implemented using gsoap in order to be able to connect it with the PMS client and provide the corresponding connection with AXCS.

13 DRM support

This module provides protection functionality to the AXMEDIS users inside the AXMEDIS system. It is located between PMS and the different modules below it.

It currently provides the functionalities corresponding to the license manager and license generator modules.

13.1 Technical Details

Reference to the AXFW location of the demonstrator	https://cvs.axmedis.org/repos/Framework/source/drmsupport/
List of libraries used	
References to other major components needed	License manager License generator
Problems not solved	• Provide different versions of DRM support module
Configuration and execution context	
Programming language	C++

13.2 Description DRM Support

It is implemented using the C++, although it has to be completed with other modules that have to be integrated. The details of each module below DRM support are provided in the corresponding section.

Implemented features:

- Creation of final user licenses and distributor licenses
- Storage of licenses
- Retrieval of licenses (if the license id is provided)

Missing Features that will be implemented:

- Integration of other modules below PMS (as specified in document DE3.1.2)
  - ♣ Key Generation
  - ♣ Secure caching
- Complete license creation and management

14 License verificator and Authorisation support

This section describes how license verification should be done in several scenarios.

DelegationControl (element within the grant or grantGroup, delegates the entire grant or grantGroup to the specified principal) and Issue right provide many of the same features. There are different cases.

14.1 Case 1: Distribution scenario using the issue right

Example

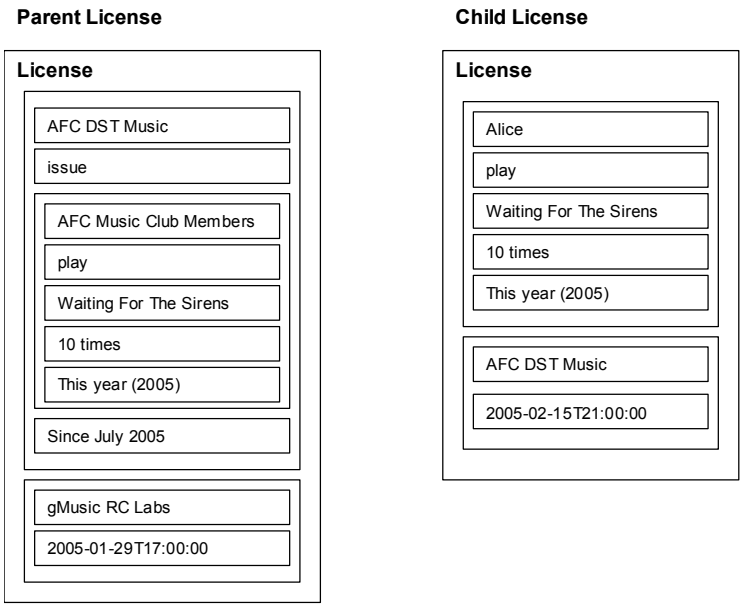


Figure License distribution using Issue right

License Verification algorithm

1. Issuer (Child License) is Equal to Principal (Parent License)
2. Right (Parent License) is Issue

3. Grant (Child License) is Resultant from Resource (Parent License)
   3.1. Principal (within resource element of Parent License) Surpasses Principal (Child License) or Principal (within resource element of Parent License) is absent
   3.2. Right (within resource element of Parent License) is Equal to Right (Child License)
   3.3. Resource (within resource element of Parent License) is Equal to Resource (Child License)
   3.4. Conditions (within resource element of Parent License) are Equal to Conditions (Child License)
4. Conditions (Parent License) are Satisfied
5. (timeOfIssue (Child License) > timeOfIssue (Parent License)) & (timeOfIssue (Child License) is within the interval of the verification process)

14.2 Case 2: Distribution scenario using delegationControl element

A license issuer can impose constraints on delegation:
- Controls on adding or changing conditions during delegation
- The allowable depth of the delegation chain
- The principal to whom the grant or grantGroup may be delegated

When a principal delegates a grant the delegated license must contain a delegationControl element that is compatible with the delegationControl element in original license. The delegationControl in the delegated license must at least as restrictive as in the original license (the principal may add additional restrictions).
Child elements of delegationControl:
- ConditionIncremental element allows conditions to be added during delegation.
- ConditionUnchanged element to specifically prevent conditions from being added during delegation. Adding a conditionUnchanged in a delegationControl within a grant implies that if this grant is delegated no more conditions can be added in the grant of the new license.
- DepthConstraint element to specify the number of times the grant could be delegated.
- ToConstraint element to specify the principals to whom the grant may be delegated.

License Verification algorithm
1. Principal (Child License) is Allowed by delegationControl (Parent License) if toConstraint element is present or is anyone if absent
2. Right (Parent License) is Equal to Right (Child License)
3. Grant (Parent License) has the element delegationControl
4. Resource (Child License) is Equal to Resource (Parent License)
5. Conditions (Parent License) are Allowed by delegationControl (Parent License)
   5.1. If toConstraint is present in delegationControl (Parent License), then conditions Conditions (Child License) are at least the same of Conditions (Parent License) and the principal (ChildLicense) has to be Allowed by delgationControl (Parent License) as follows:
      5.1.1. If forAll with a pattern within toConstraint element (Parent License), then Principal (Child License) Satisfies the Pattern
      5.1.2. If Principal within toConstraint element (Parent License), then it is Equal to Principal (Child License)
   5.2. If conditionUnchanged is present in delegationControl (Parent License), then Conditions (Parent License) are Equal to Conditions (Child License)
   5.3. If conditionIncremental is present in delegationControl (Parent License), then Conditions (Child License) are at least the same of Conditions (Parent License)
   5.4. If depthConstraint is present in delegationControl (Parent License), then:
      depthIncremental(ChildLicense) = depthIncremental(ParentLicense) - 1
   5.5. If dcConstraint is present in delegationControl (Parent License), then:
      5.5.1. Principal (Child License) is allowed by dcConstraint

5.5.2. Conditions (Child License) are allowed by dcConstraint

Examples

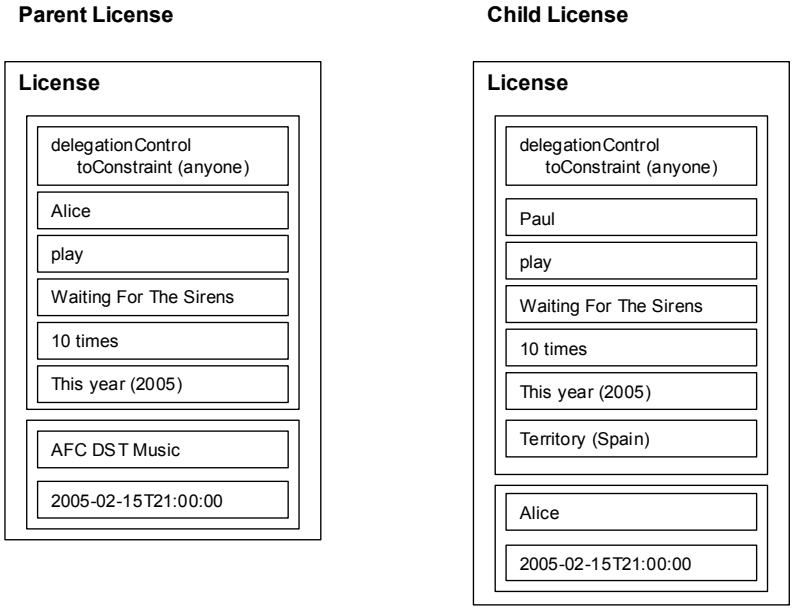


Figure License distribution using delegationControl element with toConstraint

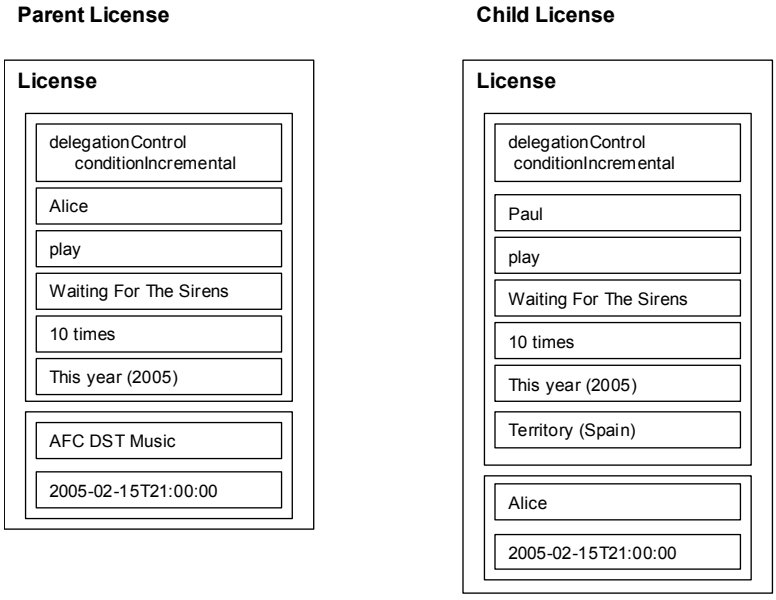


Figure License distribution using delegationControl element with conditionIncremental

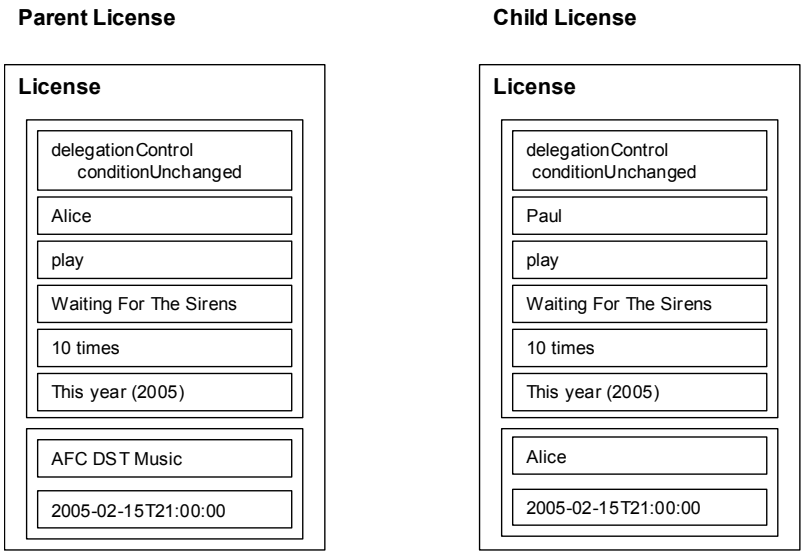


Figure License distribution using delegationControl element with conditionUnchanged

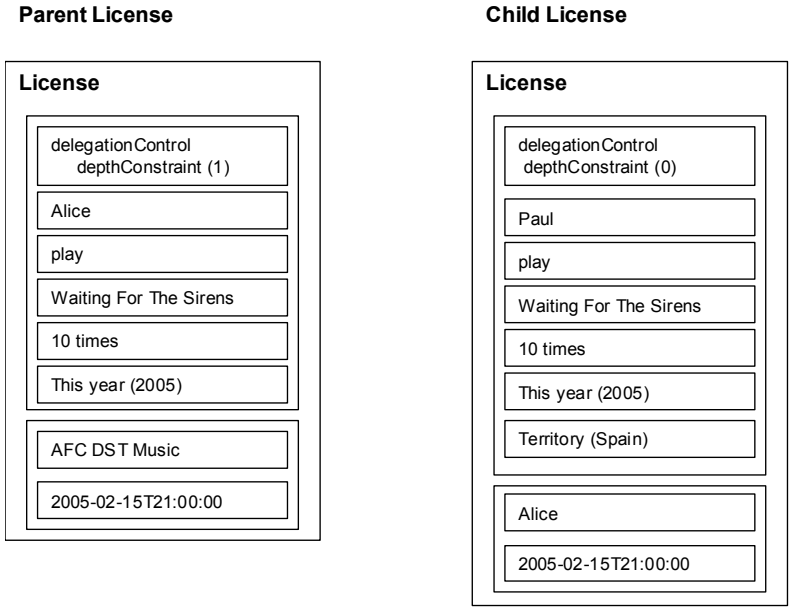


Figure License distribution using delegationControl element with depthConstraint

14.3 Case 3: Offers

An offer is a license that grants the “obtain” right. By exercising this right, a principal may obtain the grant or grantGroup that is listed as a resource in the offer. The obtain right only applies to grants or grantGroups.

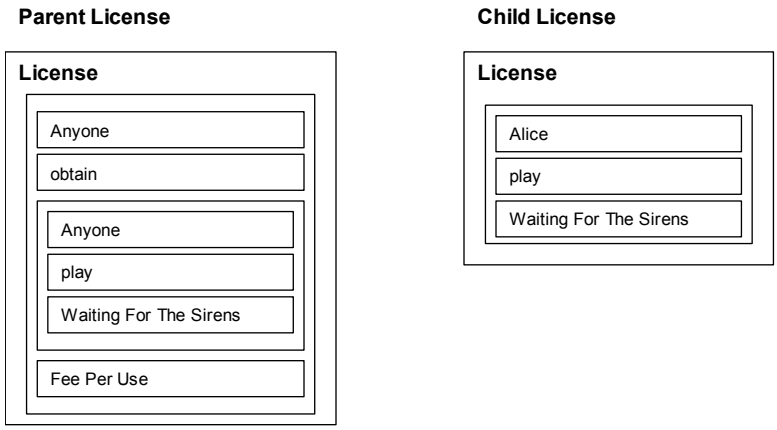


Figure Offers described in licenses

License Verification algorithm

1. Principal (within resource element of Parent License) Surpasses Principal (Child License) or Principal (within resource element of Parent License) is absent
2. Right (Child License) is Equal to Right (within resource element of Parent License)
3. Resource (Child License) is Equal to Resource (within resource element of Parent License)
4. Conditions (Child License) are Equal to Conditions (within resource element of Parent License)
5. Right (Parent License) is Obtain
6. Conditions (Parent License) are Satisfied

15 Secure Communication Support

This module is a multithreaded client/server application that provides secure communications session using openssl library.

15.1 Technical Details

Reference to the AXFW location of the demonstrator	https://cvs.axmedis.org/repos/Framework/source/seccommsup/
List of libraries used	openssl
References to other major components needed	PMS
Problems not solved	
Configuration and execution context	Windows
Programming language	C/C++

15.2 Description Secure Communication Support

The operation of this module is as follows:
It manages several secure communications using the Session class. This class has the attributes for supporting the establishment of secure communication, but they are private, so the SecureCommClient and SecureCommServer classes have to be “friend” classes of Session. This privacy is needed because this class is needed to return a session in a particular state to the application using the module, and it avoids modifications of the class from the application side of these critical attributes used in the secure communication.

The module keeps the sessions into four map data structures. They organise the information into a tree structure where every value is associated to an identifier, which allows faster access. There are different instances of the map structure, storing sessions in a specific state.

When the application wants to get some session that are in a specific state, it must call to the operation that returns all sessions that are in this state using avector data structure.

Implemented features:

- Client application
- Server application
- Secure session functionalities

The following diagrams show the protocol implemented by the client and the server applications respectively.

