

# Digital images protection management in a broadcast framework:

## "Overview/TALISMAN solution"

C. Simon	Thomson-CSF
E. Goray	RTBF
G. Vercken, B. Delivet	ART3000
JF. Delaigle	UCL
JM. Boucqueau	UCL

### Abstract

Works undertaken by international structures addressing digital video products protection are described in an overview, in order to give a deep insight into the current context. Expectations from the professionals in the field are therefore commented and analyzed. Different studies are progressing towards a generic model definition to protect digital products by several projects. Different scenarios are nowadays considered by the ACTS TALISMAN<sup>1</sup> project, the first one based upon a conservative approach called 'a posteriori' scenario stating that a work is only protected after its creation. Its major pending issue is whether anyone can be able to generate a digital protection or whether this could only be provided by an authorized institution (Copyright Authority). The second approach deals with a completely new and original view relying upon the fact new technologies enable works protection while their creation, thus avoiding circulation of non protected works involving complex management. Both approaches for a Common Functional Model for Copyright are presented and investigated in the paper.

### 1. Introduction

With the increasing availability of digitally stored information and the development of new multimedia broadcasting services, security questions are becoming ever more urgent. The acceptance of new services depends on whether suitable techniques for the protection of the information providers' interests are available. One problem that has not found a solution yet is the one of how to realize copyright protection for digitally stored data. The TALISMAN project, ACTS project Number AC019 supported by the CEC, has as objective to develop a standard copyright mechanism to protect multimedia providers digital products against piracy and illegal copying.

TALISMAN scope can be depicted as follows:

- focus on video services protection;
- address as much as possible today' video transmission means i.e. numerical formats, emerging standards (MPEG) and different broadcasting media (satellite, ATM and CATV);
- bring solutions against industrial forgery; forgery at individual level is not addressed by the project but, could later on, thanks to the mechanisms developed, be envisaged.

TALISMAN is setting up an evolutive and open framework based upon authors' societies, contents providers and broadcasters requirements allowing integration of a hierarchy of solutions for protecting video contents. Instances of such solutions encompassing low end systems based upon header description associated with the bit stream (called *labeling*) up to high end sophisticated, holographically inlayed, undeletable systems (called *watermarking*) will be developed. Associated hardware implementation to support and exploit such realizations in a cost efficient way will therefore be provided.

Besides protection techniques (labeling and watermarking), the whole system specification encompassing:

- the major actors definition in a multimedia chain;
- the qualification for their interrelationships;
- their derivation to a suitable semi-formal model

constitutes the backbone of a copyright system. This is called a **Common Functional Model** identifying on a rather abstract level major system components and different flows between them. This is one of the key issues; the objective of this paper is to provide a complete review of the context from multiple views: legal current

---

<sup>1</sup> TALISMAN stands for Tracing Authors' rights by Labeling Images Services and Monitoring Access Network

actions, professionals expectations and the replies that secure technology could bring analyzing possible alternative models.

The paper first reviews current state-of-the-art encompassing works identification lead by different international organizations, highlighting the major actors in a multimedia chain. From the potential end users' expected requirements, it then overviews existing approaches and, finally, provides a discussion around possible alternatives for a Common Functional Model for Copyright.

## 2. Works identification legal context

The world of copyright administration is fully aware of the (r)evolution in the profession involved by digital technologies over the next decade. Many works are currently carried on by different international organizations with the objective to fulfill the need for simple, effective, common means of identifying copyright material and its ownership. Works not only deal with unique international numbering, such as ISBN (books), ISRC (recordings), ISWC (musical records), UIN (audio-visual works) but also covering things which are to be numbered.

There is no international standard method nowadays neither for numbering nor for describing copyright material, storing and communicating this descriptive information to other parties.

Because of this, major international organizations (ISO, BIEM/CISAC, AGICOA/CISAC) are working in this direction. TALISMAN reviewed in detail the different approaches serving as a basis for its protection model; due to their commonalties, confidence in having a Unique Identification Number at an international level at a medium term for all audio-visual works can be stated.

### 2.1 Major International Organizations

Many works have already been carried on by different structures; the main ones together with their objectives are presented in this section but cannot be exhaustive.

Organization	Meaning	Objective
<i>AIDAA</i>	International Association for Audio-visual Authors	Association at the international level of all authors' societies managing scriptwriters or film makers' right. Above all, this association carries on with a political defense of its members' right.. On the one hand, it does not interfere so much on the modes of management of its members, and on the other hand, it has an important representation as well as the corresponding political power.
<i>AGICOA</i>	Association for International Management of Audio-visual Works	Due to manage producers' right for audio-visual works which are going to be transmitted by cable. It concerns producers from the whole world. Even if its object is limited to the right's management onto the cable, it is therefore important because of its representation.
<i>BIEM</i>	International Office of Mechanical Recording	Grouping of societies managing specifically the right of mechanical reproduction. Most of these societies are either members of the CISAC, which is also responsible for the management of representations right, or societies only managing mechanical reproductions right. BIEM interferes in a very determining way into the definition of the modalities concerning a management common to all its members.
<i>CISAC</i>	International Confederation of Authors' and Composers' Societies	Grouping of all the authors' and composers' management societies in the field of musical works, plastic and graphic arts, theater works, audio-visual works. But in practice, it is much more active in the field of music. This is the most powerful authors' structure at the international level.

<b>CESAC</b>	European Group of Authors and Composers	Counterpart of CISAC for the European Community.
<b>FERA</b>	European Federation of Audio-visual Producers	Grouping producers' associations and societies. Since the producers are not considered as authors in all the countries, FERA also involves some producers' associations that have no power of management. The political influence of the FERA is very significant.

## 2.2 Works Identification Review

During the elaboration of the compression standards (*JPEG* for still images and *MPEG II* for videos), some representatives right holders were very attentive on the fact that a certain number of bits should be reserved for works identification.

The *ISO standard N1388* which is linked with the generic encoding of moving images and its associated sound (MPEG II), is reserving since then a 64 bits « copyright space ». This space being reserved, its contents has now to be defined. ISO has as aim to set up a central and international structure (Copyright Registration Authority) in charge of works' identification attribution and registration.

By the meanwhile, many *works are carried on by the Right Holders* proposing schemes for digital works' identification. Among them:

### 1) *Unique Identification Number (UIN - AGICOA/CISAC) for video images*

In opposition to the situation for books or sound records, there is no identification system today for audio-visual works or still images in the analog or numerical field.

The foreseen 64 bits MPEG identification of digital data does not technically make possible to keep enough place to give at once all information concerning a work (type of the work, country of origin, source language, owners of the right, and chain of contracts...). The solution proposed by CISAC and AGICOA is to insert a unique number of identification that would refer to a data-file, after being allocated to each work. This data-file could be one or more international data about audio-visual works. It would then be easy to identify the works, and at the same time, exchange information about these works. The number would be given once for all to each work, without any possibility to remove it.