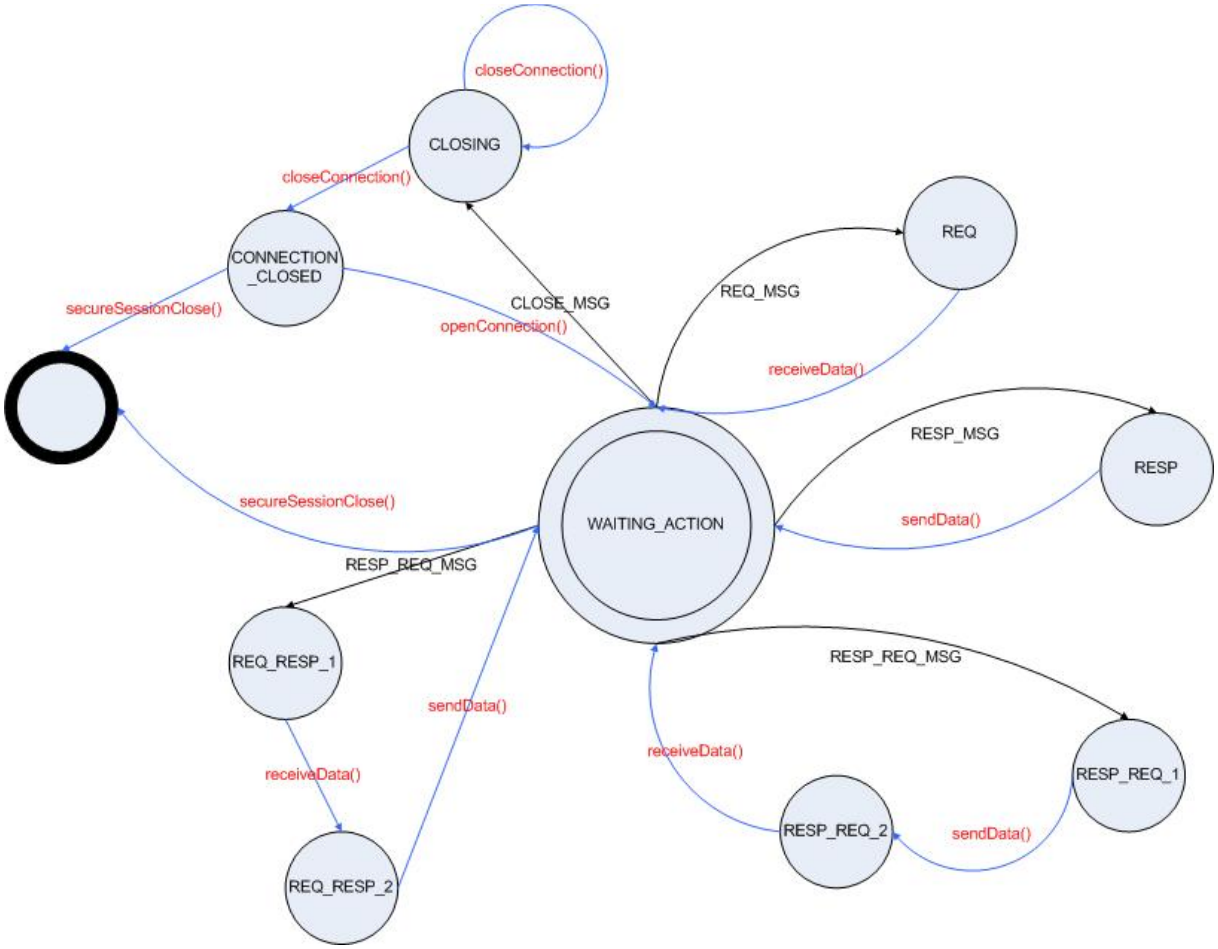


Figure Client protocol

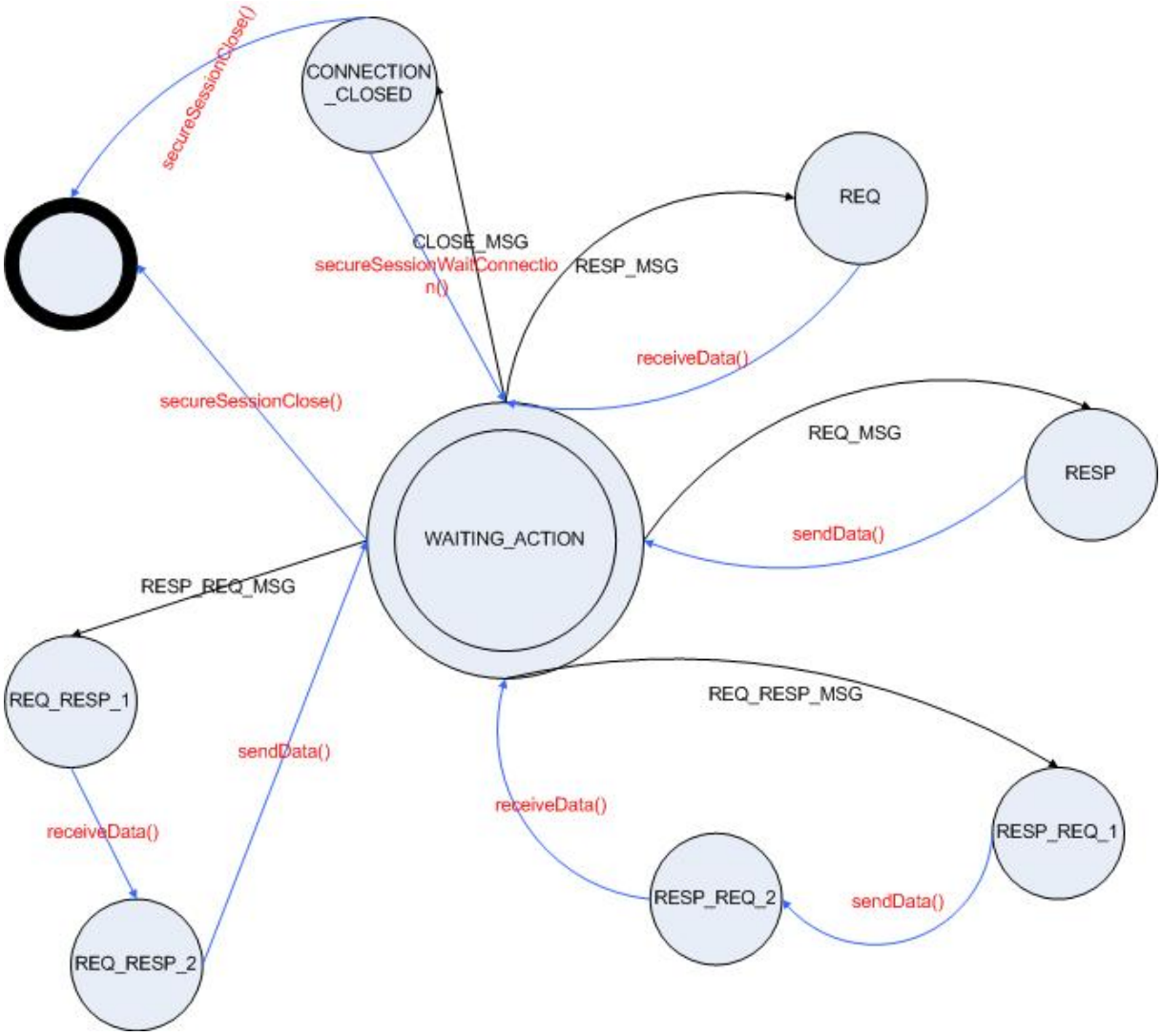


Figure Server Protocol

16 Encryption / Decryption Support

This module uses openssl library in order to encrypt and decrypt files using symmetric and asymmetric key algorithms. It also provides the possibility of signing

16.1 Technical Details

Reference to the AXFW location of the demonstrator	https://cvs.axmedis.org/repos/Framework/source/encdecsup/
List of libraries used	openssl
References to other major components needed	
Problems not solved	
Configuration and execution context	Windows
Programming language	C/C++

16.2 Description Encryption / Decryption Support

Implemented features:

- Symmetric encryption
- Symmetric decryption
- Asymmetric encryption with RSA
- Asymmetric decryption with RSA
- Digest generation
- Digital signature

17 Key generator

This module has been implemented using the openssl library. It generates symmetric keys for protecting AXMEDIS objects and also generates asymmetric keys for RSA and DSA algorithms.

This module is part of the active protection mechanisms needed inside AXMEDIS.

17.1 Technical Details

Reference to the AXFW location of the demonstrator	https://cvs.axmedis.org/repos/Framework/source/keygen/
List of libraries used	openssl
References to other major components needed	PMS
Problems not solved	
Configuration and execution context	Windows
Programming language	C/C++

17.2 Description Key Generator

Implemented features:

- Generation of symmetric keys
- Generation of asymmetric keys for RSA algorithm
- Generation of asymmetric keys for DSA algorithm

Missing Features that will be implemented:

- Integration with PMS

18 License manager

License manager module is based in the rights expression language MPEG-21 REL. It can store and retrieve licenses from a mysql database. It also provides the functionality for parsing MPEG-21 REL licenses by means of SAX parser contained in Xerces.

18.1 Technical Details

Reference to the AXFW location of the demonstrator	https://cvs.axmedis.org/repos/Framework/source/licensemanager/
List of libraries used	Mysql xerces
References to other major components needed	
Problems not solved	

Configuration and execution context	Windows
Programming language	C/C++

18.2 Description License Manager

Implemented features:

- Storage of a license
- Retrieval of a license, given its license id
- Parsing of a license, returning a license model

Missing Features that will be implemented:

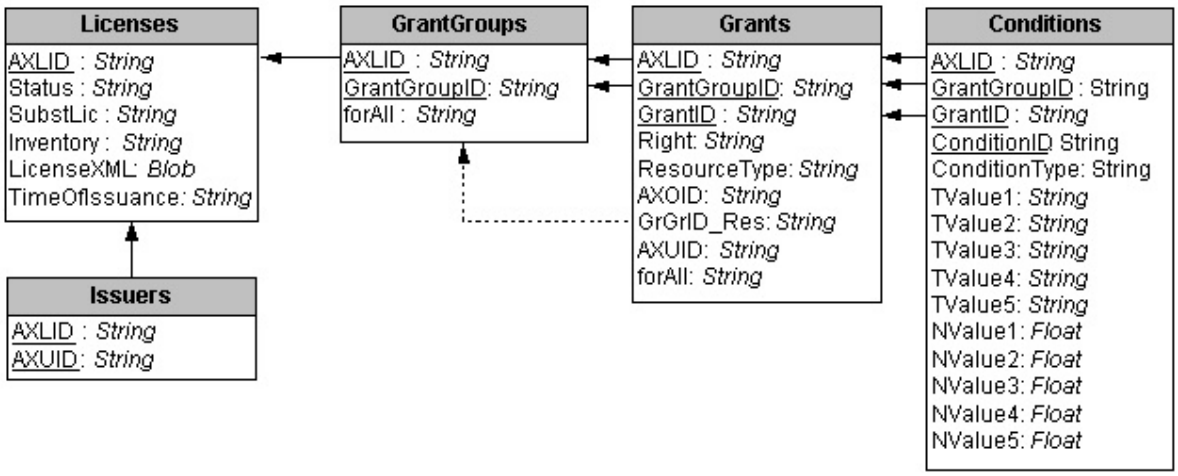
- Give support to other databases using standard interfaces like ODBC

19 License database

The license database module is the entity relationship structure of the tables that will store the license in a relational database.

To represent the content of a license in an Entity-Relationship diagram, we have to focus on the relations with a multiplicity 0..n. These relations show us the number of different tables that we need to store the represented information. The relations with a multiplicity of 1 – 1 can be stored always in the same table.

The next diagram shows how to create the different tables to store the license information. This solution provides the model for storing End-user Licenses, and also for storing Distributor Licenses.



ER diagram for licenses

19.1 Technical Details

Reference to the AXFW location of the demonstrator	https://cvs.axmedis.org/repos/Framework/source/axdb-license/
List of libraries used	mysql
References to other major components needed	
Problems not solved	
Configuration and execution context	
Programming language	Java

19.2 Description License Database

A generic interface, database independent, has been implemented using the Java language. Moreover, a specific implementation for accessing a mySQL database is also provided.

Several classes have been implemented, one for each table, providing storage and retrieval functionalities.

Implemented features:

- Storage of a license and the related fields
- Retrieval of a license, given its license id

Missing Features that will be implemented:

- Give support to other databases through the corresponding JDBC drivers

20 License generator

License generator module is based on the rights expression language MPEG-21 REL. It can create an object structure that represents a license and can convert from that object model to an MPEG-21 REL license expressed in XML. It also provides functionalities to convert that object model into SQL statements that store the corresponding license in a relational database (the structure of this database is described in License Database module section of this document).

20.1 Technical Details

Reference to the AXFW location of the demonstrator	https://cvs.axmedis.org/repos/Framework/source/licensemodel/ https://cvs.axmedis.org/repos/Framework/source/licensecreator/
List of libraries used	mysql Xerces
References to other major components needed	
Problems not solved	
Configuration and execution context	
Programming language	C++

20.2 Description License Generator

Implemented features:

- Creation of a license in MPEG-21 REL format
- Creation of the SQL statements needed to stored a license in the license database

Missing Features that will be implemented:

- Support more license fields

21 RDD Server

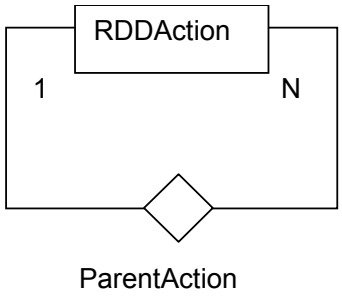
RDD server module is based in the rights vocabulary defined in MPEG-21 RDD (Rights Data Dictionary) to support the MPEG-21 REL. It stores and returns the list of parent rights (actions in MPEG-21 RDD context) of a given right (action). It is used by the Authorisation model module, which has to be developed for the next period (November).

21.1 Technical Details

Reference to the AXFW location of the demonstrator	https://cvs.axmedis.org/repos/Framework/source/rddserver/
List of libraries used	Mysql
References to other major components needed	
Problems not solved	
Configuration and execution context	
Programming language	C++

21.2 Description RDD Server

We have described the database, which represents the rights present in the multimedia extension of MPEG-21 REL. The Entity Relationship model for these tables is shown in the next figure.



Implemented features:

- Search parent right in a database of rights according to relationships between rights defined in MPEG-21 RDD

22 Protection Processor

22.1 Technical Details

Reference to the AXFW location of the demonstrator	
List of libraries used	Xerces-C++
References to other major components needed	
Problems not solved	
Configuration and execution context	
Programming language	C++

22.2 Description of Protection processor module

Implemented features:

- Parsing of IPMP descriptor
- Device fingerprint estimation
- Device profile extraction
- Basic implementation of protection commands

Missing Features that will be implemented:

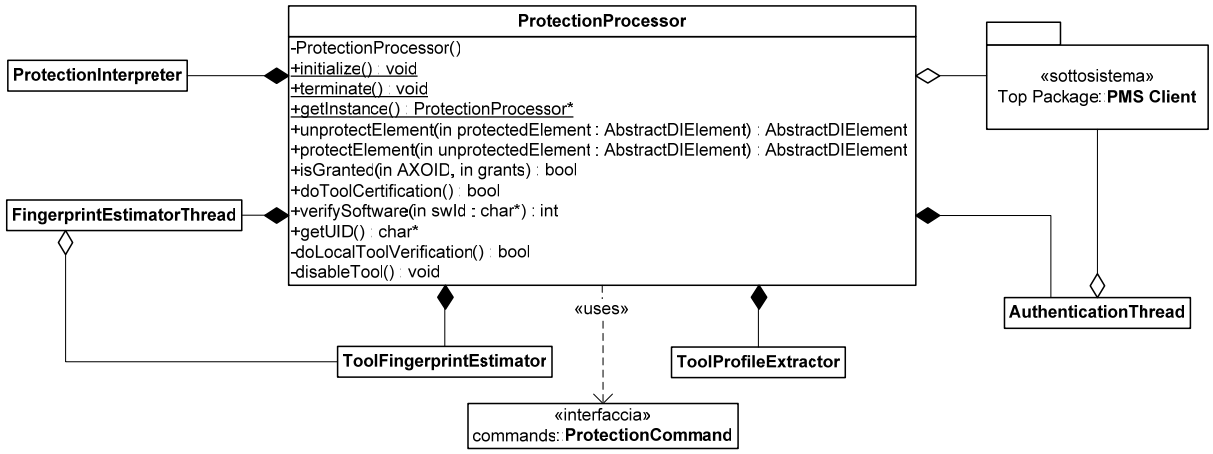
- Protection and un-protection of MPEG21 DIDL element
- Management of dynamic protection commands
- Portability on non-Windows platform

22.3 General description and architecture

This module is under development. It has been analyzed and parts thereof have been realized as prototypes. As described in the specification, Protection Processor is in charge of providing several services related to content protection. In particular, it deal with the following aspects:

1. Content protection/unprotection through coordination of protection tools, e.g. encryption, scramble, etc…
2. Interpretation of IPMP information
3. Estimation of hardware and software fingerprint
4. Extraction of hardware and software profile
5. Verification of external software such as plug-ins
6. Client-side certification of AXMEDIS tools (e.g. editors, players, etc…)
7. Client-side verification/authorization of AXMEDIS tools (e.g. editors, players, etc…)
8. Exposition of grant request functionality
9. Determination of user identity

Protection Processor is composed by several modules to better tackle the above mentioned point. Each module will cover a specific service. The Protection Processor coordinates all the modules and the latter is the unique available interface to the user.
The following figure shows the general class diagram:



As shown above, Protection Processor provides the following functions to the user:

- *protectElement*/*unprotectElement* (1. of list above)
- *isGranted* (8.)
- *doToolCertification* (6.)
- *verifySoftware* (5.)
- *getUID* (9.)

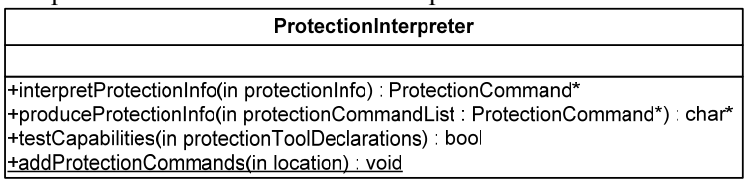
Moreover, Protection Processor internally performs the other tasks through the following support classes and internal functions:

- *doLocalToolVerification* and *AuthenticationThread* (7.)
- *ProtectionInterpreter* (2.)
- *ToolFingerprintEstimator* and *FingerprintEstimatorThread* (3.)
- *ToolProfileExtractor* (4.)

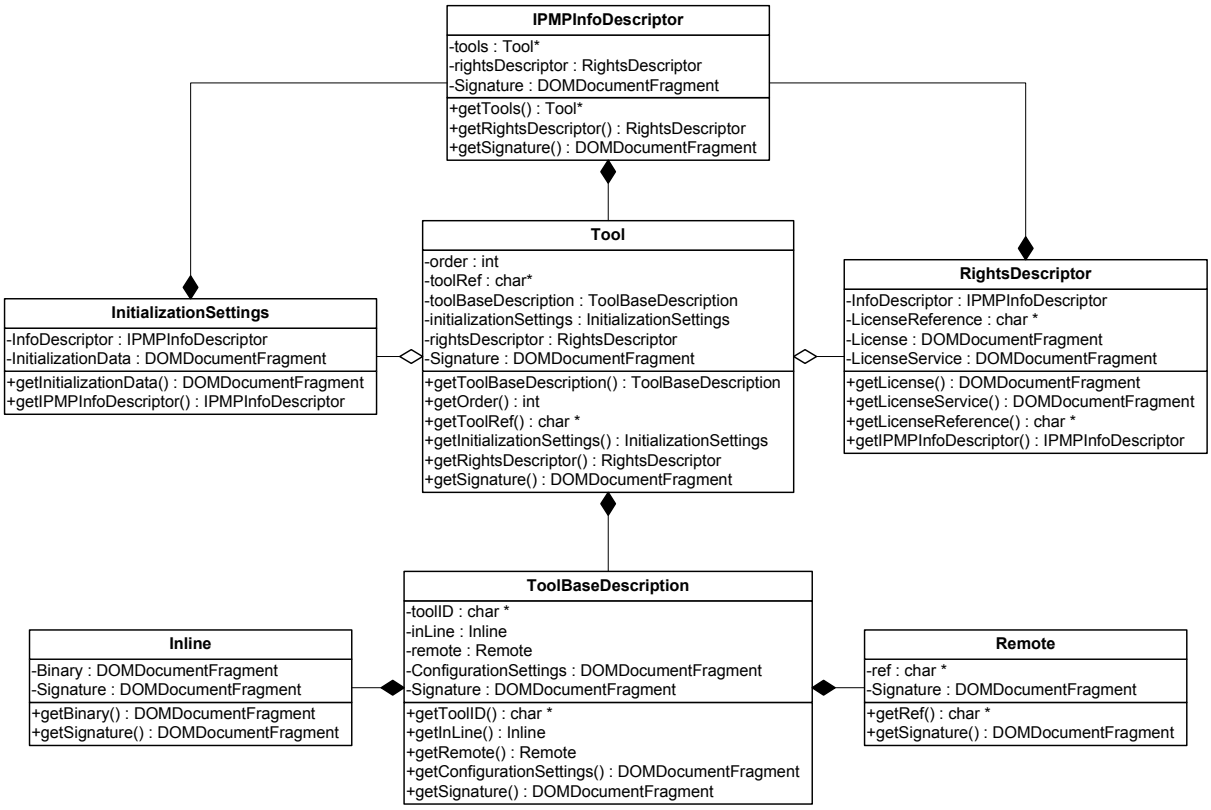
In the following, the modules, which reached the stage of first prototype, will be presented.

22.4 ProtectionInterpreter

In the next picture, the expected interface of ProtectionInterpreter is shown:



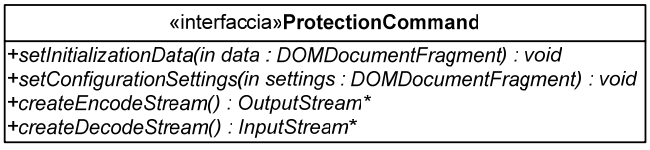
Nowadays, this interface has not been yet implemented because not all the needed interactions with other modules have been defined. However, the MPEG-21 IPMP information parser has been developed.



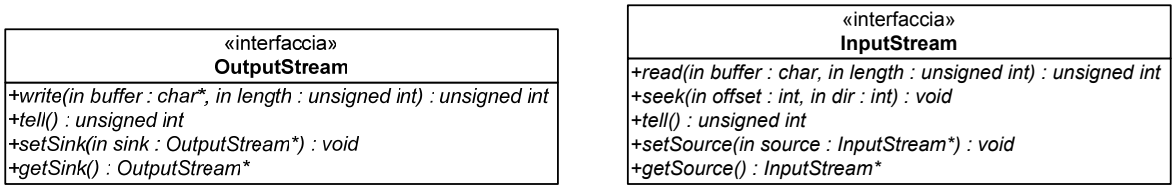
This parser allows loading in memory an object model of the protection information expressed using MPEG-21 IPMP schemas. This object classes represent the main elements defined in MPEG-21 IPMP. The structure is mainly used to retrieve the ids of protection tools and to obtain the settings for initializing and configuring the tools. These settings are expressed in XML therefore they are stored in a DOM structures.
Using the above describe information the ProtectionInterpreter is able to load and configure the protection commands needed to protect/unprotect a given element.

22.5 Protection commands

A first standard interface for all the protection commands has been designed:

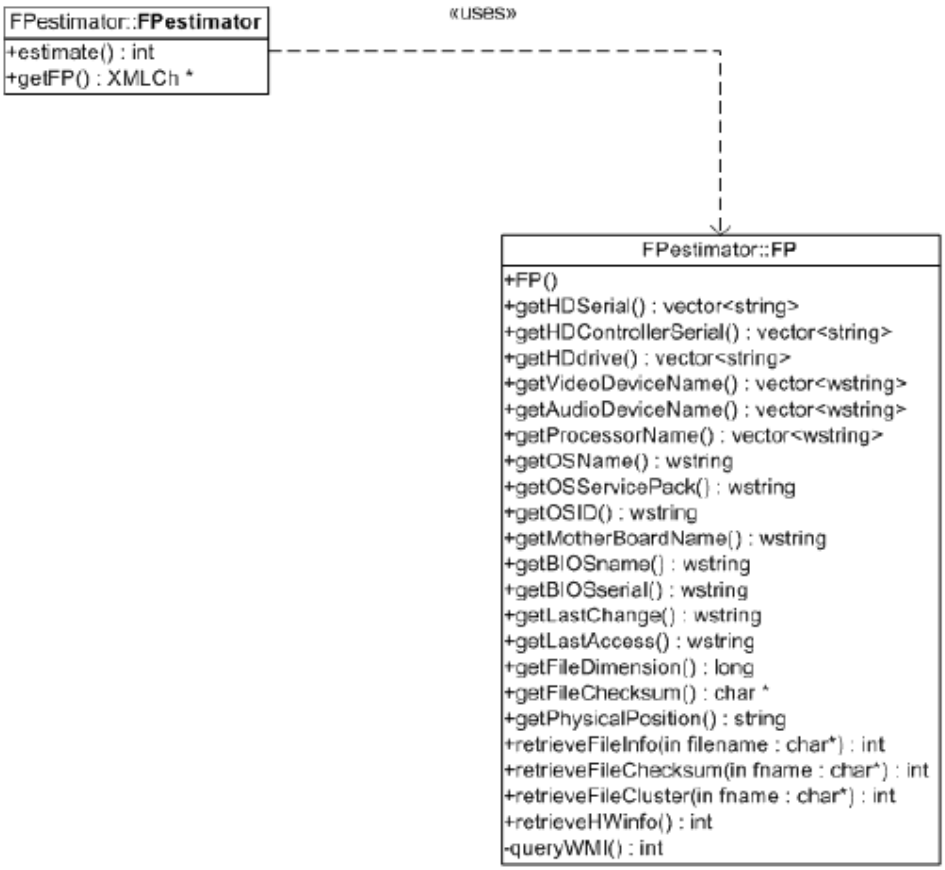


This interface exposes to method to sets initialization and configuration settings (*setConfigurationSettings* and *setInitializationData*). This functions allow to configure a given protection tool. Moreover, the interface provides two functions, which allow creating streams to protect and unprotect given content. The stream approach has been adopted to allow the management of huge-size content without the need of using big amount of memory or the need of saving unprotected version of the content on a mass-storage support.
The streams created by protection commands can be composed together thus allowing the application of more than a protection tool to the same element. The composition of this stream should be made in accordance with IPMP information. The basic interface for the input and output streams are:



As depicted in the two above picture, the basic interfaces for streams provide, in addition to the usual stream functions (for writing, reading, determining the position in the stream, etc…), functions for binding different streams each others (*setSink* and *setSource*). In particular, *setSink* sets the stream in which the actual one has to write the encoded content; *setSource* sets the stream from which the actual one has to read the content to be unprotected.

22.6 ToolFingerprintEstimator



As depicted in the figure above, the tool fingerprint estimator module is composed of two classes: *ToolFingerprintEstimator* and *TraitsEstimator*. The former class is the one used by *ProtectionProcessor* to obtain the fingerprint of the tool in XML. The latter is a utility class which is in charge of effectively recovering information on the tool. That is, *ToolFingeprintEstimator* has the knowledge to format the needed information in an XML structure, instead *TraitsEstimator* owns the knowledge to get the needed information from the operative system and the hardware platform. It is evident that the former is platform independent while the latter has to be defined for each platform the AXMEDIS framework has to work on.

23 MPEG-21 core experiment on MPEG-21 IPMP

As reported in DE4.1.1, during the definition of the AXMEDIS Data Model, lacks of expressiveness have been found out in the MPEG-21 DIDL IPMP schema. In particular, it was evident the difficulty to associate accessible metadata to MPEG-21 DIDL element once they have been protected. Due to the previous observation suggested by DSI at 72nd MPEG Meeting in Busan (Korea) (M12084 - AXMEDIS EC project and data model), an MPEG-21 core experiment named "CE on the indexing of IPMP protected DIDL content" (N7198) has been activated. DSI, FUPF and EXITECH have taken active part to the CE thus obtaining the amendment of MPEG-21 IPMP DIDL during the 73rd MPEG Meeting in Poznan (Poland). In particular a placeholder for accessible metadata has been added to the XML representation of protected DIDL element (N7426). This placeholder will be used in AXMEDIS to exposes public metadata of protected content.

24 Content Authentication and Verification

To verify content authenticity perturbations of the fingerprinting are analysed. One simple possibility is to use the distance between the original and the calculated fingerprinting together with a fixed threshold to distinguish between valid or invalid operations. This trivial description however does not reflect the difficulties of this process: Some valid content processing operations might affect the fingerprint in the same manner as some other invalid operations.

Due to the difficulties of defining an objective authenticity of images [74] proposed a concept called feature authenticity A_f :

$$A_f = 1 - \left\| feature(C_0) - feature(C_m) \right\|_{normalized}$$

where C_0 is the original document and C_m the (potentially) modified one, whose authenticity has to be validated. In [74] the case of still images is considered. The aim is to find a set of features, which closely approximate the image authenticity curve for certain modifications. The image authenticity curves map the modification to the normalized authenticity value $A_f \in [0,1]$. This authentication curve has to be defined experimentally for acceptable and unacceptable modifications. A related optimal set of features is identified. However, in practical applications this authenticity function A_f also has to be mapped to $[0,1]$ (e.g. by a threshold function) as content either is authentic or not. A huge variety exists for deriving relevant features and their post-processing. This feature authenticity A_f is used to draw a so-called authenticity vs. modification curve. This curve should support the identification of an optimal feature set.

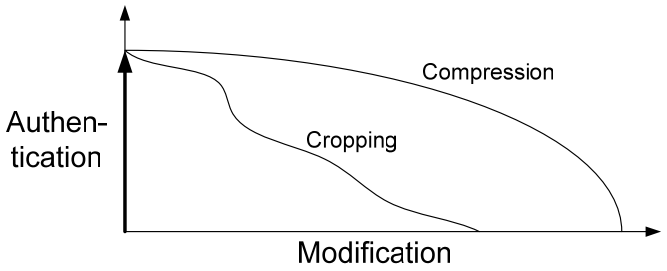


Figure Authenticity vs. Modification Curve as proposed by [74]

The specific algorithms and methods for individual content types together with a description of the scenario "Application: Content Description and Identification" are given in DE 4.2.1: Content Indexing, Monitoring and Querying.

24.1 Audio Fingerprinting

In general every audio fingerprinting system consists of a feature extraction and matching algorithm. The following sections describe the various building blocks of the audio fingerprint system developed by IGD.

Feature Extracting Block

The feature extraction block comprises the following sections.

- Data preparation
- Segmentation into Frames
- Overlapping of the Frames
- Transformation of the Individual Frames
- Extraction of the Features
- Processing and Modelling of the Features

Matching Algorithm and Distance Metric
After the calculation of the audio fingerprint, a matching with stored fingerprints is performed. For this the following steps are required.

- Matching Algorithm
- Decision Block

24.2 Image Fingerprinting

In general every audio fingerprinting system consists of a feature extraction and matching algorithm. The following sections describe the various building blocks of the audio fingerprint system developed by IGD.

1. Identification of suitable features for the calculation of image fingerprints: The basic features are higher order statistics/moments: cumulants.

2. Development and implementation of an image fingerprinting algorithm based on cumulants. The original image is rescaled and tiled. For each tile the forth order statistics (cumulants) are calculated.

3. First analysis of the implemented algorithm: Based on the some internal test images the developed algorithm was analysed and its performance has been successfully compared with other state-of-the-art algorithms.

24.3 Video fingerprinting

In general every video fingerprinting system consists of a feature extraction and matching algorithm. The following sections describe the various building blocks of the video fingerprint system developed by FHGIGD.

- Identification of suitable features for the calculation of video fingerprints: The basic feature is the similarity between different blocks in consecutive frames. This temporal similarity sequences is chosen due to is discriminability.

- Development and implementation of a video fingerprinting algorithm based on the temporal block similarity sequence.

- First analysis of the implemented algorithm: Based on the some internal test images the developed algorithm was analysed and its performance has been successfully compared with other state-of-the-art algorithms.

24.4 Prototype description

For each of the developed algorithms there will be a demonstration tool available. This demonstration tool will be available for the media types:

- audio
- images
- video

The principle demonstration procedure is the same for the different kinds of content:

1. Content is be loaded.
2. The fingerprint is calculated for the content.
3. A second piece of content is loaded (manipulated or similar).
4. The fingerprint for the second content is calculated.
5. The fingerprints are compared to identify if the two pieces are the same or similar.

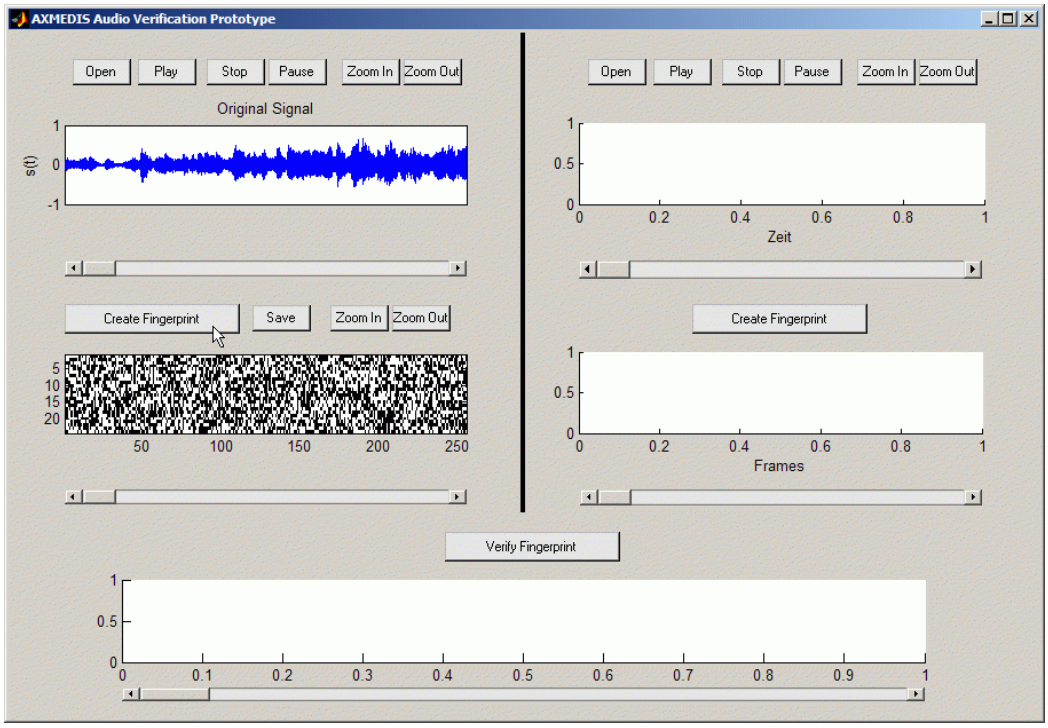
The implementation was done in MatLab[8]. The implemented algorithms and as well a graphical user interface for the demonstration can be found in the versioning control system. For the demonstration minor modifications of the source code and the graphical user interfaces are need.

Below is a detailed description of the implemented prototype. The description is based on the user related aspects not considering technical details. The location of the code is described below in section 24.5. Section 24.6 contains a short list of the implemented functionalities and the open tasks.

[8] MatLab is a tool for the development and rapid prototyping of research software (see http://www.mathworks.com).

24.4.1 Audio Fingerprinting Demonstration

The demonstrator is started in MatLab.

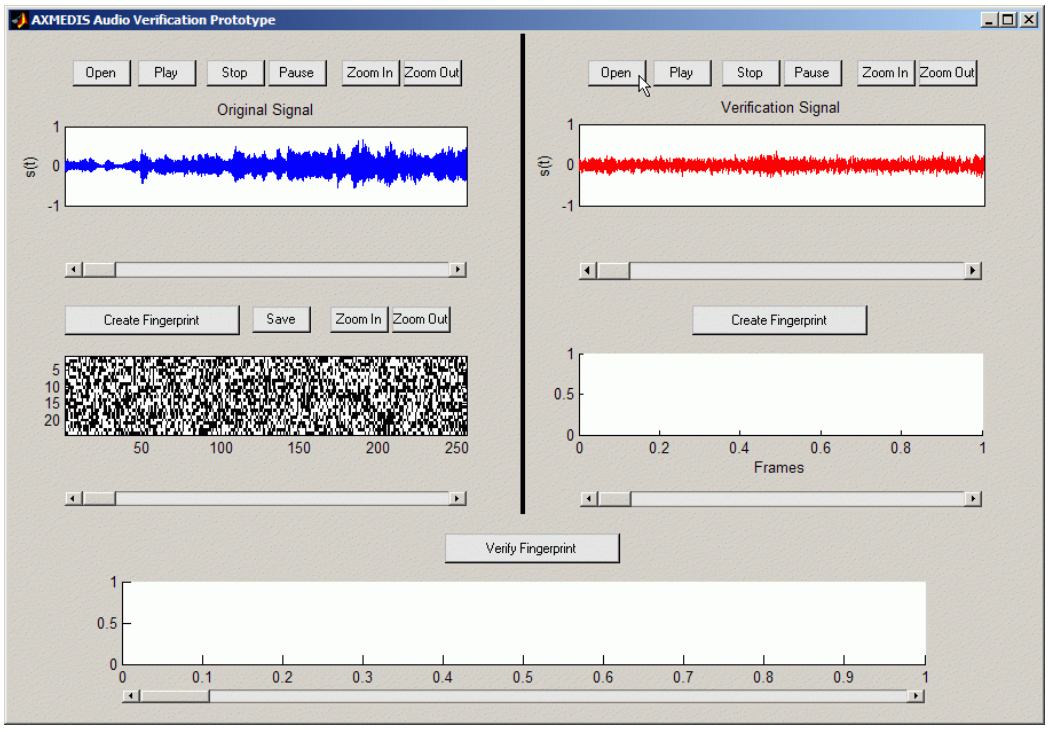


The main window is split in three parts:

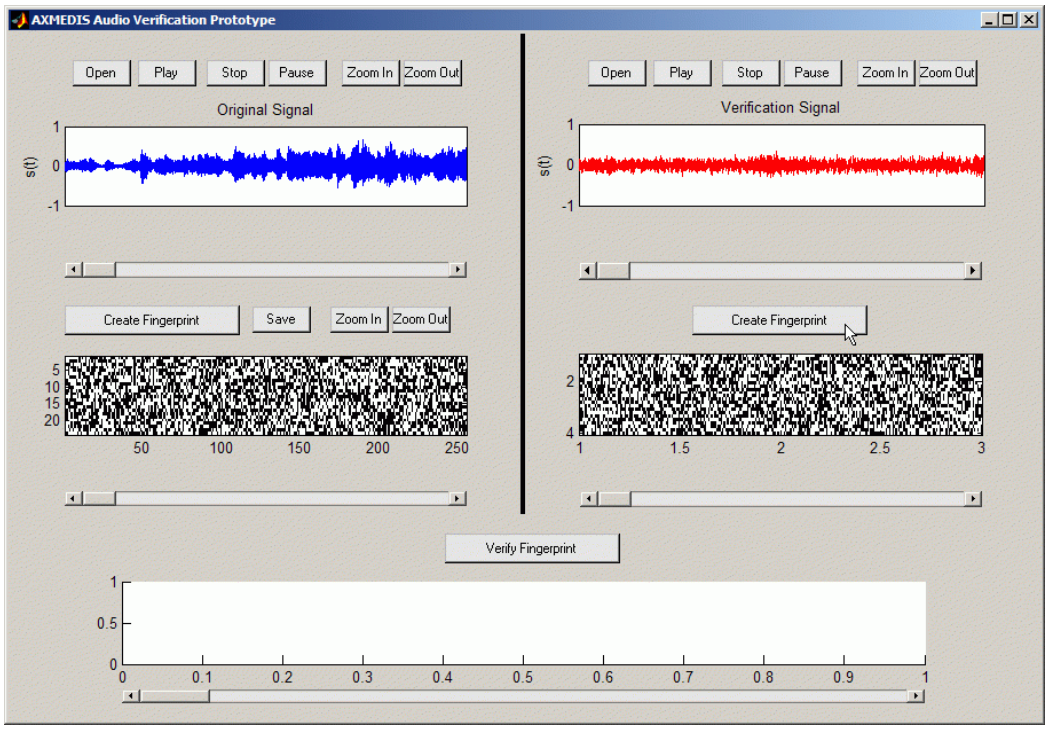
- The (upper) left part of the windows shows the information related to the original signal. The audio can be played and is also visualized as a 1D-temporal function. For this audio signal, the fingerprint can be calculated and viewed.
- The (upper) right part of the window contains the information related to the signal that should be verified. This audio signal is the processed or manipulated. The signal as well as the corresponding fingerprint can be viewed.
- The lower part contains the difference between the fingerprint of the original and the fingerprint of the signal that should be verified.