In return, to be able to represent the changes intervening into works life, the database whose number is linked, would be modifiable at any time. It would therefore be possible to control information to be stored, to proceed on updating actions and managing anomalies.

### 2) *ISPN (International System Picture Numbering)*

Besides efforts made for the codification of audio-visual works, there are some other projects about identification of fixed images. This system would have the same structure as the ISBN, with an important space for the identification of the right holders, because of the large number of fixed images especially pictures that are created every day (about 400 new pictures per week at the AFP).

The development of this codification is conducted by the SCAM in France, a civilian society for multimedia authors, directly related to photographer agencies, for a better harmonization of the codification.

### 3) *The Common Information System BIEM/CISAC (CIS)*

*"The CIS is in reply to the need of authors and right holders to identify and to distinguish the works in a standard way, and at a world level, and give information about these works."*

This identification number is common to all kinds of works (musical works, audio-visual works, literary works and works of plastic).

*"The aim of the project CIS is that all the societies concerned adopt a unique identification number for all kinds of work, for the right holders, the sound-recordings and the contracts. This unique number will then be submitted to the ISO to be standardized."*

This provides :

- the identification of a work (pattern of the existing encoding systems like the ISBN, EAN, ISRC - or of systems on the way to be created like the ISRC)

- information about the work: relative to the « interested party » (authors, composers, producers, authors' societies); relative to the work; relative to the work's right : exploitation 's contract

There is no existing method today of international description, of storage or of descriptive information communication. This method is proposed by the CIS project with the « Common Copyright Data Model » and the Common Information System Architecture for Communication.

The project CIS is not only predicting the identification number, but also the modalities of its management. The main tool is the creation of an international virtual database.

*"Each society will enter the data relative to its territory and will have a direct access to its sisters societies' data that can be used again immediately, without any transformation or recording".*

This system thus creates an international virtual data-base that allows a user to have an access to these data, wherever they are located on the network.

Studies provided by the UIN and the ISBN are integrated into the CIS.

The essential question is to know whether these identification systems are going to be reserved to members of authors' societies, or whether all the professionals will have an access to this codification for non-registered works that are not managed by societies. The answer is postponed for now.

**Identification systems also exist in the analog field:** example of ISBN (International Standard Book Number) which is the international number given for books and the ISRC (International Standard Record Code) with the aim to identify the audio-visual recordings. The ISRC is supposed to be used by the producers and the right holders.

### 2.3 The Common Copyright Data Model

The Common Information System (CIS) identification number is just one part of a complete project dealing with copyright to be submitted to the ISO for standardization; a zoom over the project is given below. Besides numbering itself, the project also covers the definition of a model working for any kind of copyright material including music, film, literary texts and computer software. The model covers four items:

- entities types
- data entity structure for Interested Parties
- data entity structure for Works
- data entity structure for agreements

The following just presents the first item (further details can be found in [1]) extracted from the CISAC proposal, thus better assessing a work characterization. All kinds of recordings and products are grouped under Work entity type.

Data Entity Type	Definition	Examples
<b>Interested Parties (IP)</b>	A person (natural or legal) who has contributed in some way to the creation of a property or acquired rights on it.	Composers, authors, performers, producers, film companies, copyright societies
<b>Work</b>	An intellectual creation which is, was or may be protected by law on authors' or neighboring rights. Works may or may not take on a physical form.	Audio visual works in particular, photographs, videocassettes, multimedia products
<b>Agreement</b>	An agreement between IPs which determines rights to work.	Agreements between authors and publishers, performers and records companies, publishers and sub-publishers
<b>Licensing Scheme</b>	A scheme or agreement under which copyrights are used.	Society licensing schemes, publisher licenses, industry agreements

The Working Group 'International Communication' is building an architecture for communication between CISAC societies. The architecture is based on the definition of an open information system to be implemented

in each society in order to facilitate communication with the whole network. This is based upon the principle of 'Virtual Databases' meaning that the database gathering all the management characteristics is distributed over a network and is seen as a unique one from the users' point of view.

### 3. Requirements towards copyright electronic protection

#### 3.1 Impact of works identification onto a protection model

A project such as TALISMAN should ensure compliance with these works principally undertaken by Authors Societies. Compatibility should apply at different levels:

- rely upon the fact that an Image Identification Number will be defined for all audiovisual works in the medium term;
- this number should be a pointer to a database (probably distributed between authors' societies) gathering all characteristics of the works;
- identify actors in the protection model encompassing Interested Parties as defined by the structures.

Interested Parties concern the persons and the societies which exist and which have a link with the work's production or exploitation and can be classified into four categories:

- "Copyright owners" : authors, publishers, producers;
- "Copyright societies" : collective management societies, press agencies;
- "Copyright users" : record companies, movies' producers, broadcasters;
- Manufacturers of equipment used for creation or diffusion (software, cameras...).

#### 3.2 Professionals today' position

Since all the professionals in the channel of broadcast images industry are involved in the appearance of digitization, they belong to different categories: broadcasters, archives management companies, producers, illustrative photographs agencies, photograph agencies, collective management societies, etc. Their view upon the topic vary widely depending upon their maturity towards digitalization and, more important, their habits in their activity. As an illustration, the following roughly describes professionals position for a few categories:

- **TV broadcasters** may be divided into two categories:
  - Major ones, already involved in TV on demand projects feeling very interested by a copyright system such as TALISMAN. Because they want to protect the programs they are producing (concerning the programs they buy, they consider that protection is the responsibility of the authors, or of the producers); also because the protection of images is a way to reassure the right holders (when their works are broadcast). Broadcasters can also avoid the increase of the works prices.
  - Smaller ones, having less investment resources, push the problem to authors and producers; anyway, they all state that cost of protection should be as low as possible.
- None of illustrative **photograph agencies**, due to their privileged human aspect, already digitize their photographs nowadays; anyway, they are quite conscious that protection should be of the highest importance in the near future but, again, at a low price. On the reverse, photograph agencies, building databases of historical, political, sports events,... are extremely sensitive to the problem, mainly over a network.
- **Collective societies** are obviously very interested by TALISMAN as this constitutes their future business.
- **Producers** consider themselves as responsible of the images protection, and are, therefore very interested by any kind of method to fight against piracy. They insist on the fact that it is very important to find the pirates as well as the forged works - without this possibility, the only protection of the identification is not efficient.

More generally, professionals facing with the arrival of the digital field, even though not always discerning easily the extent of the problems involved, obviously declare an interest to protect materialistically images,

principally the ones going to circulate over the networks. Authors' societies are the most concerned and revealed as the most active on the topic: advances and proposals in identification, major steps towards standardization.

### **3.3 Further steps towards end users' requirements**

Copyright protection of digital images involves much more sophisticated mechanisms than the ones required for analog ones: in the latter, insertion of a visible copyright can be sufficient even not totally robust. The ease to erase and modify a protection in a digital environment involves much more secure techniques such as invisible watermarking. The question then is to determine whether anyone can be able to generate a watermark or whether this could only be provided by an authorized institution. TALISMAN relies upon three major protection concepts: labeling (contents authentication), watermarking (holographically inlayed copyright) and monitoring (of the labels during broadcasting). Specific details about these concepts can be found in [2].

In order to complete the professionals' position, TALISMAN has performed a step forward towards generic requirements for protection. TALISMAN approach is a top down one, basically relying upon the end users' expectations. Requirements expected from a copyright system by potential end users can be synthesized as follows:

1. The label should protect the works Image Identification Number (called IIN, hereafter).
2. The labeling and the watermarking should provide different levels of protection in order to answer to every different professionals' needs and the investment they are able to give over.
3. The monitoring should be able to:
  - find the forged works
  - identify the pirates
  - count the diffusion (facilities of management)
  - provide adaptable functions according to the different professional categories (any kind of professionals should be able to manage its own monitoring)
  - provide a checking on-line
4. It should be possible to integrate labeling and watermarking functions into digital movie-cameras.

This synthetic definition can be derived into technical impacts over implementation:

- Label should protect the IIN means that the label should be undeletable and so linked with the watermark encoding the IIN. The unerasability means that protection mechanisms should rely upon security mechanisms involving keys management. Therefore, the question arising is should keys be managed by a centralized authority (unique Certification Authority), collaborative policy between Certification Authorities or should protection be totally independent from any Authority? This issue is fully discussed in section related to Common Functional Model.
- In order to provide different levels of protections compliant with different investments capabilities, the model should be generic enough to be evolutive and enable to host low end up to high end solutions. Also, the different professionals needs can vary in their expression: protection of the whole video (envisaged for large video), compliance of the protection with small changes (contrast, composite videos) for archived sequences for instance.
- Ability to detect the pirates means ability to later enable further compliance with fingerprinting. Capability by professionals to manage their own production means a non centralized way of protecting works (possibly relaxed in a collaborative protection based upon distributed databases). Checking on line impacts greatly the algorithms complexity at least if economical constraints want to be reasonably expected.
- Finally, the ability to further embed the copyright mechanism inside a camera can derive into a new approach. All approaches proposed until now (including Authors' Societies forecast) rely upon the fact that the Author must realize his work before protecting it, thanks to its attachment to an

Author Society recording the fact that the work exists and is the Author's property. This is an "a posteriori" protection and recognition. One of the major problems involved with this approach is the non protection of the work during its creation, transformation, transport and storage. Secure technology opens the possibility of a new approach (called "a priori") stating that the ideal solution should be the one allowing protection of the work during its creation. This new approach and resulting model is developed at the end of the paper.

## 4. State-of-the-art Models

Definition of the major actors in a multimedia chain, qualification of their interrelations and their derivation to a suitable semi-formal model, technically viable, is a major component of a copyright system. This is called **Common Functional Model** which should identify on a rather abstract level the major components of the system, the different flows between the components and their consequence in terms of technologies.

Such a work has been undertaken in a number of projects but having major objectives somewhat different from TALISMAN: CITED which is a horizontal action has identified the major protagonists but did not derive any implementation, COPICAT based upon CITED model targeting the educational area and ACCOPI covering both access control and protection problems.

### CITED

The objective of the ESPRIT II project CITED (Copyright in Transmitted Electronic Data) [3,4] was to investigate whether a solution could be found to new copyright problems that were arising by using technical means to control the copying of copyrighted information stored in digital form. CITED has examined the copyright-related requirements for transferring electronic materials through networks and has developed a generic model for controlling and charging the use of copyright protected materials. This model has been defined through a set of classes of functional components which monitor use operations, make decisions about the acceptance or denial of the use operation requested by the user, de- and encrypt information being transferred, generate usage reports and invoice, etc.

CITED architecture relies upon two basic blocks:

- the CITED protected information sub-system, or application, including the information product itself (e.g. a database), or a set of information (sub-)products and the computer program permitting to access it to perform the requested usage operations (e.g. an information storage and retrieval software,
- the CITED copyright management, usage monitoring and access protection sub-system, that continuously:
  - monitors the exchanges of information between the actors and the information product, from the start to the end of all operation sessions,
  - authorizes the performance of usage operations by the actors who have the use rights to do it and who have the necessary use right credits,
  - registers the actually performed usage operations in order to deny the authorization when the actor has no more necessary use right credits or has passed a use right charges threshold.

This requires the intervention of following classes of components:

- a monitor(MON), whose role application and CITED sub-system protection against external attacks, and possibly, to trap all basic events appearing at the level of its interface with the application, and to communicate those events to the Event Capture Tool,
- an Event Capture Tool (ECT), in charge of trapping all basic events, filtering these basic events and assembling them into CITED complex events, transmitting these CITED complex events to the CSA.
- a clearing service agent (CSA), whose role is taking decisions about the acceptance or denial of the usage or production operations requested by the actors, transmitting the actually performed operations to the URC and the notarisator (NOT),

- a use right collector (URC), whose role is storing data necessary for the CSA in order to take the relevant decisions and storing actors and information operation historic.
- a notarisator (NOT), whose role is to store relevant historic and accounting data issued by the CSA and the attack data issued by the Monitor, to issue these data, on the request of the use right manager,
- and, possibly, a marker, whose role is to mark the information product and have an electronic signature added to the encryption of the information.

CITED does not specify the actual implementation of the proposed model. In practice, there exist many problems in implementing and applying this model. First, it has been defined as a generic model so that technical mechanisms and application-related architecture are necessary to be developed before implementing the CITED model. Moreover, the basic concept developed in the CITED model, which is to keep track of the use and copying of digital material, are arising technical and/or judicial problems. Another difficulty in implementing the CITED model is that its enforcement requires a global agreement and acceptance of this model, and may require revision of copyright laws. This may hinder the realization and practice of the CITED model in a short term because it needs a long time to meet these prerequisites.

## **COPICAT**

The ESPRIT project 8195 COPICAT (Copyright Ownership Protection in Computer Assisted Training) [5] aims to meet the challenge of copyright protection for electronic data used in distance learning packages, which is a scope somehow different from TALISMAN. It is concerned with the development of both a copyright protection mechanism for electronically published material and a copyright management system.

COPICAT builds on CITED through the construction of mechanisms which serve to protect copyright material against a range of potential misuse. In particular, the problem-owners have targeted a series of scenarios and related risks corresponding to the delivery of educational material to the potentially very large customer base represented by corporate and private Internet users.

Absolute protection is not achievable: what is required is to make user misbehavior not worthwhile. As with photocopying a book, it should be less rewarding to behave illegitimately than legitimately

- Material of different value should have different degrees of protection
- The basis for protection of material should be maximally under the control of its rights holders
- A multiplicity of delivery strategies should be supported, transparently to applications
- A legitimate user may also be a misuser: protection against misbehavior is relevant at the point of access, as well as during delivery

Solution-space models have been developed to address all of these points (including the last and most difficult). A functional demonstrator for COPICAT will be available mid-1995 and the full COPICAT system will be demonstrated on a pilot site (University College Dublin) in mid-1996 to use multimedia material from the educational domain for testing, marking the end of the project.