The demonstration starts with loading the original signal (as shown above). For this signal the fingerprint is calculated.

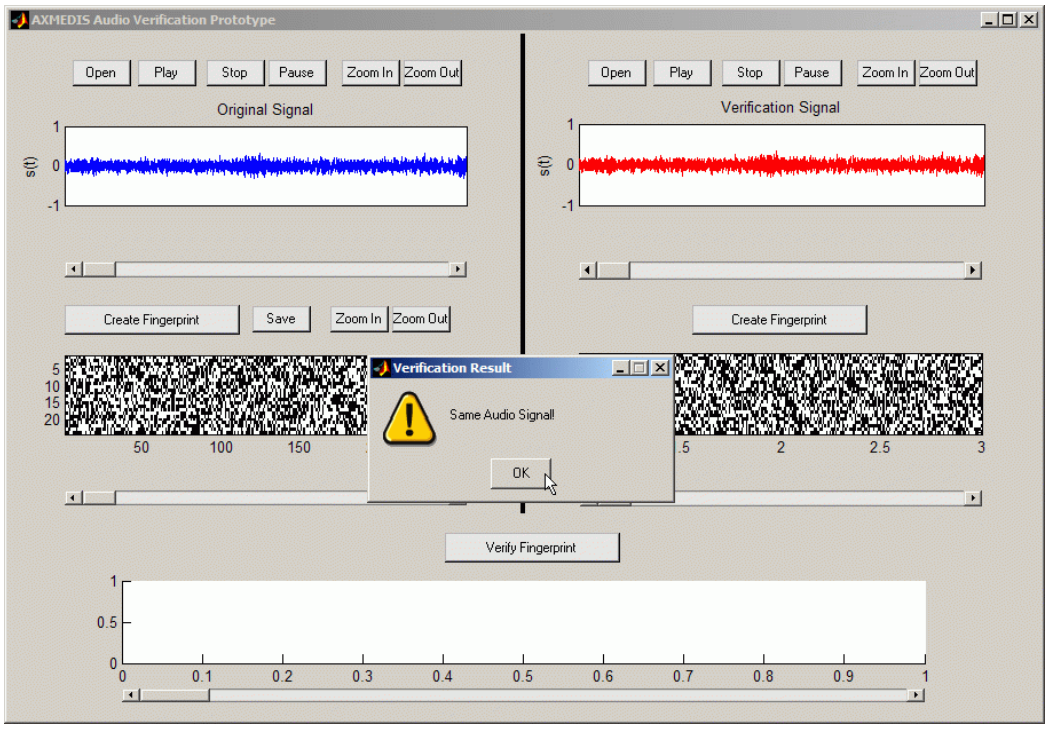
In the second step, the verification signal is loaded as shown below.



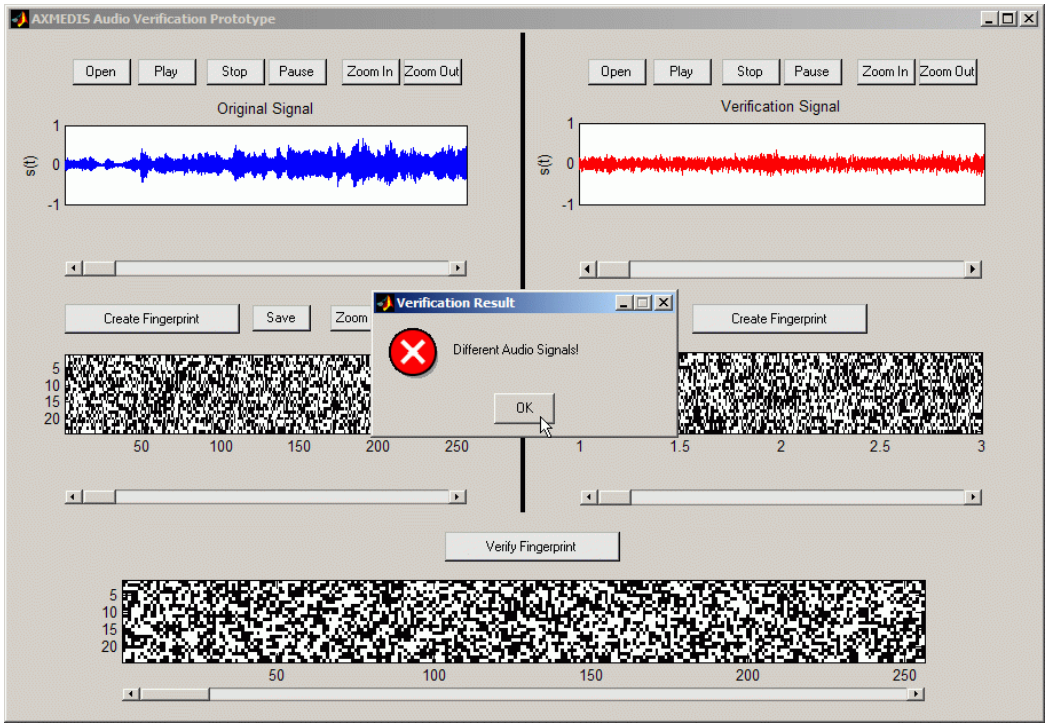
After loading the reference signal, its fingerprint is calculated.



The fingerprint of the original signal and the reference signal are compared. If the signals are similar, a corresponding message box opens:

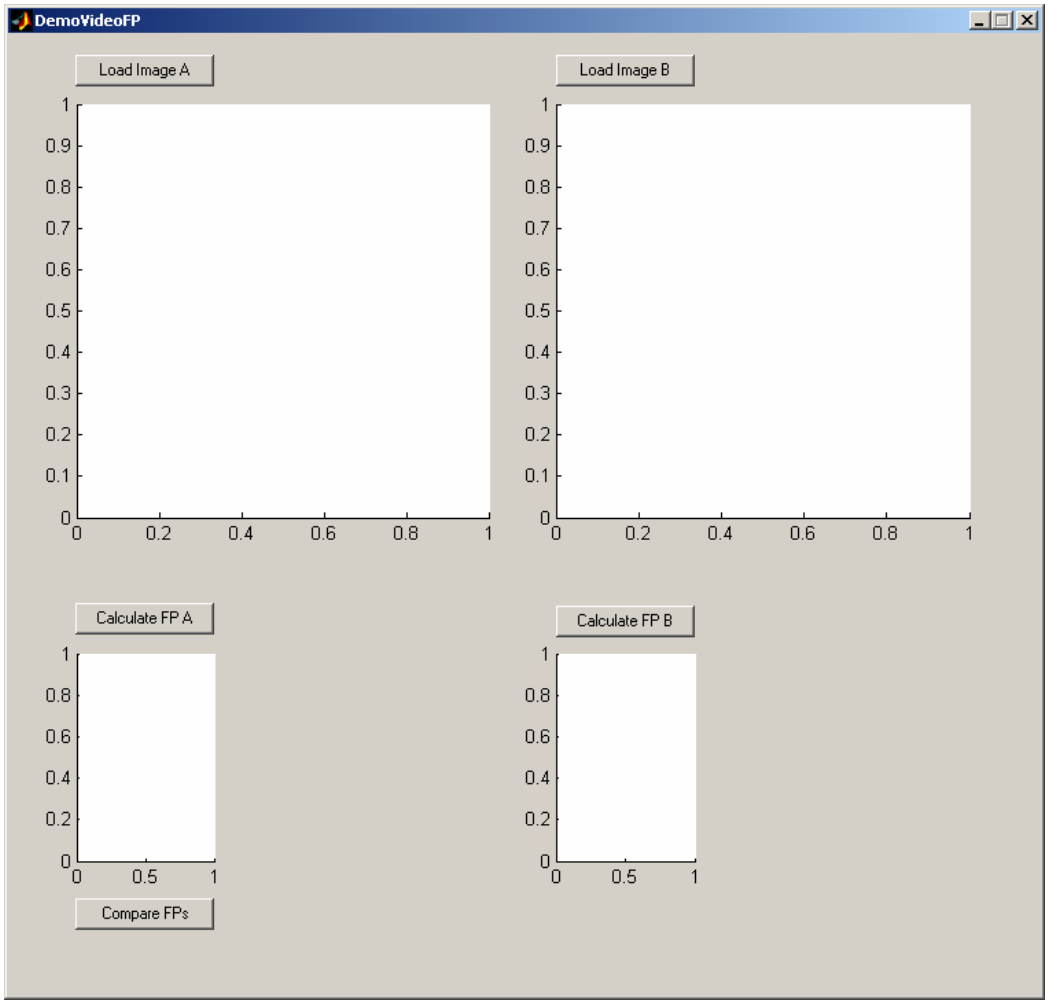


In the case of different signals, an error is shown:


AXMEDIS Audio Verification Prototype
Open
Play
Stop
Pause
Zoom In
Zoom Out
Original Signal
Verification Signal
s(t)
Create Fingerprint
Save
Zoom
Verification Result
Different Audio Signals!
OK
Verify Fingerprint

24.4.2 Image Fingerprinting Demonstration

When the application is started in MatLab, a dialog is shown.

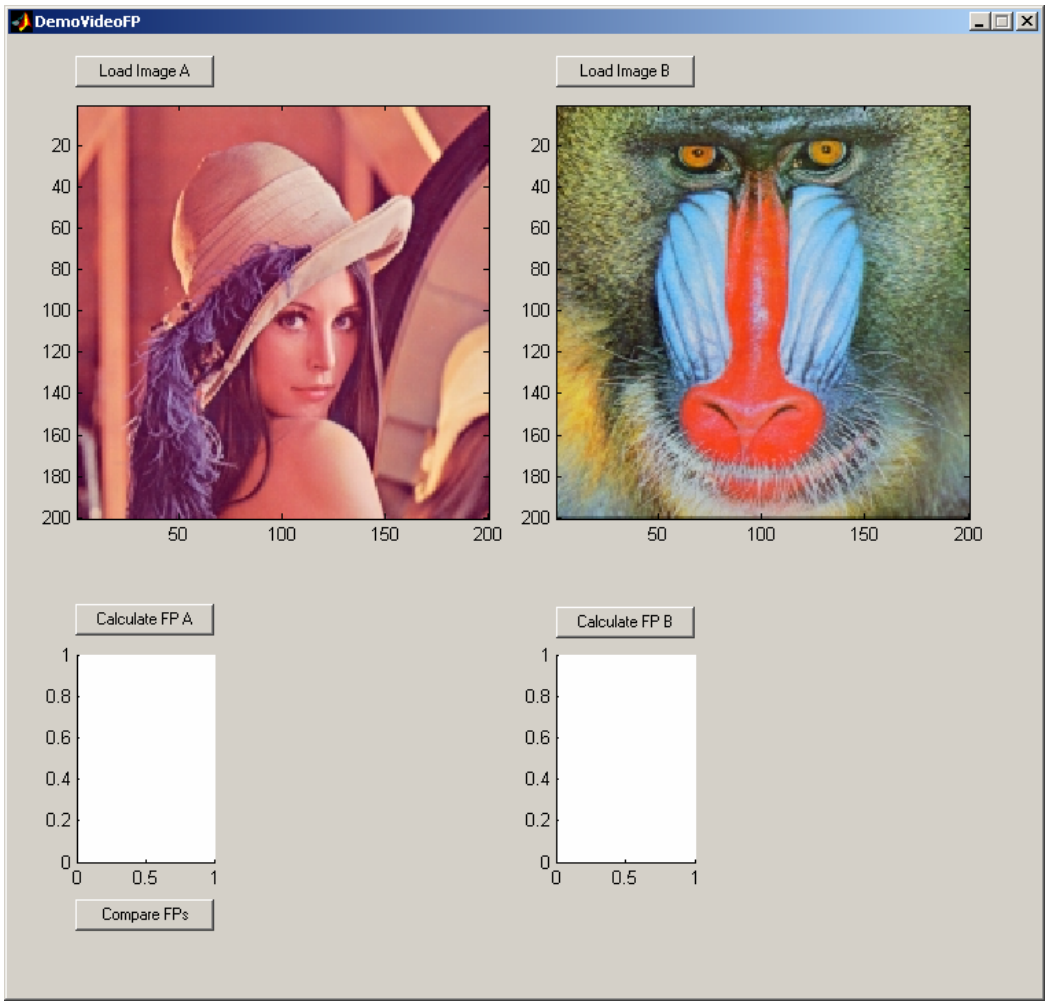


This dialog consists of four buttons, which allows to

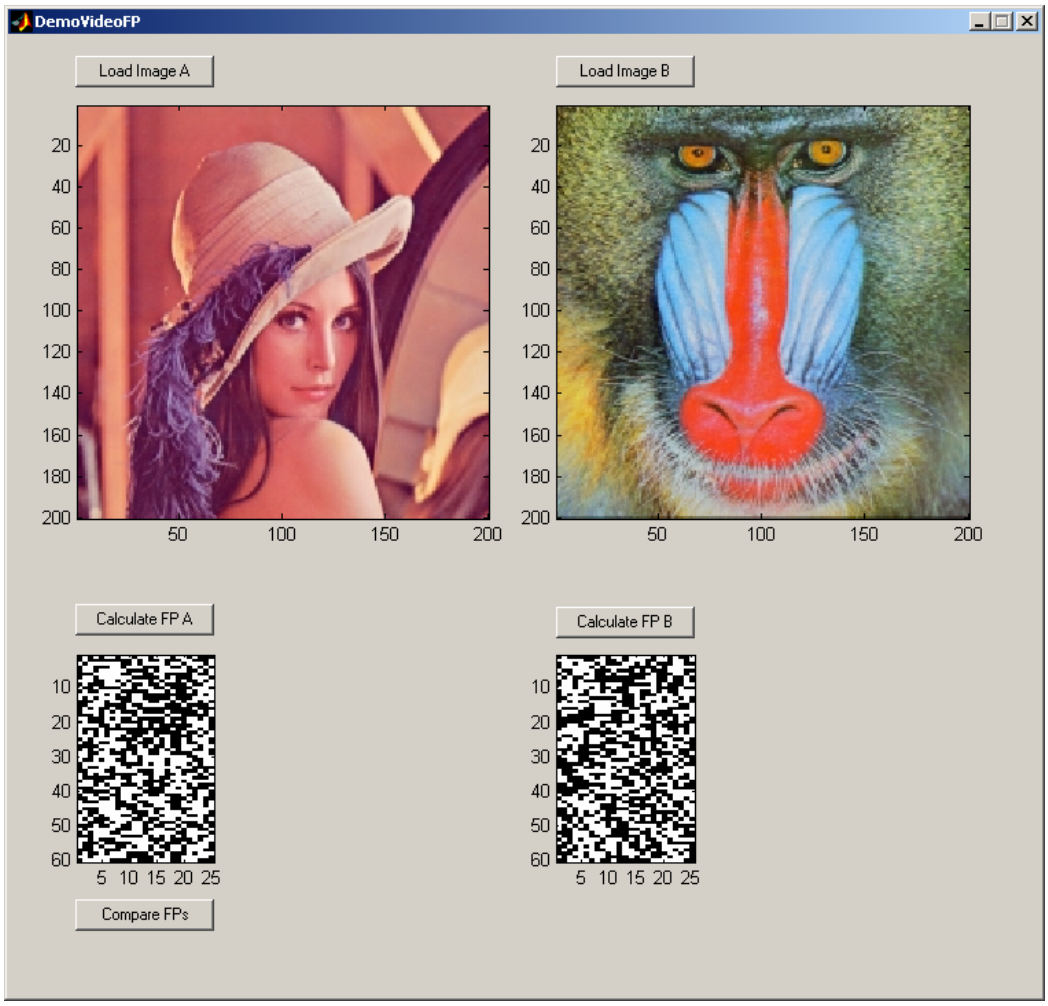
- load the reference image and the image under evaluation, to
- calculate the fingerprints for the reference image and the image under evaluation, and to
- compare the calculated fingerprints.

For the visualization of the input images and the calculated fingerprints different areas are available in the user interface.

For the demonstration, the users can load selected images:



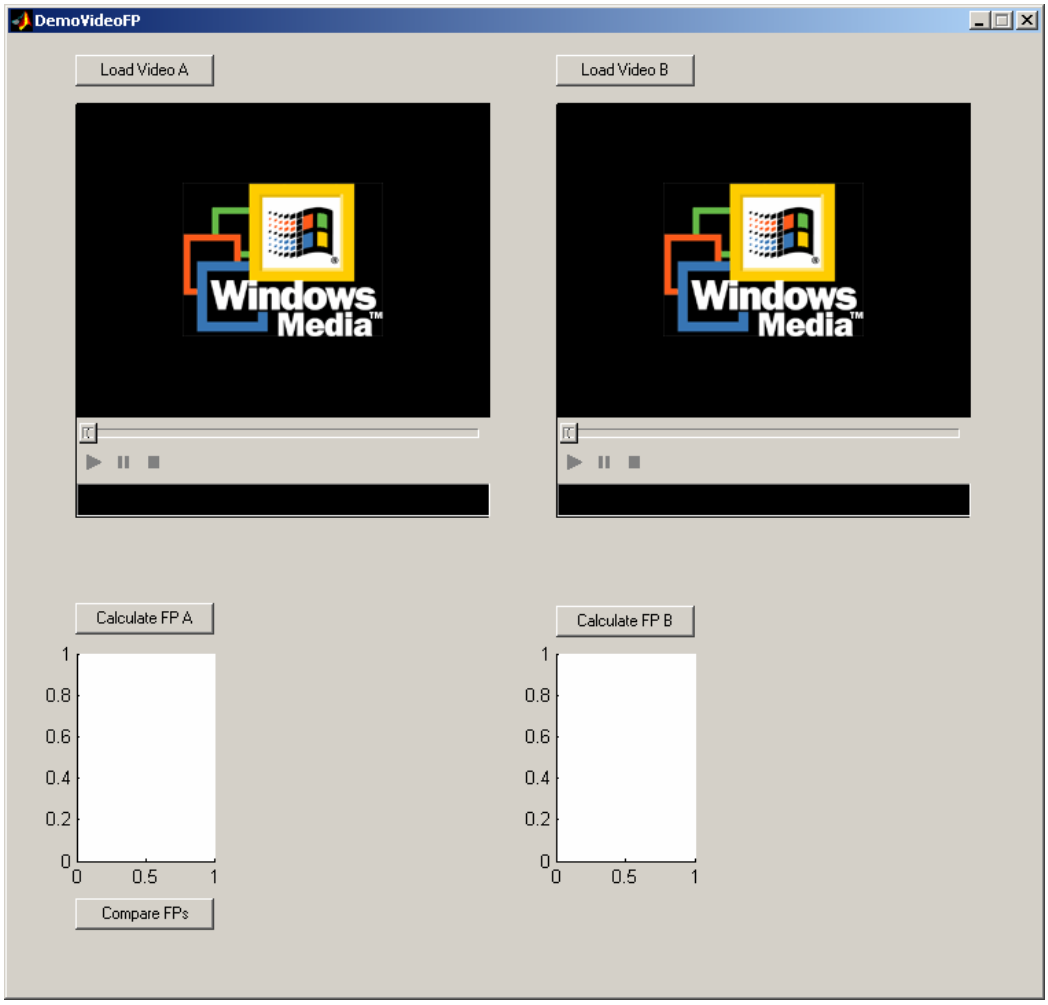
The fingerprints are calculated for the loaded images and shown visually:



After calculation of the fingerprints, the fingerprints can be compared. Dependent on the input content the fingerprints are either different (as in the above example) or similar.