COPICAT is in a good position to implement the CITED generic model. Whilst the project treats the educational domain as its prime development target, the project is nevertheless a "horizontal" action, seeking solutions which can be applied in a broad range of application domains.

## **ACCOPI**

ACCOPI aims to design a model allowing the copyright protection (CP) management in the framework of broadcast digital services. ACCOPI is also involved in the conditional access (CA) issue. Its CFM includes CP and CA functions to achieve an open, equitable and interoperable system. The most relevant functions are:

- a Trusted Third Party, whose role is similar to the CITED CSA and the NOT,
- a Watermarker, whose role is similar to the CITED MAR,
- an agent, whose role is similar to the CITED MON and URC.

The ACCOPI solution can be considered as a sub-set of the CITED one. It does not provide the same level of security but the parameters which have to be taken into account for broadcasting tools are also different. The ease to manage is much more important. Nevertheless, compatibility between ACCOPI and CITED can be guaranteed. Because of all these characteristics (other models compatibility, focus towards multimedia system,

de facto link with access control features, ease of management), ACCOPI is revealed as being one of the best candidate for TALISMAN.

## 5. Analysis of candidate protection models for TALISMAN

The following presents current TALISMAN analysis for possible Common Functional Models (CFM). The objective of the CFM is to identify on a rather abstract level the major functionalities of a Copyright Model highlighting the major issues involved in the specification. This section is not supposed to cover technical solutions such as labeling or watermarking fully investigated in [2]. This first starts with the identification of the actors in the digital video world followed by the roadmap to get a work protected, thus defining the interactions between these actors.

Two approaches can be envisaged:

- one which is called an '*a posteriori scenario*' relying upon the fact that the author only protects his work after the production, thanks to the author's attachment to an Author Society. This approach is derived from the RACE ACCOPI project one completed with a discussion around the ability to add a Copyright Authority enabling a better protection. This approach is quite conservative compared with the second one as it keeps existing rules and interests.
- the second one is more innovative and based upon an '*a priori scenario*' allowing protection of a work during its creation.

### 5.1 *A posteriori scenario*

The following describes the basic functions necessary to establish the flow of information from the creator to the consumer.

#### Basic multimedia chain functions

- The function of **copyright owner (CO)** is played by creative people involved in the construction of services. It is the most upstream job in the multimedia chain and consists in its artistic (can also be scientific or sociologic) contribution (e.g. photograph, actor, programmer, singer, journalist). Generally he has contracts with a service producer, possibly via an agent. He holds the rights and wants his rights to be protected.
- The function of **service producer (SPd)** is played by an assembler of media objects, it is indeed the content provider. Most of the time he is the first maker of multimedia services able to charm non professional users (e.g. a TV station, a radio station, a database owner, a film producer). He is responsible for the media he makes. That role could be also played by a pirate who broadcasts illegal copies.
- The function of **service provider (SPv)** consists in the multiplexing of several services into what we call a *bouquet*. In its simplest version, a bouquet can be a single service. Bouquets can be very attractive and can act as an added value to the services. So, the SPv is an integrator of services (e.g. a TV station, a cable operator, a satellite operator, a national PTT).
- The function of **carrier (Cr)** or network provider deals with the network management and consists in fulfilling the infrastructure capacity with bouquets and to assure the feeding in services to the subscribers. We assume that a Cr does not look inside a service or a bouquet and does not change any thing inside the bitstream he has to transmit and should not be implied in copyright protection (e.g. a TV station, a cable operator, a satellite operator, a national PTT).
- The function of **user (U)** is played by common people interested in watching TV or accessing databases or any kind of services. He receives these services by a connection to the cable, the switched network or through a satellite channel. He accesses the services through his terminal and the entitlements contained in his ACU. He wants these services to be secure and he can be

interested in authentication of the pictures he buys. This role could be played by a pirate who makes illegal copies.

The five functions described here form what is called *the basic multimedia chain*. The copyright protection features are not included; this requires the definition of additional functions.

## Copyright protection necessities

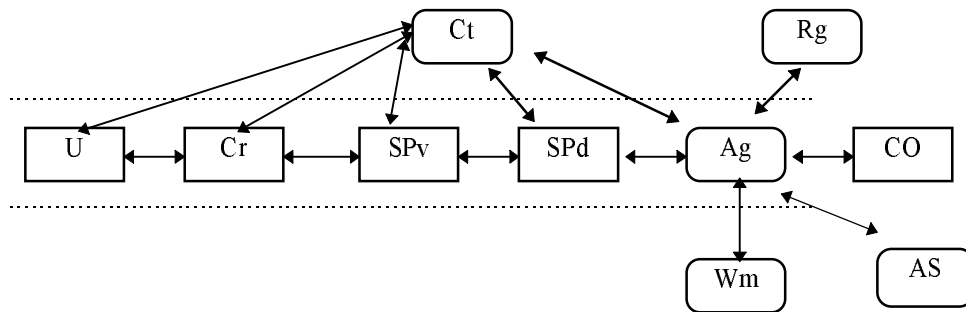
- The **Agent (Ag)** manages the copyright owner's business. He has a contract with one (or several) copyright owners which allows him to act in his name. Thus, he is the central function in the copyright protection part. He will enter into contracts with all the other functions involved in copyright protection; he is the key stone of the copyright protection. A Copyright Owner could be his own agent.
- The **Watermarker (Wm)** encrusts in each image the copyright information, according to the watermarking algorithm that has been chosen by the copyright owner or his agent. He performs both labels and watermarks. In particular applications he could be omitted if the label and watermarks are directly made at the realization of the pictures (e.g. in the camera). The Watermarker has only contracts with those agents he works for.
- The **Registrar (Rg)** manages a database containing information about image marks, owners and beneficiaries. He is responsible for the registration of all sold images. It could be a legal trusted part and could be referred to in case of conflict.
- **Authors Societies(AS)** are collective associations defending the Copyright Owner's rights. They attribute a unique identification number (IIN) to each new video work.
- The **Controller (Ct)** keeps the tools which are used to detect the labels and the watermarks. He is able to retrieve the signature and the watermark from each image and has control over the broadcast images at any time in order to detect possible misuse. He records all the fraudulent uses of his agent's pictures and tries to find their origin.
- The **Pirate (Pir)** makes illegal copies of images he receives and distributes them, sometimes pretending to be the author (possibly after editing the image in order to hide its origin).
- The **Trusted Third Party (TTP)** is not for the moment involved in the basic Common Functional Model, but it could become an important part of the CFM. Its role is generally to bring a certification for the cryptographic keys and to guarantee their validity. It is a fair authority serving as a intermediary in the key exchanges.

## Interaction between the functions

1. A Copyright Owner (CO) performs a work
2. The Copyright Owner enters into a contract with an Agent (Ag)
3. The Copyright Owner or his Agent contacts an Authors' Society (AS) and asks for a IIN (Unique Identification Number)
4. The Agent makes the work labeled and watermarked by a Watermarker (Wm - subcontractor specialized in the technology)
5. The Agent gives copyright protection information to a Registrar (Rg - database containing information about picture ownership and beneficiaries)
6. The Agent enters into a contract with a Controller (Ct - subcontractor specialized in monitoring) and provides him with the information necessary to illegal copies detection
7. The Controller surveys the network, provides accounting detects the frauds and records them
8. The Controller contacts the Agent and warns him of frauds concerning Copyright Owner he has contract with
9. The Agent contacts the Copyright Owner and activates juridical action

## Description of a possible basic Model and protocol

Figure 1 represents the different functions (actors) together with their interactions. This defines the so-called 'basic model' i.e. the minimal steps for a protection.



**Figure 1: A basic Common Functional Model**

Steps of the procedure are deeply analyzed and justified one by one.

1. As mentioned above, the Copyright Owner is the creative person or society at the origin of the video, so he has IPR for his work and he wants them to be respected. For example he does not want his pictures to be modified (the integrity has to be guaranteed). He does not either admit that copies of his images circulate without his authorization. Moreover he desires to collect rights proportionally to the number of broadcast or sold pictures. Of course the role of Copyright Owner can be played by a pirate who copies a picture and then pretends to be the author. That impostor can even ask an identification number for the copy after the Copyright Owner. Two same images (the original and the copy) can have their own IIN. In that case he will probably try to collect rights like any Copyright Owner.
2. The Agent is the keystone of the copyright protection, he enters into contracts with as many controllers he considers necessary (different countries, different networks..). The Copyright Owner can be his own Agent of course. He also contacts the Registrar.
3. The IIN will be granted by an Authors' Society to every new work without control ( as mentioned above it can be a illegal copy) it is only a sort of pointer to a database, it references the picture but does not give any right.
4. The Watermarker performs both labels and watermarks for the Copyright Owner. The watermark indicates undoubtedly the ownership of the picture. The role of the label is quite different, it first guarantees the authentication for the user. Nobody has interest to put a non authentic label next to the content, the user's device could refuse to read it, the user could refuse not buy the picture for example. The label contains a signature for the authentication, but also the name of the picture beneficiary who will collect the rights. This one is of course responsible for the content; if it is an illegal copy an action will be brought against him. The name of the Copyright Owner has of course to be put into the label but it will probably not be enough. In fact there are several cases where the name of the Service Provider (SPv) will have to be known. For example TV stations often postprocesses the pictures they have bought and mixes them. The result can sometimes be considered like a new product and may even receive a IIN. In this case, the Service Producer (SPd) will be responsible for the end product that's why he has also to sign the label with his private key. Each time a new postprocessing occurs, a new signature has to be provided. There will be a sort of hierarchical signing of the picture (an onion-like signature). If the picture in question is an illegal copy, the last person who signed will be held responsible but can refer to the one who gave him the picture (who signed before him). The difficulty will then to know who will collect the rights. Concerning private and public keys, it could be interesting to have a Copyright Authority certifying of the validity of the keys. So if contents provider is indeed a pirate, he will have to use his own key and will act in his own name. Concerning the watermarking, this onion-like structure is more difficult because some watermarking algorithms do not withstand the overwatermarking.
5. The Agent gives the copyright information (IIN, private key for label, secret key for watermark, name of the beneficiaries) to the Registrar. The date of deposit can be very useful in case of conflict (it should be a legal

entity). The Registrar has only a passive role of registration in the copyright protection. All sales have to be signaled to the Registrar.

6. When the Agent enters into a contract with a controller, he gives him all the information, public key for label, secret key for watermark, name of beneficiaries. The Controller has to be honest (he has the watermarking key, so he can remove it..) otherwise he will lose all his contracts. An Agent can pay several controllers if necessary, each Controller controls his part of the network. The Agent has the responsibility of the choice of the Controller.
7. One Controller surveys all the pictures he is able to, on broadcast networks, point-to-point communications if possible, CD-ROM... For each picture, he checks first the watermark. If the watermark is one of his customers, he then checks the label. He compares the label owners (who will collect the rights) with the beneficiaries in his list while recording the video. If the label owners do not correspond to the beneficiaries of his list, there is a problem and possibly a fraud.
8. If a conflict occurs, the Controller after recording the presumed fraud, he warns the Agent and gives him all information useful to bring an action against the presumed infringer (date of the record, name of the copy owner, record of the illegal broadcast video...).
9. In case of conflict, the Agent tries to contact the presumed infringer and question him about the picture in question. If no agreement is found, he still can refer to the justice. In order to defend his Copyright Owner's interests, he needs the Registrar as a witness of his legal deposit and he needs the recording of the illegal broadcast. In front of the judge, he will be able to prove he has watermarked the picture and he is able to prove when he did it (date of the deposit)

## Cases of conflicts analysis

### I. Label authentic:

- A. *label unchanged*: the pirate just made an unauthorized copy, and changed nothing neither in the content nor in the label. It is very easy for the Controller to detect the fraud, but it is more difficult to locate the origin if the Controller does not know the sender. This case will probably occur for CD-ROM or digital video cassettes.
- B. *label oversigned*: the pirate made an unauthorized copy and did not change the content but appended his signature after the first signature (onion-like structure). It is easy for the Controller to detect the fraud that occurs if the oversigner is not a beneficiary. This case will happen when a Service Provider will mix different images among which some are illegal copies. This Service Provider will be held responsible for the infringe. He will have to defend himself if the illegal copy was sold to him by a pirate.
- C. *label removed*:
  1. no label: the pirate made an illegal copy, removed the label and broadcast the picture without label, possibly free of charge. This case can occur if some malevolent person wants to harm a rival Copyright Owner for example. It can also happen in CD-ROM or digital video cassettes. It is very easy for the Controller to detect the fraud, but it is more difficult to locate the origin if the Controller does not know the sender.
  2. label replaced: the pirate is an impostor, he pretends to be the author of the picture. The Controller has only to compare the name of the label owner who will be held responsible for the fraud and he will have to defend himself.

### II. label non authentic:

- A. content changed: the label allows to determine whether a content has been modified; This case should not occur, a pirate has no interest to do that because once the content has been changed the label is no more authentic so it is obvious that the work of initial author has been distorted.
- B. signature changed: the label is no more authentic, so the Copyright Owner will not collect his rights anymore. This case will occur when a malevolent person wants to harm a Copyright Owner.

- III. overwatermarking: the pirate pretends to be the real author and probably he desires to collect rights in the place of the real Copyright Owner. The Controller has to check the label in order to find the origin of the fraud. Normally, the pirate wants to collect rights so he has put his name in the label. In this

case the Registrar will be very important because of the date of the deposit. In any case the real owner is the only person possessing the original.

## **Key management**

The keys used in the cryptographic algorithms have to be known by the right person at the right time.