24.4.3 Video Fingerprinting Demonstration

When the application is started in MatLab, a dialog is shown.

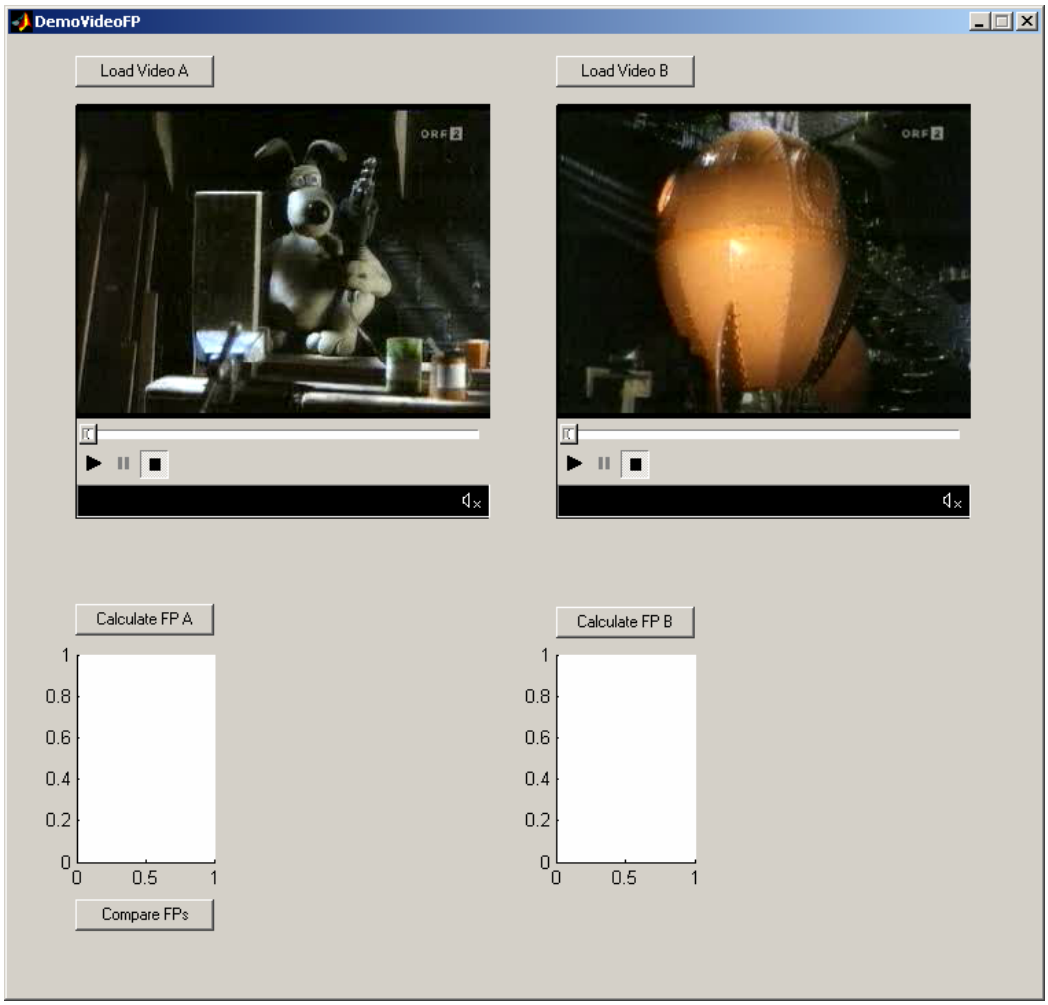


This dialog consists of four buttons, which allows to

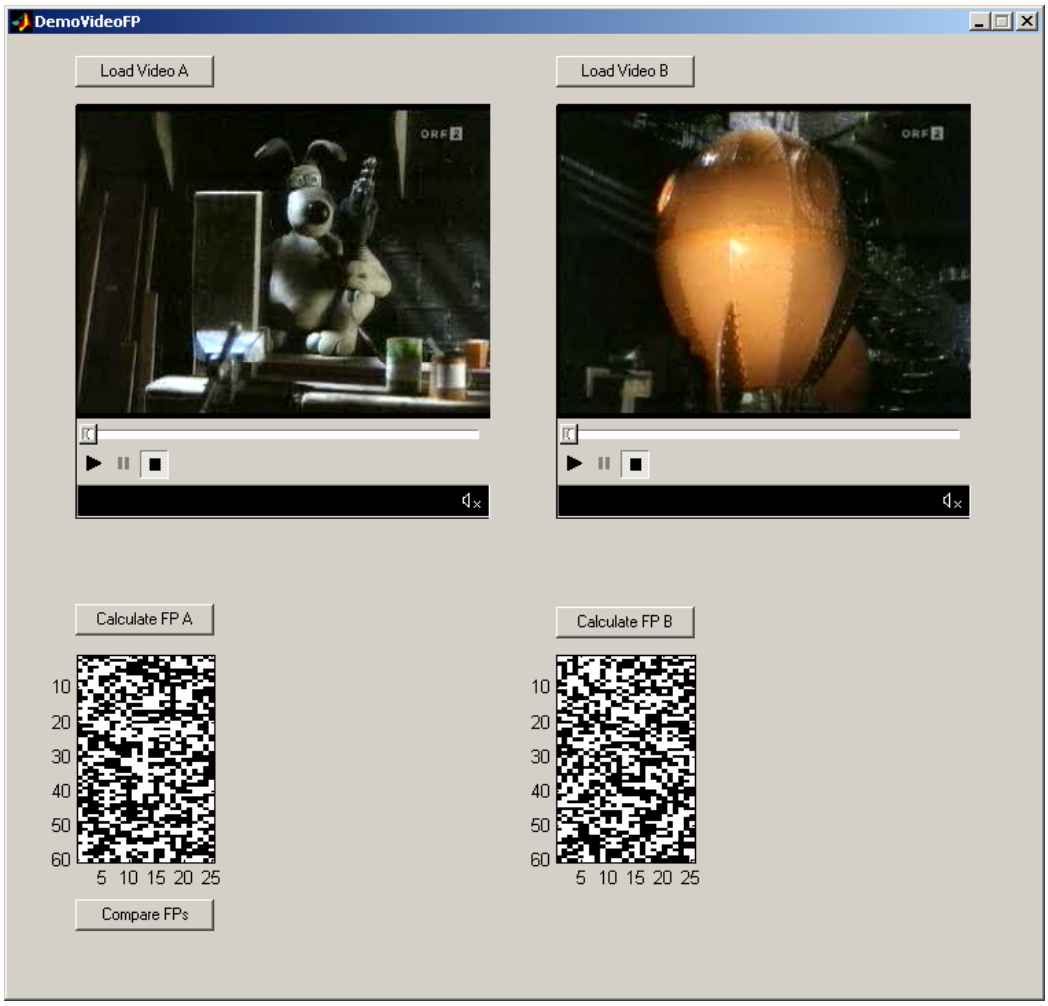
- load the reference video and the video under evaluation, to
- calculate the fingerprints for the reference video and the video under evaluation, and to
- compare the calculated fingerprints.

For the visualization of the input videos and the calculated fingerprints different areas are available in the user interface.

For the demonstration, the users can load selected videos:



The fingerprints are calculated for the loaded images and shown visually:



After calculation of the fingerprints, the fingerprints can be compared. Dependent on the input content the fingerprints are either different (as in the above example) or similar.

24.5 Technical Details

24.5.1 Audio fingerprinting

reference to the AXFW location of the demonstrator	A path in the CVS for example: https://cvs.axmedis.org/repos/Framework/source/fingerprint/audio/Matlab
List of libraries used	-
References to other major components needed	-
Problems not solved	-
Configuration and execution context	-
Programming language	MatLab

24.5.2 Image fingerprinting

reference to the AXFW location of the demonstrator	A path in the CVS for example: https://cvs.axmedis.org/repos/Framework/source/fingerprint/image/Matlab
List of libraries used	HOSA, see http://www.mathworks.com/ (only for MatLab implementation)
References to other major components needed	-
Problems not solved	-
Configuration and execution context	-
Programming language	MatLab

24.5.3 Video fingerprinting

reference to the AXFW location of the demonstrator	A path in the CVS for example: https://cvs.axmedis.org/repos/Framework/source/fingerprint/video/Matlab
List of libraries used	-
References to other major components needed	-
Problems not solved	-
Configuration and execution context	-
Programming language	MatLab

24.6 Description Content Authentication and Verification

24.6.1 Audio fingerprinting

Implemented features:

- Calculation of the fingerprint/perceptual hash
- Implementation of graphical user interface for demonstration

Missing Features that will be implemented:

- Implementation in C/C++
- Detailed evaluation and improvement

24.6.2 Image fingerprinting

Implemented features:

- Calculation of the fingerprint/perceptual hash
- Implementation of graphical user interface for demonstration

Missing Features that will be implemented:

- Implementation in C/C++
- Detailed evaluation and improvement

24.6.3 Video fingerprinting

Implemented features:

- Calculation of the fingerprint/perceptual hash
- Implementation of graphical user interface for demonstration

Missing Features that will be implemented:

- Implementation in C/C++
- Detailed evaluation and improvement

25 Bibliography

[1] MPEG 21, http://www.chiariglione.org/mpeg/standards/mpeg-21/mpeg-21.htm.
[2] ISO/IEC, ISO/IEC 2nd Edition TR 21000-2 – Vision, Technologies and Strategy.
[3] ISO/IEC, ISO/IEC 2nd Edition FCD 21000-2 – Digital Item Declaration.
[4] ISO/IEC, ISO/IEC FDIS 21000-3 – Digital Item Identification.
[5] ISO/IEC, ISO/IEC CD 21000-4 – Intellectual Property Management and Protection.
[6] ISO/IEC, ISO/IEC IS 21000-5 – Rights Expression Language.
[7] ISO/IEC, ISO/IEC IS 21000-6 – Rights Data Dictionary.
[8] ISO/IEC, ISO/IEC IS 21000-7 – Digital Item Adaptation.
[9] ISO/IEC, ISO/IEC FDIS 21000-8 – MPEG-21 Reference Software.
[10] ISO/IEC, ISO/IEC IS 21000-9 – File Format.
[11] ISO/IEC, ISO/IEC FCD 21000-10 – Digital Item Processing.
[12] ISO/IEC, ISO/IEC TR 21000-11– Evaluation Methods for Persistent Association Technologies.
[13] ISO/IEC, ISO/IEC TR 21000-12 – Test Bed for MPEG-21 Resource Delivery.
[14] ISO/IEC, ISO/IEC CD 21000-14 – Conformance Testing.
[15] ISO/IEC, ISO/IEC WD 21000-15 – Event Reporting.
[16] ISO/IEC, ISO/IEC FDIS 21000-16 – Binary Format.
[17] ISO/IEC, ISO/IEC WD 21000-17 – Fragment Identification of MPEG Resources.
[18] OMA DRM Specification, OMA-TS-DRM-DRM-V2_0-20050614-C.
[19] DRM Architecture, OMA-DRM-ARCH-V2_0_6-20040820-C. 20 August 2004.
[20] OMA DRM Rights Expression Language, OMA-Download-DRMREL-V2_0-20041210-C. 10 December 2004.
[21] Open Digital Rights Language (ODRL). http://odrl.net.
[22] "XML Encryption Syntax and Processing", W3C Candidate Recommendation 10 December 2002, URL:http://www.w3.org/TR/2002/REC-xmlenc-core-20021210/
[23] "XML Signature Syntax and Processing", W3C Recommendation 12 February 2002, URL:http://www.w3.org/TR/2002/REC-xmldsig-core-20020212/
[24] Microsoft DRM, http://www.microsoft.com/windows/windowsmedia/drm/default.aspx
[25] TV-Anytime, http://www.tv-anytime.org/
[26] TV-Anytime Rights Management and Protection Information for Broadcast Applications (Normative), ETSI TS 102 822-5 V1.1.1. November 2004.
[27] Binding of Rights Management and Protection Information, ETSI TS 102 822-5-2 V1.1.1. June 2005.
[28] Internet Streaming Media Alliance (ISMA), http://www.isma.tv/
[29] Digital Media Project (DMP), http://www.dmpf.org/
[30] Interoperable Digital Rights Management Platform, D440, 15 April 2005.
[31] IETF RFC 1737, K. Sollins and L. Masinter, Functional Requirements for Uniform Resource Names, December 1994.
[32]Music Industry Integrated Identifier (MI3P) Project, http://www.mi3p-standard.org/
[33] MI3P-DICT-10-FDS, The MI3P Data Dictionary Standard - Final Draft Standard. March 2005.
[34] MI3P-ELMS-10-FDS, European Licensing Message Suite - Final Draft Standard. March 2005.
[35] MI3P-DSRM-10-FDS, Digital Sales Reporting Message Suite - Final Draft Standard. March 2005.
[36] MI3P-ERNM-10-FDS, Electronic Release Notification Message Suite - Final Draft Standard. March 2005.
[37] MI3P-GRid-10-FDS, The Global Release Identifier Standard (GRid) - Final Draft Standard. March 2005.
[38] MI3P-MWLI-10-FDS, The Musical Work Licence Identifier (MWLI) - Final Draft Standard. March 2005.
[39] Creative Commons, http://www.creativecommons.org/
[40] Real Networks, http://www.realnetworks.com/
[41] Helix DRM, http://www.realnetworks.com/products/drm/index.html

[42] Real Networks Media Commerce Suite,
http://www.realnetworks.com/products/commerce/description.html
[43] Trymedia ActiveMark DRM, http://www.trymedia.com/services/security_drm.shtml
[44] Light Weight Digital Rights Management (LWDRM), http://www.lwdrm.com/eng/
[45] Fraunhofer-Institute for Integrated Circuits IIS, http://www.iis.fraunhofer.de/
[46] Fraunhofer-Institute for Digital Media Technology IDMT, http://www.emt.iis.fraunhofer.de/
[47] Fraunhofer-Institute for Secure Telecooperation SIT, http://www.sit.fraunhofer.de/cms/de/index.php
[48] SafeNet, http://www.safenet-inc.com/
[49] DMDsecure, http://www.dmdsecure.com/
[50] Windows Media Product Vendors,
http://www.microsoft.com/windows/windowsmedia/service_provider/Software/default.aspx
[51] ContentGuard, http://www.contentguard.com/
[52] Sun Microsystems, Inc., http://www.sun.com/
[53] TANDBERG Television, http://www.tandbergtv.com/
[54] SeaChange International, http://www.schange.com/
[56] IDRM, http://www.idrm.org/
[57] Open eBook Forum, http://www.openebook.org/
[58] Rights and Rules Working Group, http://www.openebook.org/oebf_groups/rrwg.htm
[59] PRISM, http://www.prismstandard.org/
[60] PRISM specification, http://www.prismstandard.org/specifications/
[61] OASIS, http://www.oasis-open.org/home/index.php
[62] ebXML, http://www.ebxml.org/
[63] cXML, http://www.cxml.org/
[64] XrML, http://www.xrml.org/
[65] DPRL, http://www.oasis-open.org/cover/DPRLmanual-XML2.html
[66] ODRL, http://odrl.net/
[67] Wikipedia. Cryptographic Hash Function. http://en.wikipedia.org/wiki/Cryptographic hash function, June 2005.
[68] ECRYPT, Network of Excellence. Recent collision attacks on hash functions: Ecrypt position paper. Technical report, ECRYPT, Nov 2004.
[69] Bruce Schneier. *Applied Cryptography: Protocols, Algorithms, and Source Code in C*. John Wiley & Sons, second edition, 1996.
[70] Bart Preneel. Cryptographic primitives for information authentication - state of the art. In *State of the Art in Applied Cryptography*, 1997.
[71] RFC-Editor. The request for comments (rfcs), 2005. http://www.rfc-editor.org/.
[72] P. Cano, E. Batlle, T. Kalker, and J. Haitsma. A review of algorithms for audio fingerprinting. In IEEE Workshop on Multimedia Signal Processing, pages 169–173, 2002.
[73] I. J. Cox and J. Paul M. G. Linnartz. Public watermarks and resistance to tampering, Aug. 30 2001.
[74] M. Schneider and S. F. Chang. A robust content based digital signature for image authentication. In *IEEE International Conference on Image Processing (ICIP'96)*, 1996.

26 Glossary

DRM Digital Rights Management

Appendix A. Contracts Scheme

B2B and B2C Contracts analysis

This section is dedicated to the analysis of the contracts actually in use for the exploitation of music, video, images and text. It is divided in two part: one dedicated to the analysis of the main contractual clauses and the second one in which contracts are studied and compared on the basis of the different media devices used to provide content to the final consumer.