### **1) label:**

- There is a private key only known by the Copyright Owner and the Agent (and the Watermarker during the marking).
- There is a public key necessary for the Controller and for the user. Either we put the public keys into the label but the label risks to become very long if there are a few signings, or we only put the name of the private key owner and the user will have to refer to an electronic directory containing public keys. The last option can reveal heavy if there are many keys in the directory. In both case the validation of the keys should be done by a Copyright Authority.

### **2) watermark:**

- There is a secret key known by the Copyright Owner, the Controller, the Agent and the Registrar (and the Watermarker during the marking).

## **Problems involved by the model**

- According to the procedure, there is no control a priori, i.e. before the broadcast of the picture. So, that picture can even be an illegal copy. There is only a control a posteriori once the picture is already on the network. It is obvious that all the frauds will not be detected but only a small percentage of them. What is more a pirate can collect rights at the place of the real Copyright Owner because there will be no control at the attribution of the IIN. This could be balanced by expensive fines for proved frauds.
- The concept of watermarking is based on secret key cryptography. Once someone has discovered the CO's key he can remove all this Copyright Owner's watermarks. The only solution is to change the key when it is discovered and to possess several keys. Nevertheless when one key is discovered, the pictures watermarked with the use of this key are no more protected towards the one who discovered the key.
- Eventually, in front of a judge the only thing the CO is able to prove is that he watermarked the picture but not that he is the real owner. This can be a juridical problem difficult to solve.

## **Alternative model including a Certification Authority**

In order to re-enforce the protection (i.e. avoid any pirate copy already watermarked to be brought to an agent to be marked again, a Trusted Third Party called 'Copyright Authority' which only delivers the agreement to watermark a work if this is authorized. Notice that this Trusted Third Party can be unique or distributed (see the end users' analysis to this aim). This leads to an alternative model called '*a certification model*' compared with the previous '*basic model*'.

In a certification model, a certification has been added by means of a Certifying Authority realizing the labeling and the watermarking for all of the Copyright Owners after having checked if the picture has not been watermarked before. That system is only effective on a certification network in which all the pictures should be certified by the Copyright Authority.

## Comparisons of the models

### Synthesis

<i>Advantages of the basic model</i>	<i>Advantages of the certification model</i>
can easily be effective in a short time	difficult to attack
do not concentrate the control into one or few authorities	broadcasting of illegal copies almost impossible on the certification network
	the user can be confident in the information he receives
	cases of conflicts are more limited

<i>Drawbacks of the basic model</i>	<i>Drawbacks of the certification model</i>
less secured	heavy management
no control at the origin of the chain but only once the picture circulates on the network	difficulty to impose the certification model as a standard
there is a fear that a pirate could collect rights for a pictures he does not holds the copyrights	
the only proof that can be done is that the image has been watermarked	certification disappears when the picture is broadcast on a non certification network
there is probabilistic rate of copies detected	

### Discussion

The realization of the functions of the basic model can be done very quickly, at the opposite of the certification model which requires more new functions and far more functionalities. The function of certifying authority would be difficult to implement due to the heavy management it has to cope with.

Moreover, the certification network has no reason to exist if it is not widely accepted. It is easy for a pirate to diffuse his illegal copies on a non certification network, so if the certification networks are not widely accepted, a content provider will not take trouble to enter into the heavy procedure of the certification.

However, with the basic model some problems can arise:

- ⇒ First the network is less secure so a certain number of illegal copies will be distributed before the fraud is detected.
- ⇒ Secondly, there is no control at the moment the watermarking of the pictures, so a pirate can watermark a picture and pretend it is his while the real Copyright Owner's controller has not detected a fraud, he can thus collect the rights at the place of the real Copyright Owner.
- ⇒ Thirdly, in front of a judge, the only thing you can prove is that you have watermarked the picture not that you are the real owner. This can be a juridical problem difficult to solve.

### 5.2 A priori scenario

TALISMAN must analyze every possible new concept and original solutions and models satisfying information and multimedia society future requirements, even though existing rules or vested interests should be modified. This approach, as opposed to the previous more conservative one, is an original solution based on a new approach for Copyright itself.

Mechanisms proposed until now are based on the fact that the Author (Originator) should realize his work before protecting it, thanks to an Author Society attachment. One of the problems with this concept is the heaviness of the protection process and the non protection of the works during its creation, transformation, transport, storage.

By the meanwhile, secure existing technology allows to build a new approach and find solutions better suited to new creation technique appearing with multimedia society, based on the concept that work can be protected during its creation.

Constraints deriving are:

1. An Author must have at his disposal anywhere in the field of creation some elements related with legal elements (rights) enabling his work protection on the go.
2. The first constraints automatically sets up other ones. In order to satisfy the first constraint, a state-of-the-art technology module (Security Smart Card) dealing with related legal elements should be used. Related legal elements should be distributed to the Authors before work creation.

This is the basis of an 'a priori' scenario leading to the definition of new types of transaction satisfying the two first constraints.

## **Basic Steps**

### **Creation Steps**

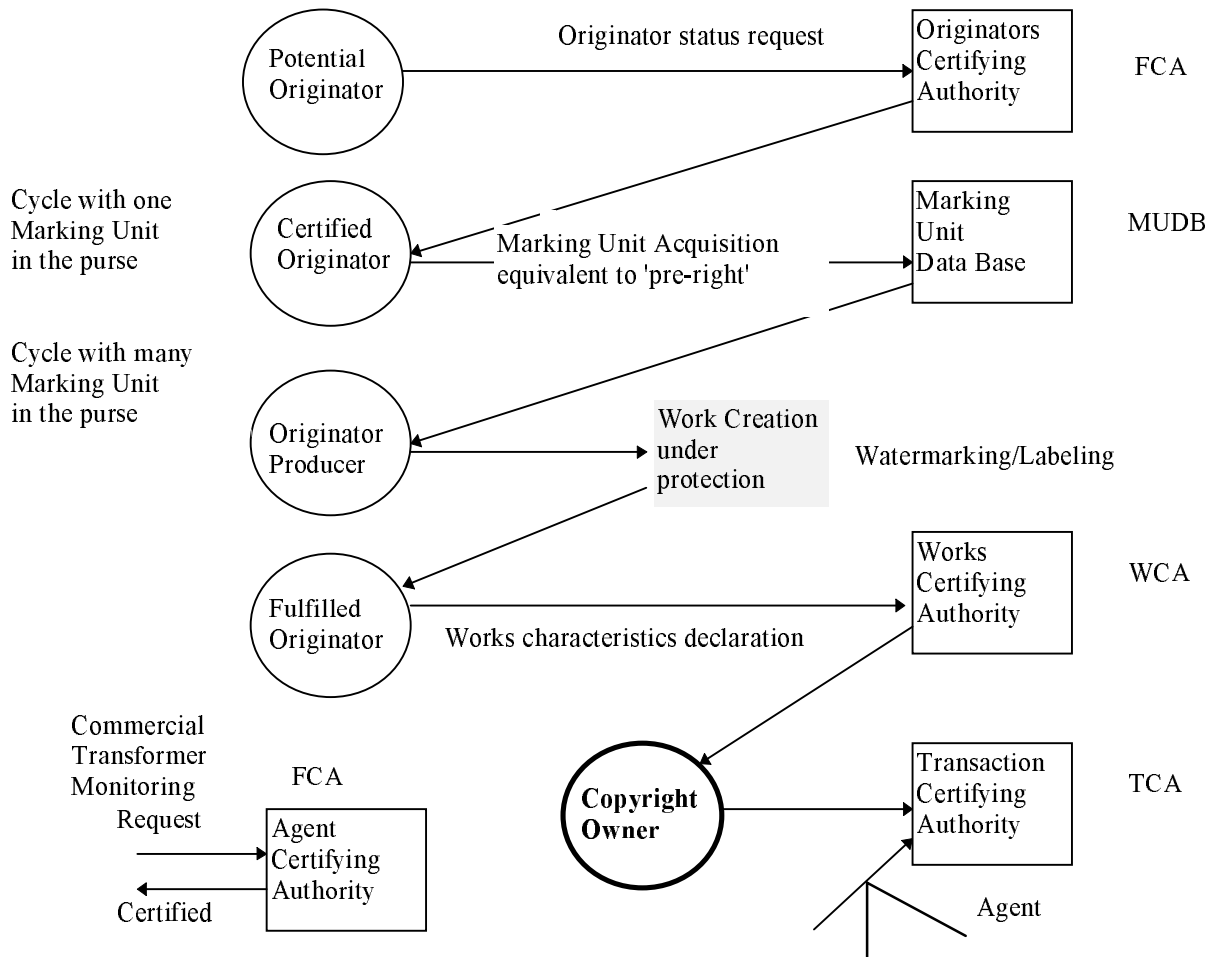
This concept introduces new roles and new functions. If one analyzes chronologically the process of creation starting from scratch, five steps can be identified.