PART A)
This section of the analysis is aimed at verifying the contractual practices actually in use concerning both the B2B and the B2C context with respect to the following contractual clauses :

a) The Parties.
b) Definitions.
c) Rights granted.
d) Territory.
e) Exclusivity.
f) Duration.
g) Remuneration method.
h) Licensee's Undertakings
i) Warranties Indemnities
l) Termination
m) Jurisdiction

In particular this analysis has had as its objects the following contracts identified by the role of the parties:

1) Music Content owner /distributor.
2) Music Content owner / on line music retailer
3) Audio and video Content provider/ service provider
4) Video content owner / distributor.
5) Music content owner / ring back tone distributor
6) Video content provider / Satellite Broadcasting provider
7) Video content broadcaster / web site.
8) Video content owner / Satellite Broadcasting provider.
9) Video content owner / licensee. .
10) Video content distributor /licensee.).
11) Audio video content distributor / aggregator/distributor/consumer.
    a) Conditions for use.
    b) General licence conditions.
12) Educational content owner / Distribution.
13) Images/text and other content owner / web site of cultural content
14) On line music retailer: Terms of service. – B2C
15) Video content provider: condition of contract. - B2C
16) Text content provider: Internet Service Agreement
17) Digital archive of images content provider: statement of the user.
18) Digital archive of images content provider: licence agreement for the digitisation and archiving of primary sources
19) Digital archive of images content provider: Licence agreement for inclusion of copyright digital images on website.
20) Literary content and photos from a web site.

a) The parties

Parties of the contract	
Licensor	**Licensee/ distributor/ consumer**
1) Music content owner	Distributor, which provides the contents to *"digital shops",* phone operator, and/or providers.
2) Music content owner	*"Online music store otherwise known as a digital music download service".*
3) Audio video content owner	Company offering to customers a service *"which allow them to purchase from us authorised music and audio-visual digital files".*
4) Video content owner	Distributor
5) Music content owner	Distributor of ring backs tone services.
6) Video content owner, provider and distributor.	Satellite Broadcasting company operating networks for exhibition of audiovisual material over all forms of cable or satellite television, including basic cable television, pay and subscription television, pay-per-view and satellite transmission. Moreover it distributes contents via internet or "worldwide web" for access by television or personal computers.
7) Video content broadcaster	Owner of a web site that *"features movie, music and television related news, data and merchandise offers and related Content and merchandise offers".*
8) Video content owner	Satellite Broadcasting company is a company performing, displaying and broadcasting video contents.
9) Video content owner	Licensee: scheme of license contract used to grant the right to broadcast programs whose rights are owned by the licensor.
10) Video content distributor	Licensee scheme of contract to grant the right to transmit excerpts of video programs.
11) Audio video content distributor c) Conditions for use d) General licence conditions	Licensee: aggregator/distributor/consumer
12) Educational content provider	Distributor
13) Images/text and other content owner	Web site, which is supposed to provide to consumers cultural contents.
14) On line music retailer	B2B providing music contents to consumers.
15) Video content provider	B2C contract
16) Text content provider	Company allowing to registered subscribers to use the information provided on its web site
17) Digital archive of images content provider	
18) Please see number 17 above.	
19) Please see number 17 above.	

20) Literary and photo content owner	This web site contains articles, editorials, opinions, text, directories, photographs, illustrations, comics, advertising copy, trademarks and service marks.

b) Definitions

The attention has been focused on all the definitions having an impact on the discipline displayed by the contracts, as far as the scope is concerned.

Relevant definitions	**Comments**
1) - *"Download"*: the reproduction of records by mean of the downloading on the hard disc of a PC or on a different device such as a telephone of the user. - *"Encoding"*: the activity, which allows the files' digitalisation. - *"Third party ayant cause"*: digital shops and telephone operators and/or providers	All the three definitions contribute to limiting the object of the contract under different points of view. The first definition (*"download"*) concerns the technical mean, which allows the transfer of the content. The second definition ("encoding") limits the possibility to elaborate the content granted. The third one involves the relationship between the distributor and the third parties, which get in their turn the grant of rights from it.
2) No specific text about definitions.	
3) No specific text about definitions.	
4) Article 1) of this contracts terms foresees that any definition is specified in the attached "Schedule of Definitions". In this part of the document there are the following sections: a) Cinematic Rights Definitions; b) PayPerView Rights Definitions; c) Ancillary Rights Definitions; d) Video Rights Definitions; e) Pay TV Rights Definitions; f) Free TV Right Definitions; g) Video Use Definitions; h) Other Rights Definitions; i) Additional Definitions.	On one hand the definitions concern technological aspects of the transmission of the content. This applies to letters a), b), c), d), e), f). On the other hand letters h) and i) refer to the characteristics of the licence and to the relationship between the parties and have a significant impact on the above mentioned issues. For instance we draw the attention on the definition of First Negotiation which is the following: *"First negotiation means that, provided that Distributor is then actively engaged in the distribution business on a financially secure basis, Licensor will negotiate with Distributor in good faith for a period of ten (10) days regarding the matter for which Distributor has a first Negotiation right before entering into negotiations regarding the matter with any other Person. If no agreement is reached within this time period, then Licensor will be free to stop negotiations with Distributor and then to negotiate and conclude agreement regarding the proposed matter with any other Person on any terms".*
5) No specific text about definitions.	
6) No specific text about definitions in the body of the agreement but there is a reference to an Addendum not included	
7) Art. 1 foresees the definitions of "Affiliate",	The most interesting aspects are the following.

"Annual ceiling", "Arbitration proceeding", "Capital Stock", "License Guidelines", "Web site Competitor", "Web Content", "Web Content Pages", "Ceiling Amount", "Co-branded Site", "Collaboration Agreement", "Content", "Contract Year", "Hollywood Content", "Hollywood Site", "Intellectual Site", "Intellectual Property Rights", "Internet", "Internet site" or "Web site", "Market value", "Mirror site", "Person", "Television content" and "Term".	"Arbitration proceeding" rules all the proceeding to which a reference is made in article 7. "license Guidelines": these guidelines limit in a the use of the granted right.
8) Article 1. The definitions provided are the following: "Cable systems", "content", "Documentation", "download", "dub", "Exhibit", "Internet", "Person", "Private Dwellings", "Satellite Systems", "Stand Alone Systems", "Still images", "Term", "Title", "Territory", "Version" and "Video on demand".	The definitions apply to both technical and not technical aspects of the agreement. Some definitions deserve a deeper attention. Firstly the quite wide concept of "documentation" is linked to the fact that the licensed contents are videos for adults and this activity is allowed just if some requirements are fulfilled. Another interesting definition is the "territory" the territorial coverage of the contract is clearly enounced.
9) The text of the definitions is included in Addendum A and includes the following items: "television", "free television", "terrestrial free television", "cable free television", "satellite free television", "pay television", "terrestrial pay television", "cable pay television", "satellite pay television", "home video", "home video rental", home video sell-through", "commercial video", "pay per view", "non residential pay per view", "residential pay per view", "video-on-demand", "ancillary", "Airline", "Ship", "Hotel".	
10) The "archive" is the whole video content from which excerpt is requested by licensee No other specific definitions.	
11) No specific text about definitions.	
12) "Title 1", which seems to be a kind of second part of the recitals section, foresee the definition of the following items: "Ressources" (resources), "Utilisateur" (user), "Etablissement" (entity), "Etablissement client" (entity which is a customer), "Plate form " (distributor platform), "Recettes brutes hors taxes" (gross turnover), "Abonnement" (subscription).	The most important definition is the definition of the distributor's platform. This platform is exploited by the distributor on a contractual basis and so it can suffer form modifications due to some changes in the management of the platform and, as a consequence, in the way the rights granted are exploited.
13) Art. 1 Definitions. This article concerns "the images", "the works", "the database", " the website", "the Tariff".	The most important definition concerns "the Tariff" which implies some consequences on the calculation of the fee. "The Tariff means the current general tariff of reproduction and user's rights for works of visual arts, as published in the "Tarif general des droits de reproduction et d'utilisation pour les oeuvres des arts visuals", by SOFAM [*]
14) No specific text about definitions.	

15) Several definitions are foreseen in the contract, some of them concern the video content providers and their identity.	In the framework of this section the role of other subjects, which are not the parties of the contract, is clarified, and defined as a video content provider role.
16) No specific text about definitions.	
17) No specific text about definitions	
18) No specific text about definitions	
19) No specific text about definitions	
20) No specific text about definitions	

* SOFAM is the Belgian authors' collecting society of visual arts.

c) Rights granted

It's the object of the license and so it is a part, which needs to be focused in the most effective way. Therefore the text of the contract has been quoted.

Rights granted	**Comments**
1) The licence has the following objects: - the right to allow the users to download against payment recordings and video clips through web sites and portals of telephone operators; - the right to sell to the users "true tones" for mobile phones; - the right to allow the users to download photos and images to be used as "wallpapers" in the mobiles; - the right to use the name of the artists to provide the above mentioned service; - the right to allow the use of the "Artwork" while the downloading of the recordings; - the right to adapt the recordings and the videoclips to get the opportune editing for the best use in a wireless environment.	License objects: licensee has the right to allow consumers to download music and video files, true tones and wall papers through web portals and through mobile.
2) The license has the following objects: - the right to resell music files through a digital music download service; - the right to convert the catalogue to the required format for digital downloads.	The licence has as its object the sale of digital files and it includes the digitalisation of content before making them available on the web.
3) The licence has the following objects: - the right of the distributor to sell to his customers music files by mean of downloading or streaming; - the right to display on their service any cover artwork associated with the recordings and any promotional materials associated with the artist.	The object of the licence is just the right to distribute music files. One of the obligations of the content owner is making available a format of the content duly digitalised.
4) Being this contract an off line contract, the licence has as its rights the following objects: - Home rental; - Home sell; - Commercial use.	There is no particular comment. Despite of the fact that this is an off line contract, its structure seems to be compatible also with a digital environment.
5) The licence has the following objects: - *" the right to reproduce the recordings onto Licensee's computer server for its internal business purposes and for subsequent distribution to approved sub-licensees"*	License grant the reproduction rights of music content for the purpose of their distribution as ring back tones

for use in their respective ring back tone services offered to their respective subscribers to personalise the connecting tone to be heard by the calling parties over a regional wireless transmission network; - to reproduce the recordings for subscribers to pre-listen the ring back tone over the Internet provided the Recordings shall not exceed fifteen seconds and the Recordings are protected from permanent download and further copying.	
6) The right granted are the following*:* *- The right to distribute and publish the Pictures using all forms of satellite, cable or Internet transmission to television sets, computer monitors or other devices intended to receive and exhibit audio visual images, whether now known or hereafter discovered.* *- The rights to distribute and publish the Pictures via a "narrow band" Internet service and all forms of Interact transmission whether now known or hereafter discovered.* *The Television, Pay-Per-View and Internet Rights granted hereunder include the rights to exhibit, broadcast, display and radio simulcast, all or any portions of the Picture(s);* *- The right to make such edits, changes, alterations and modifications in the Pictures, including changing the title of any Picture, as Satellite Broadcasting company determines in its sole discretion, is appropriate or necessary for time restrictions, to comply with any applicable censorship requirements, to create new versions to accommodate Satellite Broadcasting marketing plans or to take advantage of new opportunities to market and exploit new and different versions of adult motion pictures in and throughout the Territory in the media licensed hereunder;* *- The rights granted shall include the right to create, at its sole cost and expense, new and different versions of the Pictures for exhibition via satellite, cable or the Internet, as contemplated above.* *- The right to translate and dub the title and soundtrack of any and all versions of the Pictures in any languages, and to distribute such dubbed versions throughout the Territory.* *- The right to copy, in any form or medium which Satellite Broadcasting determines appropriate, the Pictures and to distribute such copies in the normal course of its satellite, cable or Interact business.*	The description of the rights granted is very complete and does not seem to request further comments.
7) The rights granted are the following*:* (i) the right to use, copy, publicly display, publicly perform, distribute, or otherwise make the Video provider's content available on the Web Site during the term, and *(ii) Archive the Provider's Content after expiration of the Term, to the extent provider has the right to so license such Content to the Web Site*	The rights listed should be read in coordination with the Video Content Provider Guidelines, which limit and define further the relationship between the parties.

8) Licensor grants to Licensee: *(a) The exclusive right and license, to exhibit in the licensed territory, the Title and/or any excerpts there from or Versions thereof by means of Satellite Systems and Cable Systems via VOD and the Internet delivered by Satellite Systems and Cable Systems;* *(b) The non-exclusive right and license, also outside the Licensed territory, but within the Territory's possessions, to Exhibit the Title and/or any excerpts therefrom or Versions thereof by means of Satellite Systems and Cable Systems via VOD and the Internet delivered by Satellite Systems and Cable Systems;* *(c) The non-exclusive right and license throughout the Territory to Exhibit Titles and/or any excerpts therefrom or Versions thereof by all means now known or later discovered via Stand Alone Systems and the Internet, with the understanding that for purposes of the Internet, the Territory shall be deemed to be the entire universe, subject in the case of Internet rights to the provisions of Section 2 (below);* *(d) The non-exclusive right and license to duplicate each Title and to distribute such Title, to and only to the extent necessary or desirable to effectuate the Exhibition and exploitation of that Title in accordance with the terms hereof;* *(e) The non-exclusive right to advertise, promote and publicise Licensee's Exhibition of the Titles and all matters relating thereto in all media and/or medium now known or hereafter devised, to use Still Images and/or excerpts from the Titles in connection with such advertising, promotion, and publicity and to market, advertise, promote and publicise Licensee's exhibition of Titles and Still Images;*	No particular comments seem to be necessary.
9) The rights granted are the following: *"Licensor grants Licensee the exclusive rights ("Rights") indicated in Item 2 of Addendum A relating to the Program(s) and the territory ("Territory") indicated in Item 3 of Addendum A."*	This contract clarifies the content of the rights granted making reference to an attached document (Addendum A). In this case the latter is a scheme, which does not allow any further comment.
10) The sentence of the contract referring to the rights granted is the following: *Distributor grants to User, with respect toArchive, the Rights in the Territory, both as specified in point above.*	In this case User/licensee is granted with the right to use the requested excerpt of the Archive following terms and conditions set forth in this contract
11) The right granted are the following: *"6. The Licensee shall be entitled to fully or partially incorporate the Licensed Material in any audiovisual works*	In this context it is interesting to remark that rights granted include the possibility to incorporate the *"licensed material"* in a work

created, produced or co-produced by the Licensee ("the End Product"). *7. The Licensee shall be entitled to distribute the End Product, containing the Licensed Material, only for the use, medium, period of time, territory, the number of broadcasts and any other restrictions specified by the Licensee in the accepted purchase order form.* *8. The Licensee shall not undertake any expanded use of the Licensed Material without the prior written approval of the Licensor. Nor shall the Licensee be allowed to transfer or sublicense all or part of its rights to any third party, whoever this party is and regardless of the nature and importance of the transfer/sublicense.* *9. The Licensor does not grant any rights and does not make any warranties with regard to the use of names, trademarks, designs, works of art or architecture depicted in any Licensed Material and the Licensee must make sure that all the necessary rights or consents regarding any of the above, as may be required for reproduction, have been obtained."*	created, produced or co-produced by the licensee. No unauthorised expansion of the licensed material is allowed.
12) *Par le présent contrat, l'Editeur confie à titre exclusif à XXX Distribution, qui l'accepte, la distribution de ses Ressources au sein du catalogue XXX Distribution auprès des Etablissements en vue de permettre leur consultation par les Utilisateurs via la plate-forme XXX Distribution assurant l'accès aux Ressources hébergées par l'Editeur sur son serveur. "* Translation: *"By mean of this contract, the Content Owner grants to the distribution Company, which accepts, the exclusive right to distribute the contents of the Content owner's catalogue among the entities in order to allow the users to consult them via the Distributor platform assuring the access to the contents hosted by the publisher in its server"*	The right granted is a distribution right. It should be paid attention to the fact that the translation of the French word "établissement" should be understood as a venue where the content is displayed or performed. The translation in English as "entity" is aimed to give the idea of how wide is this concept.
13) The rights granted are the following: *"**3.1** Subject to the terms of this Agreement, the Licensor grants to licensee a non-exclusive, worldwide licence to market and sub-license the Works and the Images to publishers and other end-users.* ***3.2** Unless otherwise agreed by the parties, licensee's licence to grant sub-licences is subject, on a case-by-case basis, to the prior written approval of the Licensor of the identity of the end-user and the terms of the sub-licence.* ***3.3** Unless otherwise agreed by the parties, licensee will grant the approved licences using the standard licensing contract as set out in the Appendix to this Agreement. In any case, sub-licences may never be granted for a period of more than three years and must always be personal to the end-user.* ***3.4** Licensee will use its reasonable endeavours to find end-users*	The rights granted to the licensee are the right to market and sublicense the content owned by the licensor. Any sublicense is nevertheless strictly conditioned to the prior approval of the licensor and to the use of a standard licensing contract drafted by the licensor himself.

for the Works and the Images, in order to maximise the financial return from its sub-licensing of the Works and the Images for both parties. ***3.5*** *Subject as provided in this Agreement, all intellectual property rights and rights in the nature of intellectual property rights in the Works, the Images and the objects depicted in the Works and the Images, are reserved to the Licensor and any relevant rights owners.* ***3.6*** *The Images, the Works, the carriers by which they were delivered to licensee and any other materials delivered to licensee for the purposes of the sub-licences remain the Licensor's property and will be returned to the Licensor as soon as possible and in any event upon termination or expiry of the relevant sub-licence.*	
14) Hereunder the text concerning the granted rights: *"You shall be authorised to use the Products only for personal, non commercial use.* *You shall be authorised to use the Products on five Apple-authorised devices at any time.* *You shall be entitled to export, burn or copy Products solely for personal, non-commercial use.* *You shall be authorised to burn a play list up to seven times.* *You shall be able to store Products from up to five different Accounts on certain devices, such as an XXX and XXX mini, at a time.* *Any burning or exporting capabilities are solely an accommodation to you and shall not constitute a grant or waiver (or other limitation or implication) of any rights of the copyright owners in any content, sound recording, underlying musical composition, or artwork embodied in any Product* *You agree that you will not attempt to, or encourage or assist any other person to, circumvent or modify any security technology or software that is part of the Service or used to administer the Usage Rules.* *The delivery of Products does not transfer to you any commercial or promotional use rights in the Products."*	This contract concerns a B2C relationship. Therefore the main aspect that gets ruled is the use of the content which is downloaded from the on line music store. The use must be a personal one and in no case a commercial one.
15) The rights granted are specified in a separate contract offer. They can vary in a wide range going from the transmission of video contents to more integrated services.	No comment seems to be necessary.
16) The subscriber has the right to use the information provided by the web site and to interact with it.	No comment seems to be necessary.
17) The user has the right to use any part of the Data Collection	Any duplication, reproduction or

and website only for the purposes of non-commercial research or teaching.	sale of all or part of any of the Data collections in any form is expressly forbidden.
18) The right owner grants to the licensee the right to store images in the Digital Archive	No comment seems to be necessary.
19) The owner grants to the licensee the licence to place images on the website.	No comment seems to be necessary.
20) The content owner grants the right to use contents contained on this web site.	The use of the contents is restricted to the respect of the intellectual property rights of the licensor. Therefore no derivative work is allowed.

d) Territory

The limitation of the Territory where the license displays its effects is very important as far as the on line environment is concerned.