1. Emergence of the idea of the work
2. Acquisition of a Marking Unit (one Marking Unit for one work = Extended IIN)
3. Creation (or production) of the work under protection (watermarking) with the dedicated Marking Unit
4. Declaration (description) of the work and registration to a registry office. The work description is linked to the Marking Unit
5. Business (sale, rent ... of the work).

### **The Author or Originator**

It follows that the Originator's work can be defined very precisely in five chronological steps of the creation process as described in Figure 2.

1. The potential Originator: people who have an idea, nothing else (anybody can be a potential originator);
2. Certified Originator: People asking to be recognized as an Originator (even if he never created anything) by a Functions Certifying Authority (FCA). The FCA (may be a TTP) supplies an electronic identity card (Smart Card SC) containing all the identity parameters of the Originator and an empty zone to store the Marking Unit.



**Figure 2: Exploded CFM based on 'a priori' scenario**

3. **Originator Producer/Creator:** Makes the acquisition (one or several) of the Marking Unit stored inside his Originator identity card (SC). This Smart Card is like a personalized purse of a Marking Unit (Smart Card = Copyright Purse); SC = Cpurse.
4. **Fulfilled Originator:** Originator who created a peace of work and used a Marking Unit to watermark his work. The CPurse memorizes the fact that one MU was used.
5. **Copyright Owner:** Fulfilled Originator declaring the description of his work to a Works Certifying Authority (WCA). The work is now certified and officially protected.

If we consider that for the future all electronic picture equipment (video camera professional or otherwise, photo camera, computer, video recorder) should be equipped with a Smart Card Reader (easy and at a low cost), the use of the MU for each work will be an easy and secure way to watermark work. The only problem will be the high cost of watermarking chips at the beginning.

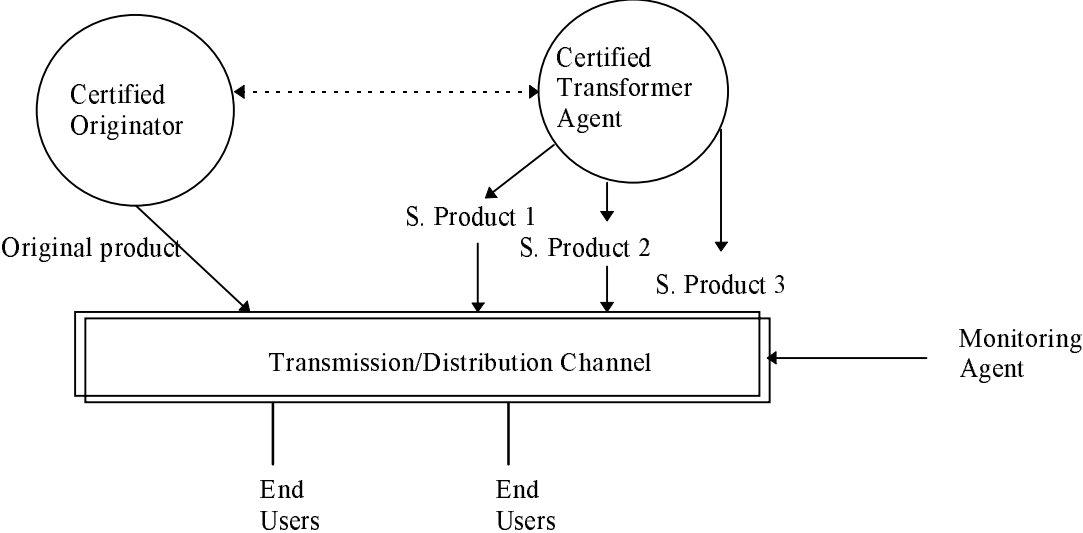
Nevertheless, this model gives flexibility and security to originators. As an example, an ENG (Electronic News Gathering) cameraman should be in the field with a purse with many MU and should use a new MU for each new video subject without acquisition of new MU, travel to find MU etc. The same scheme can apply for an Originator working on a graphic computer.

### **Agent: Commercial - Transformer - Monitoring**

When a work has been completed, it can be sold, rented or modified in different sub-products (work transformation). To do that, the Copyright Owner will contract with one or many specialized Agents.

In this model, we consider that all types of Agents should be certified by an FCA (Functions Certifying Authority). The FCA (may be a TTP) supplies an electronic identity card (Smart Card SC = CPurse) containing

all the identity parameters of the specialized Agent. This approach enables the setting up of a new powerful and secure way of working (ex: Transaction contract over computer networks). Figure 3 exploded CFM shows the example of a Transformer Agent creating sub-products from the original product with a second level of watermarking and copyright on the transformation. In this case, this agent uses a Cpurse with a Marking Unit like the originator.



**Figure 3: Transformer Agent creating sub-products**

In the same way, the Copyright Owner can contract with a specialized agent for Monitoring. Due to the security of the Cpurse, the parameters and the keys enabling monitoring can be given (in a secure way) to this agent. As for the Transformer agent, the contract and parameters can be transferred over a computer network.