In particular there are several different options, which can be examined.

Territory	Comments
1) Italy, Vatican City, Republic of San Marino.	Despite of the fact that a transmission via internet is foreseen, no particular limitation is included in the contract as far as this aspect is concerned.
2) The Universe	This contract disciplines the licences granted to an on line store. In this case the territory is not limited at all and the license applies to the entire universe.
3) The contract foresees two different options: - one or more specific countries; - the world and the universe.	Under a technological point of view it should be taken into consideration the fact that the licensee points out that the use of P2P protocols is foreseen. This could influence the possibility to verify that the territory where the service gets provided is really the one, which is defined in the contract.
4) Italy	The contract has as its object an off line service.
5) The People's Republic of China (excluding the Hong Kong Special Administrative Region, the Macau Special Administrative Region and the Taiwan Province)	No further comment seems to be necessary.
6) *"The territory in which Licensor may exercise each and all of the rights granted herein shall be the territory of North, Central and South America ("Territory"), except that due to the nature of the Internet, the Internet Rights granted herein are worldwide in scope. Distributor's rights may be exercised in any country in and throughout the Territory, including their respective territories and possessions."*	It is interesting noting that the territory is clearly limited with the exception of the use on the internet, whose "nature" is taken into consideration. The concept of the "nature of the Internet" is very vague.
7) No specific discipline about this issue.	The contract foresees that the contents owned are displayed on the web site of the licensee without any further territorial limitation.
8) In the part of the contract dedicated to the	Here is another case where the contract makes a

"definitions" there is a specific discipline for the territory which is the following: *"As to each Title, "Territory" means all countries in North America, Central America and South America including the respective territories, possessions, and commonwealths of all such countries, except with respect to the exercise of the Rights in connection with the Internet, in which case "Territory" shall refer to the entire universe."*	distinction between the exercise of a right in connection with the internet and the exercise of the same right in other forms. The first option implies the definition of the territory as the entire universe.
9) The scheme of the contract foresees the indication of the territory in an Addendum.	No further comment seems to be necessary.
10) The scheme of the contract foresees the indication of the Territory.	No further comment seems to be necessary.
11) The territory issue is not disciplined in the examined "General licence conditions" but in the purchase order form.	No further comment seems to be necessary.
12) The possibility to limit the territory where the contract applies is foreseen by article 2 which in its turn at Annexe 2.	No further comment seems to be necessary.
13) The right granted by the contract is making available the contents in a web site and no territorial issue is taken into consideration.	No further comment seems to be necessary.
14) Document named *"Terms of sale"* (on the web site) the following rule is imposed to all the customers: *"Purchases from the Web Store are available only in the XXX territory and are not available in any other location. You agree not to use or attempt to use the service from outside of the available territory. Apple may use technologies to verify such compliance."*	A strict limitation is imposed to customers downloading music files. No more details are foreseen about the technologies, which could be used to verify their compliance with this rule.
15) Nothing about the territory is foreseen in the contract.	No comment seems to be necessary.
16) Nothing about the territory is foreseen in the contract.	No comment seems to be necessary.
17) Nothing about the territory is foreseen in the contract.	No comment seems to be necessary.
18) Nothing about the territory is foreseen in the contract.	No comment seems to be necessary.
19) Nothing about the territory is foreseen in the contract.	No comment seems to be necessary.
20) Nothing about the territory is foreseen in the contract	

e) Exclusivity

Exclusivity clause	**Comments**
1) The exclusivity right is granted in relation to the territory.	No comment seems to be necessary.
2) The right of *"exclusive access to current and future song(s) and album release for digital sale only"*.	The exclusivity is granted in relation to the mean used to sell the music files (internet).
3) The license is a non-exclusive one.	No comment seems to be necessary.

4) The licence grants the rights on an exclusive basis.	No comment seems to be necessary.
5) The exclusivity is granted in relation to the territory and to the term.	No comment seems to be necessary.
6) The licence grants several rights on an exclusive basis and other rights on a non-exclusive one. In particular the exclusivity on all the new contents released by the licensor is shared between the licensor himself and the licensee for the first 90 days after the release. Also the rights on specific kind of contents are granted on a non-exclusive basis.	No comment seems to be necessary.
7) The rights are granted on a non-exclusive base.	No comment seems to be necessary.
8) A part of the rights is granted on an exclusive basis. Another part of them on an exclusive one (please see c the rights granted).	No comment seems to be necessary.
9) The exclusivity is granted on the licensed rights in relation to the territory and the program.	No comment seems to be necessary.
10) The right is granted on a non-exclusive basis.	No comment seems to be necessary.
11) Exclusivity is not foreseen.	No comment seems to be necessary.
12) Exclusivity is granted.	No comment seems to be necessary.
13) Exclusivity is not granted.	No comment seems to be necessary.
14) Exclusivity is not foreseen.	No comment seems to be necessary.
15) Exclusivity is not foreseen.	No comment seems to be necessary.
16) Exclusivity is not foreseen.	No comment seems to be necessary.
17) Non-exclusivity is explicitly foreseen	No comment seems to be necessary.
18) Non-exclusivity is explicitly foreseen	No comment seems to be necessary.
19) Non-exclusivity is explicitly foreseen	No comment seems to be necessary.
20) The licence is a non-exclusive one	No comment seems to be necessary.

f) Duration

Duration
1) One year, automatically renewable
2) One year.
3) One year and afterward till the 90th day after the notice by one of the parties of the will to terminate the contract.
4) Till a specific date (many years)
5) Six months renewable for another six-month period … unless Licensor gives not less than 1 month prior written notice to Licensee before the expiry of the initial term, in which case the term will end after first period
6) The term of the agreement is seven years commencing from the date of delivery of the first picture.
7) The term is a period of seven (7) years, unless earlier terminated in accordance with the terms and conditions
8) *"The term of this Agreement and the period of time in which Licensee and/or its permitted assignees or sublicensees may exercise the Rights shall be for a period commencing on the date hereof and extending up through and that date that is five years and six months from the date hereof (the "Term" or the "License Period)".*
9) The term of the Agreement can be determined in the Addendum A.

10) The possibility to foresee the term of the agreement is foreseen in the body of the contract but not determined.
11) The parties can agree a term for the contract in the purchase order form.
12) The standard contract model foresees the possibility to fix a term.
13) The Agreement expires after XXX period*, unless it is renewed in writing by both parties. During any renewal period, the Licensor shall have the right to terminate this Agreement upon giving 30 days' notice in writing*
14) No term is foreseen.
15) It is an open-ended contract
16) No term is foreseen.
17) No term is foreseen.
18) No term is foreseen.
19) No term is foreseen.
20) No term is foreseen

g) Remuneration method

The method used to calculate the remuneration is often based on a royalty system.

Remuneration method	**Comments**
1) The licensor is remunerated with a percentage (40%) on the net income received by the digital reseller for the download of recordings and video files. As far as ring tones and wallpapers are concerned a percentage of 50% on the net amount paid to the licensee is due to the licensor.	In the first case the remuneration is calculated on the basis of the income of a third party (the digital reseller). In the second one the calculation takes place on the basis of the income of the licensee.
2) The licensee remunerates the licensor paying a percentage of 20% of each track or album sold.	It is not clear if the 20% should be calculated on the net income or on the gross one.
3) Two different methods of remuneration are foreseen. The first one consists in the payment of a percentage on the net income of the licensee. This method applies to the income coming from subscriptions. The second one consists in a percentage on a fixed wholesale price. The rate is calculated on the basis of the kind of product which is sold and applies to "à la carte" purchases.	No comment seems to be necessary.
4) The receipts are divided among the licensor and the distributor according to a 50% percentage each of the gross income.	No comment seems to be necessary.
5) The remuneration method is based on royalty for each recording used as a ring back tone No detail about the rate of the royalty is reported. Art 6) Most favoured nations *If at any time during the Term hereof, Licensee pays any royalty for the same or equivalent rights as granted herein to any other major international record companies, or to any agent of the same (including any music industry rights society), that is greater or more beneficial than the Royalty specified*	It seems to be quite unusual foreseeing a clause for the change of currency from XXX rate to another currency- Until July the 21st 2005, the change took place at a fixed rate. The contract also includes a particularly interesting clause in art. 6.

above, Licensee shall pay such royalty and offer such other financial terms to Licensor retroactively to the accounting period during which such higher royalty and other sum(s) are accounted to such other record companies.	
6) The remuneration method is based on one hand to the delivery of company's' shares and on the other hand, as far as the new releases are concerned, on a license fee.	It is quite unusual the payment of a remuneration by means of the delivery of company's shares.
7) An annual fee is foreseen.	No particular comment seems to be necessary.
8) There is nothing of explicitly foreseen about the remuneration. It seems that a fixed payment (*"fair and adequate consideration"*) has been made by the licensee to the licensor before the sign of the contract.	No particular comment seems to be necessary.
9) The remuneration system foresees the payment of a fixed amount.	No particular comment seems to be necessary
10) The remuneration system foresees the payment of a fixed amount.	No particular comment seems to be necessary
11) The fees assessed for the Licensee's use of the Licensed Material shall depend on the use, period of time, territory, the number of broadcasts and any other elements specified by the Licensee in the Purchase order form.	The quantification of the fee depends on a separate document called "purchase order form".
12) The remuneration method consists in a commission on the distributors' income.	No comment seems to be necessary.
13) The fee is calculated on the basis of the tariff of reproduction and user's rights for works of visual arts, as published by SOFAM	It is the only case, among examined contracts where a reference to a Tariff is made.
14) Fixed fee, being a B2C system.	No comment seems to be necessary.
15) Fixed fee is foreseen.	No comment seems to be necessary.
16) No fee is foreseen.	No comment seems to be necessary.
17) No fee is foreseen.	No comment seems to be necessary.
18) No fee is foreseen.	No comment seems to be necessary.
19) No fee is foreseen.	No comment seems to be necessary.
20) No fee is foreseen	No comment seems to be necessary

h) Licensee's Undertakings

This part of the contract disciplines the obligations of the licensee.
This discipline can apply, for instance, to any modification, adaptation, transformation or translation of the content, creating derivative works.
It is worth taking note of the fact that in general all the agreements include the acknowledgment by the licensee of the intellectual property rights of the licensor.

Main Licensee's Undertakings	**Comments**
1) The obligations of the licensee concern first of all the management of the licensor's catalogue (art. 5). Secondly the licensee is requested to verify the payments received from the users and to transfer to the licensor the amounts agreed in the contract.	The right to adapt the contents in a suitable editing format is granted in the license.
2) The obligations of the licensee concern both the financial aspect (payment of the fees) and the use of the contents (pages 1 and 2 of the contract and paragraph named *"Warranties by retailer"*. In particular no alteration of the latter is allowed but the one	The discipline of this aspect seems to be complete and does not seem to need further comments.

necessary to convert the catalogue into a suitable format for the digital retail sale. Further obligations are the following: a) informing the content owner of any claim related to the contents; b) always acknowledging the property of the contents.	
3) The contract (article 4 in particular) disciplines this aspect referring mainly to financial aspects. The licensee undertakes to obtain *"all necessary consents and licenses for the use of the musical compositions embodied in the Recordings"*. No particular limitation is set as far as the use of the contents is concerned.	No further comment seems to be necessary.
4) The contract foresees specific limitations as far as dubbing, subtitling and editing activities are concerned. They need to be specifically approved by the licensor (art. 4, b). The *"Deal terms"* provide a discipline for the financial aspect.	No further comment seems to be necessary.
5) The contract (art. 2) disciplines in quite a strict way the obligations of the licensee and this under several points of view. First of all the minimum price is fixed by the licensor and the use of the content cannot be linked to any advertising or commercial aim different from the one foreseen in the contract (ring back tones providing service). Secondly, the use of the recordings cannot exceed 40 seconds. Thirdly the licensor itself reserves the right to supply the service directly to the user for the first period of the contract. Finally the licensee commits to provide licensor with digital copies used pursuant the license and whose further use by the licensor is free. The licensee accepts to be bound to any contractual restriction which affects the right of the licensor and to obtain all the necessary licenses required in connection with the reproduction and public performance of the Recordings.	No further comment seems to be necessary.
6) The rights granted to the licensee (art. 2) include the possibility to create new versions of the pictures. It is important to take notice of the following sentence: *"Such derivative versions may constitute separately copyrightable derivative works of Licensor…"*. On the other hand, the licensee undertakes to refrain from creating any compilation of the pictures for separate exhibition, other than for promotional purposes or *"in connection with a multi-channel Interact feed"*. The right to translate and dub the title and soundtrack of any and all versions of the picture in any language is foreseen and the right to copy the pictures in any form or medium as well, distributing these copies in the normal course of CBS's satellite, cable or interact business. It is forbidden to the licensee selling such copies directly to the public.	The rights granted to the licensee seem to be very wide and include the right to create new versions of the pictures. This activity is not limited to the translation or dubbing.
7) The licensee undertakes to respect the discipline given by the "XXX License Guidelines", a document that identifies its obligations (art. 2). The licensee has the obligation to refrain from distorting or misrepresenting any material contained in the licensor's content. In the event that the licensee desires to use any music included in	No further comment seems to be necessary.

the licensor's archive, it undertakes to pay the legitimate fee to the content owner. As far as a notice of copyright is concerned, the licensee undertakes to put this notice on each content provided by the licensor.	
8) The rights granted to the licensee include the possibility to elaborate the pictures getting derivative works (art. 2). The licensee undertakes to refrain from changing the name of the titles including some words whose copyright is owned by the licensor and listed in an attached document. The right to sublicense is given to the licensee but limiting it to the off line distribution. The right to sublicense in an on line context is strictly limited.	No further comment seems to be necessary.
9) The licensee undertakes to refrain from making any use of the contents other than the one agreed in the contract (art. 5). Minor modifications or reductions made by the licensee to the contents are allowed if they are justified by technical or programming requirements (art. 9).	No further comment seems to be necessary.
10) The user is entitled to use the licensed content just in a specific programme (art. 4).	No further comment seems to be necessary.
11) As far as the "Conditions for use" are concerned, the user undertakes to respect intellectual property rights and not to allow other people to have access to the web site using the password of the user himself (art. 23). The "General license conditions" foresee the right for the licensee to use the content respecting the limits set by the contract. Neither an *"expanded use"* without prior written consent of the licensor nor any sublicense is allowed (par of the document named *"Rights granted"*).	No further comment seems to be necessary.
12) In this contract the licensor seems to be in a weaker position than the licensee. The obligations of the licensor are carefully described. They include the obligation of the licensor to provide its contents in a format compatible with the technical requirements of the licensee's platform (art. 11.2).	No further comment seems to be necessary.
13) The rights of the licensee are restricted, as far as the possibility to sublicense is concerned, being this forbidden without the consent of the licensor (art. 3). The only use allowed of the contents is the incorporation in vignette form in the database, available on the licensee's web site (art. 2.2). No right to alter the contents is granted (art. 7).	No further comment seems to be necessary.
14) The contract is concluded between an on line music retailer and a user. The user undertakes to use the products purchased only for personal, non-commercial use (art. 9).	No further comment seems to be necessary.
15) This contract too is concluded between a content owner and a consumer. Therefore the user undertakes to use the contents for personal use. Moreover the user undertakes to use some specific devices (indicated by the content owner) to get the service (art. 10).	No further comment seems to be necessary.
16) The text content provider forbids to the user any unlawful use of its web site and its web services. Any commercial use is forbidden as well (art. 5).	No further comment seems to be necessary.

17) This contract concerns the access to a website which has a didactical aim. Therefore the user undertakes to use the contents of the website for non-commercial research or teaching. Any downloading or changing of contents of the site is not allowed without the consent of the owner of the web site.	No further comment seems to be necessary.
18) The activity of digitisation licensed to the licensor is restricted to a not commercial use as, for instance, research, testing, demonstration or educational purpose (art. 4).	No further comment seems to be necessary.
19) The licensee or any organization using images included in the web site are allowed to do so just for testing or demonstration purposes and for a commercial one (art. 5).	No further comment seems to be necessary
20) The licensee undertakes to use the licensed contents just for personal and non-commercial uses. Therefore, for instance, no derivative work is allowed.	. No further comment seems to be necessary

i) Warranties and indemnities

The warranties are given mostly by the licensor to confirm that it is really entitled to grant the rights as foreseen in the contract.
As far as the licensee is concerned it is worth noting that this term is often used to state that this party of the contract has already obtained all the necessary authorizations for the lawful execution of the activity foreseen by the contract. On the other hand indemnities are not always foreseen.

Warranties and indemnities	**Comments**
1) The licensor guaranties that it owns the rights licensed in the agreement and it states that it will keep the licensee free and harmless from any claim related to the object of the contract (art. 3). Neither a warranty by the licensee nor an indemnity for the breach of the contract is foreseen.	No further comment seems to be necessary.
2) The discipline of the warranties of the licensor is not very clear. The most important sentence, under this point of view, seems to be the final part of point 9: *"Any sound recordings and the underlying musical compositions that are provided on behalf of OWNER to XXX must be owned or controlled by OWNER and/or have been cleared by OWNER"*. In the section *"Warranties and Undertakings by the Owner"*, the sentence that is used is slightly more ambiguous: *"The OWNER warrants and undertakes with the retailer that it is authorized to enter into and give effect to this agreement;…"*. The warranties by the retailer are more wide and partially concern aspects which have been already examined in the *"Licensee's undertakings"* section. They refer to the respect of the rights of the content owner, in particular in relation with the terms of the contract (for instance use of the rights granted within the license period and territory). No indemnity is foreseen. The only regulation about this is given, in general terms, in point 2.14 in case of *"claims, damages and demands arising out of any breach or non performance by the retailer of all or any of the retailer's warranties in this clause"*.	No further comment seems to be necessary.
3) Art . 4 disciplines this aspect. As far as the licensor is concerned, the warranty consists in assuring that not only it owns the rights granted but also that it has regulated	No further comment seems to be necessary.

all the relationships with third parties which own rights related to the contents so that the use by the licensee is completely legitimate. The licensee warrants that it will get all the necessary licences for the use of the musical compositions granted and pay all mechanical royalties due. The payment of an indemnity is foreseen in case of a claim brought against the licensor by a third party in relation to a breach of the contract by the licensee (art. 7).	
4) The warranties given by the parties are particularly wide. The licensor (art. 17) warrants that it owns the right granted but also commits to do all reasonable effort to ensure that its suppliers of digital technology do not display any solution, which could harm or make more difficult the activity of the licensee. The licensor (art. 18) warrants that it is able to execute the contract in a lawful way not infringing any discipline or regulation. An indemnity is foreseen for any breach of the contract by both parties, licensor and licensee (art. 19).	No further comment seems to be necessary.
5) The licensor warrants that it owns the rights granted (art. 7). The licensee warrants that it is based in a specific territory, the same where the license takes place. As far as the legitimate use of the rights granted is concerned, it commits not to license or distribute to any third party suspected of being involved in piracy cases. Both parties undertake to keep the other harmless from any claim coming from a breach of the contract by the party concerned.	No further comment seems to be necessary.
6) The licensee warrants being able to execute the contract (art. 11). On the other hand the Licensor guarantees that it owns the rights granted and that the contents are lawful. Both parties undertake to keep the other harmless from any claim coming from a breach of the contract by the party concerned.	No further comment seems to be necessary.
7) The licensor and the licensee warrant that they own the rights necessary to execute the contract. As far as the licensee is concerned, the reference is made to the rights related to its web site. In this case too, both parties commit to keep harmless the other party in case of breach of the contract by the concerned party.	No further comment seems to be necessary.
8) The licensor warrants that the licensed contents are lawful (art. 6). This aspect is particularly sensitive considering that the contents licensed are films for adults. Further warranties concern the absence of any debt related to the production of the contents. The licensee, on its hand, warrants that he will obtain all the licenses, permits and approvals necessary for the execution of the contract. As far as the indemnities are concerned, the parties recognize the right of the other party to be indemnified in case of breach of the contract by one of them. Moreover the licensee warrants that any derivative work will be lawful and produced in full respect of any regulation (art. 7).	The specific discipline is due to the fact that the contents licensed are pictures and films for adults.
9) The licensor warrants that it owns the rights on the licensed contents and that there is no other agreement with third parties, which can restrict the use of the licensee (art. 5). The licensee warrants that it will not make any other use of the content other than the one agreed in the contract.	No further comment seems to be necessary.

This contract too foresees the clause examined in the above mentioned contracts and related to the indemnity, which should be paid by one party to the other one in case of legal action taken following a breach of the contract by the concerned party.	
10) The licensor (user) warrants that it will not use the content to damage or offend a third party. On the other hand also choosing the music score is requested to be consistent with the content (art. 6). In any case any action taken for the misuse of the video content will be in the exclusive responsibility of the licensor.	No further comment seems to be necessary.
11) a) No regulation about warranties is foreseen. b) The licensor warrants on one hand that it concludes the contract with the consent of all the other parties involved in the production of the licensed material. On the other hand it warrants that the copy of the licensed content is free from defects. The licensor warrants indemnifying the licensee in case a legal action is taken against the latter for a use of the content, which has been in accordance with the general conditions, here examined (paragraphs 28 – 33).	No further comment seems to be necessary.
12) The contract foresees only the guarantees of the licensor (art.11). It warrants that it will keep harmless the licensee for any action taken because of the content on the licensed material. Moreover it guarantees to the users the access to its on line resources. There is no clause disciplining indemnities.	No further comment seems to be necessary.
13) The licensor expressly does not warrant anything related to the content of the agreement (art. 8). On one hand the contract limits the liability of the licensor. On the other hand the licensee warrants indemnifying the licensor of any cost, claim, demand and expense *"arising out in connection with the subject matter of this Agreement"*.	No further comment seems to be necessary.
14) Art. 18 foresees a strict limitation of the warranties given by the on line shop.	No further comment seems to be necessary.
15) Art. 12 limits the responsibility of the licensor. The contract foresees an obligation of the user to indemnify the licensor for any cost or expense suffered for a breach of the contract whose responsibility is on the user.	No further comment seems to be necessary.
16) Art. 6 limits the responsibility of the internet service provider and limits its liability.	No further comment seems to be necessary.
17) No warranty is foreseen.	No further comment seems to be necessary.
18) The licensor warrants that it owns the licensed contents and that it will indemnify the licensee in case of breach of this warranty (art. 3).	No further comment seems to be necessary.
19) The licensor warrants that it owns the licensed contents and that it will indemnify the licensee in case of breach of this warranty (art. 4).	No further comment seems to be necessary
20) As already seen in some other contracts, this contract includes a very wide disclaiming clause of the licensor form all warranties and liabilities.	. The position of the licensee is particularly weak compared to the licensor's one. The aim of the latter seems to be avoiding any kind of responsibility linked

	to the use of the web site by the users.

l) Termination

The aspects of the license period and of the termination circumstances are shortly examined hereunder.

Termination	**Comments**
1) The licence period is of 12 months and the contract is tacitly renewable, for further periods of 12 months each (art. 8). No termination case is explicitly foreseen.	No further comment seems to be necessary.
2) The contact is valid for 12 months. No possibility of tacit renew is foreseen (art. 1). No termination case is explicitly foreseen.	No further comment seems to be necessary.
3) The licence period is of 12 months. The termination can occur also in case of serious breach of one of its obligations by one of the parties or when a receiver, a liquidator or trustee in bankruptcy is appointed for either party and not removed within 60 days of its appointment (art. 6)	No further comment seems to be necessary.
4) The licence period expires at a fixed date.	No further comment seems to be necessary.
5) Schedule A foresees a fixed license period tacitly renewable. The contract (art. 4) foresees the possibility for the licensor to terminate the contract upon notice in one of the following cases: - breach of the contract by the licensee; - attempt of the licensee to assign any of its rights without the consent of the licensor; - change in the control or ownership of the licensee. The contract terminates automatically if: - licensee is dissolved or its assets are liquidated or it becomes insolvent; - a bankruptcy proceeding takes place with respect to the licensee or its assets.	No further comment seems to be necessary.
6) No discipline of this aspect is foreseen.	No further comment seems to be necessary.
7) The licence period is seven years. The licensor can terminate the agreement in one of the following circumstances (art. 6): a) breach of the contract or of the *"License guidelines"* by the licensee; b) insolvency or bankruptcy of the licensor; c) more than 15% of the shares of the licensee are owned by a competitor of the licensee; d) the licensee discontinues using the web site approved by the licensor.	No further comment seems to be necessary.
8) The license period is five years and six months (art. 3.1). The contract does not foresee explicitly any circumstance, which involves the termination of	No further comment seems to be necessary.

the contract. Special importance is given to the timely delivery of the material but a breach of the contract under this point of view does not seem to have as a consequence the termination of the contract.	
9) The license period is fixed in the Addendum A. Nevertheless the contract foresees some circumstances where it can be terminated before the term: a) the licensee is insolvent; b) the licensee discontinues business with regard to audiovisual exploitation; c) the licensee fails to pay to the licensor the amounts agreed in the contract; d) the licensee reproduces materials in excess of normal transmission requirements; e) the licensee transports the Materials outside of the *"Territory"* without the consent of the Licensor.	No further comment seems to be necessary.
10) A fixed license period is foreseen.	No further comment seems to be necessary.
11) a) There is no fixed licensed period but it is foreseen that any misuse of the license can involve the termination of the agreement (art. 22). On the other hand a modification of the conditions of the license by the licensor gives the faculty to the licensee to terminate the contract (art. 10). b) No discipline of the termination is foreseen in the contract. This aspect will be regulated in the *"purchase order form"* (art. 7).	No further comment seems to be necessary.
12) A fixed license period is foreseen. The contract specifies that it can be terminated in case of breach by one of the parties of the obligations set by the contract (art. 13).	No further comment seems to be necessary.
13) The contract foresees a fixed license period but it can be terminated in case of breach of the agreement by one of the parties or if the licensee is insolvent (art. 10).	No further comment seems to be necessary.
14) The licensor can terminate the agreement even if it suspects a breach of the contract by the licensee. The licensor reserves the right to modify or discontinue the service without being liable to any third party (art. 14).	No further comment seems to be necessary.
15) The term of the license period is not fixed.	No further comment seems to be necessary.
On the other hand it is possible terminating it by mean of a notice of 60 days (art. 21). The licensor can terminate the agreement in case of insolvency or bankruptcy of the licensee (art. 22).	
16) No term of the contract is foreseen but the licensor can terminate it at any time in the event of any conduct of the licensee deemed	No further comment seems to be necessary.

"unacceptable" or in the event of a breach of the contract (art. 9).	
17) The agreement foresees that any breach of it will lead to immediate termination (central part of the contract, there is no indication of the article).	No further comment seems to be necessary.
18) No discipline of the termination of the contract is provided.	No further comment seems to be necessary.
19) No discipline of the termination of the contract is provided	No further comment seems to be necessary
20) There is no fixed licensed period. On the other hand, the licensor reserves the right, in its sole discretion, to restrict the access to the web site in case of violation of the discipline given by this agreement	No further comment seems to be necessary

m) Jurisdiction

Jurisdiction	**Comments**
1) Tribunal of Rome is competent for any dispute arising from the contract (art. 10).	Both parties reside in Italy but it is specified the jurisdiction belongs to the Courts of the city where the licensor is based.
2) The agreement is governed by the Jamaican law and the Jamaican courts are the courts of competent jurisdiction (art. 10.1). Nevertheless article 11 foresees an obligation to refer any dispute to arbitration in accordance with the Arbitration act of Jamaica.	The courts of the licensee's country have the jurisdiction.
3) The contract is governed by English law and English Courts have the exclusive jurisdiction (art. 10).	Both parties are English. No particular forum is specified.
4) The copyright law of the United States of America applies. Any dispute is to be resolved by mean of a binding arbitration regulated under the XXX Rules for International Arbitration. The agreed forum is New York (page VST – 5)	The jurisdiction is not of the country where the licensor is based. On the other hand the licensee and, as a consequence, its base is not known.
5) The license is construed in accordance with the substantive and procedural laws of the Hong Kong Special Administrative Region (art. 8, lett. c).	The courts of the licensor's country have the jurisdiction (in an inappropriate way we consider People's Republic of China and Hong Kong Special Administrative Region two different countries).
6) No discipline of this aspect is foreseen.	
7) The contract is governed by the laws of the State of New York (art. 7.10).	The courts of the licensor's state (in the U.S.A.) have the jurisdiction.
8) The agreement is governed by the laws of Colorado and the federal laws of the United States of America. The parties agree that any dispute shall be resolved by the courts *"located in Denver, Colorado, Philadelphia, Pennsylvania or New Jersey"* (art. 15).	Both parties are U.S.A. companies. Both states where the companies are based have the jurisdiction.
9) The agreement is governed by the Italian law	The courts of the licensor's country have the

and the Courts of Rome are competent to solve any dispute. Nevertheless licensor may commence proceedings before the Courts of licensee's country (art.15).	jurisdiction.
10) The law, which is applicable to the contract, is the Italian law and the exclusive Forum is the forum of Rome (art. 11).	The courts of the licensor's country have the jurisdiction.
11) a) the agreement is governed by the Belgian laws. Any dispute will be solved by mean of an arbitration, which will take place in Brussels. Nevertheless in case of proceeding of a legal action by the licensor, Belgian courts have the exclusive jurisdiction (art. 34 – 35). b) as in point a) Belgian laws apply and an arbitration is foreseen to solve any dispute. Nevertheless the licensor can commence a legal action before a competent jurisdiction in Belgium *"to obtain injunctive or other appropriate relief, in case the licensor is of the opinion that such action is necessary or desirable. In such event, the courts of Belgium shall have exclusive jurisdiction."* Art. 46 – 47.	The courts of the licensee's country have the jurisdiction.
12) French law applies to the contract. The jurisdiction is of the French courts, the agreed forum is Paris (art. 14).	The courts of the licensee's country have the jurisdiction.
13) Art. 12 disciplines that the national law of the licensor applies to the contract and that any dispute will be solved by the national courts of the latter.	No further comment seems to be necessary.
14) The agreement is governed by the laws of the State of California. The jurisdiction resides in the courts of the State of California (art. 22).	The courts of the licensor's country have the jurisdiction.
15) Italian law applies and the parties agree the jurisdiction of the Italian Courts in Milan (art. 27).	The courts of the licensor's country have the jurisdiction.
16) The contract is governed by the laws of the State of Georgia (U.S.A.) and the jurisdiction for all disputes resides in the Superior Court of Dekalb County, Georgia or in the United States District Court for the Northern District of Georgia, Atlanta Division, Atlanta, Georgia (art. 12).	The clause seems to put the user in a weak position considering that, signing the contract, he agrees to indemnify the licensor for any legal action commenced before Courts different from the ones indicated in the contract (Georgia's Courts).
17) The agreement is governed by English law and is subject to the exclusive jurisdiction of the English courts (art. 9).	The courts of the licensor's country have the jurisdiction.
18) The agreement is governed by English law and is subject to the exclusive jurisdiction of the English courts (art. 10).	The courts of the licensee's country have the jurisdiction.
19) The agreement is governed by English law and is subject to the exclusive jurisdiction of the English courts (art. 13).	The courts of the licensee's country have the jurisdiction.
20) The law of the State of Florida applies to the contract. The jurisdiction resides in the courts of the County of Palm Beach, State of Florida and	The courts of the licensor's country have the jurisdiction. The clause contains a further disclaimer having as

any legal proceeding must be commenced within one year after the occurrence of the facts giving rise to the cause of action.	its object the use of the contents in territories where the law of the State of Florida does not apply.

PART B)
Analysis of the contracts with respect to the different media devices, which are used to provide the content to the consumer: PC, Mobile, satellite etc
The table hereunder shows the digital devices used in the execution of every contract examined in part A): computer, TV set top box, mobile phones.

Contract	**Device**
1	The contents can be either downloaded from a web site (so using a computer) or sold to the users by mean of mobile phones (true tones).
2	Computer
3	Computer
4	It seems that in this contract the execution takes place off line. Nevertheless its execution could also take place by mean of a digital device (TV set top box).
5	Computer
6	TV set top box, computer
7	Computer
8	TV set top box. Computer.
9	Any kind of TV, also using TV set top box.
10	Any kind of TV, also using TV set top box.
11	Computer
12	TV set top box
13	Computer
14	Computer
15	TV set top box
16	Computer
17	Computer
18	Computer
19	Computer
20	Computer

It is necessary taking notice of the fact that at this stage contract practices are still developing in order to deal with the new issues set by the transmission of contents by mean of electronic devices.
An important role in this scenario is played by technical protection measures and this under two different aspects: on one hand they are used to structure copyright related aspects of what is offered to the consumer, on the other hand they are used to structure the commercial offering, what is the offer to the consumer[9].
The analysis, which is proposed hereunder, examines three different devices used to exploit contents: Internet, TV and mobile phones.

Computer

[9] This aspect has been examined by Timo Rukkia (Nokia Corporation) in his article *"Contractual balance in digital content services"* available in the internet
(http://www.indicare.org/tiki-read_article.php?articleId=113).

A preliminary distinction should be done between B2B (business to business) and B2C (business to consumer) contracts.

The contents that circulate in the Internet in a B2C (business to consumer) context may be offered against the payment of a fee (contract n. 14) or for free (contract n. 16, 17 and 20).
These two options involve different definitions of the main clauses, which discipline the relationship between the licensor and the licensee/customer/user.
In case of a remunerated license, the customer can often proceed to a wide use of the content, for instance producing derivative works. The copyright on the latter belongs either to the licensee (this seems to be the solution adopted in contract n. 11) or to the licensor (contract n. 6 art. 2.6). A third option could be sharing the copyright between the licensor and the licensee.
On the other hand, some contracts, despite of the remuneration for the service, oblige the licensee to a personal and non-commercial use of the licensed content (contract n. 14 art. 9).

In a B2C context the owner may choose between different forms of license and under this point of view an important role is played by a preliminary distinction between subscription models and Digital Rights Management (DRM) regime.
In the first case the user buys a file, in the second just rents it and therefore the discipline is much stricter and the need for efficient technical protection measures is clear[10].

The warranties related to the service and given by the licensor are quite wide in case of a remunerated license considering that the quality of the service is the first step to get purchases from users.
If the service is not remunerated, the licensor usually uses a disclaimer clause, which limits its responsibility, and liability in case of damages occurred to the user (contract n. 20 art. 10).

B2B (business to business) context requests further comments.

- The exclusivity clause often applies.
- The restriction of the license to a specific territory, by mean of a specific clause, is possible if supported by adequate technical protection measures as, for instance, the detection of the location of the URL.
- The rights granted to the licensee may include the possibility to produce derivative works.
- The restrictions of this right can vary. Contract n. 8 art. 2, g) for instance obliges the licensee to refrain from using some words which are trademark or trade name owned by the licensor.
- The termination of the contract is generally foreseen in case of breach of the contract by one of the parties but a specific clause regulates in most of the cases a "warning" procedure aimed to solve the dispute without terminating the contract (for instance contract n. 3 art. 6). A notice is sent by one of the parties to the other and a delay is set to rectify the breach.

TV set top box
The contracts whose execution occurs by mean of digital television can also be distinguished in two categories: B2B and B2C.

In a B2C context the exploitation of the rights granted may occur on a personal and not commercial base.
The service is generally against remuneration, which is generally calculated on a video on demand (contract n. 15) base or by mean of a periodical subscription.

In a B2B context, the discipline of the territory where the rights are granted is often different from the one in case of exploitation via Internet.

[10] An interesting analysis is available in an article by Philip Bohn, Berlecon Research, Berlin *"Do you subscribe to digital music?",* http://www.indicare.org/tiki-print_article.php?articleId=112.

In this case, it is easier, compared to the exploitation via Internet, granting a right limiting the exploitation to some specific countries and this without particular technical protection measures. This difference is put in evidence in contract n. 8, art. 1.15.

Mobile phones

It should be noted that the contractual regulation of the contents' transmission via mobile phones is still developing and the state of the play shows a lack of samples of contract drafted by the main players.
Some multinational companies, which have been contacted to get the samples of the contracts used by them, have stated that till now they have not drafted any sample of contract to discipline all their B2C or B2B relationships, leaving all to a case by case discipline.
This preliminary remark helps to explain why an analysis which is based on contracts is necessarily limited by the lack of material to examine.

Nevertheless it is worth proposing some very short comments.
Examining the use of this device it is clear that we can distinguish, also in this case, between a B2B and B2C context.
The relationship B2C is apparently simple and the right granted is often directly remunerated by the customer by a prepaid card.
The relationship B2B deserves one more comment.

The territory where a right is granted in the context of a license is not particularly problematic to define and this is thanks to the structure of cells and clusters, which allows the operation of these devices.