**Description of the transactional flow (protocol)**

The starting point of the model is the fact that the Originator has an idea but is not recognized as an Originator. The first step will be the "official" request for the status of an Originator. Anybody can do this whether or not they have an idea. The Originator requests this status from an FCA (Functions Certifying Authority - this is better for the explanation of the model to define the general concept without considering existing Authorities such as Authors Societies) registering the Originators' identity and the required function (Originator, in this case), see Figure 4. In the case of an Agent, more information will be needed to deliver the status and the corresponding CPurse due to the fact that these functions are more sensitive and critical in the business.

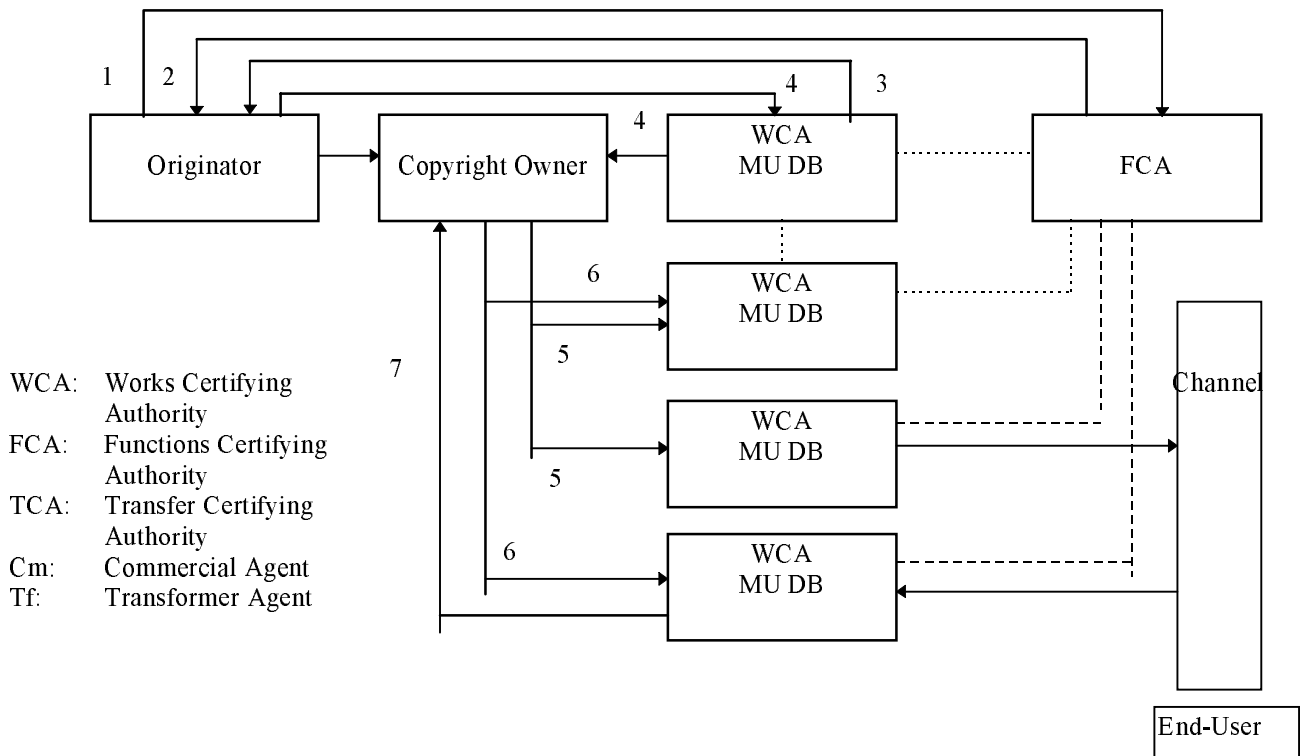
The FCA records the identity in its database and in a CPurse Secure Smart Card). This identity is linked to an Originator Number (representing the Country, date of registration, DB identification, registration number, access code, etc.) in the database. This identity SC is now like an empty personalized Cpurse.

Next step is the acquisition of Marking Units for the Copyright Purse. To fill this, the Author goes to the Marking Unit DataBase terminal, or company and fills the purse with 1,2, 5, 10 or more MU and associated Keys. For each MU, the database takes a pair of mathematically associated keys, Ks (secret, private) and Kp (public) and stores Ks in the Cpurse alongside with MU. We can later consider the fact that the FCA should also fill the Cpurse with the MU.

The format of each MU stored in the purse can be as follows:

Date	Country	Unique Number dedicated to 1 work	Reserve	Signature on F1.F2.F3.F4
Field1	F2	F3 = IIN	F4	F5

This MU DataBase must be unique (or distributed but connected) to a country in order to ensure that each MU is unique.



**Figure 4: A priori Common Functional Model**

The Originator is now ready to start the creation of the work safely. For cameramen, the camera is equipped with a watermarking module and an SC reader.

The Copyright purse is fitted in the reader. The camera asks the Originator (via the display) for the key code to use the first MU. This is downloaded into the watermarking module requiring three kinds of information: MU, Ks, Krn. Krn is a Random key number issued by the CPurse itself. The Random Key is recorded alongside with the used MU and its Ks inside the SC.

Downloading inside the WM is made with a secure protocol. The watermarking module (WM) will memorize the MU, Ks, Krn in a secure memory and will change it only if a new key code is entered and a new MU, Ks, Krn downloaded.

A handshake protocol between the watermarking module and the CPurse indicates to the Cpurse that WM has received the MU (integrity of the MU was checked by the WM). The Cpurse records the acknowledgment from the WM for this MU containing the serial number of the WM (as an example). The camera is ready to work under protection.

When the work is completed, the Originator takes the Cpurse to the WCA (Work Certifying Authority) for official registration of his work. The computer of the WCA receives from the Cpurse the identity of the Originator, the MU used, the associated Random key number and the WM acknowledgment. These information are stored in the Originator's database. The WCA database informs the MU database that Mu x, y, z etc. Have been used and checks the correlation between the identity and the MU in the MU database; this is compared with the information received from the SC.

The Originator provide a work description (characteristics) and the work is now officially registered and protected by a watermarking Copyright. The Originator can now sell the work and the associated Right.

### **A priori model evaluation**

For practical implementation of this CFM, mechanisms used allow a very flexible implementation based around one or several databases (TTPs) whether linked or not. All Certifying Authorities and databases can be centralized in one Authority with a lot of SC terminals installed around the country (Bank card terminals could

be imagined to be even used in the future). The approach is flexible and could be extended to non professional market of picture and, possibly, to some other matter than picture. Extension of this model towards monitoring still needs to be deeper investigated. Also, compliance of the model with nowadays institutions and legal ways of protection is to be analyzed.

## Conclusion

The paper presented two major approaches for a Common Functional Model for Copyright: one called an '*a posteriori scenario*' relying upon the fact that the author only protects his work after the production, thanks to the author's attachment to an Author Society. This approach derives from the RACE ACCOPI approach completed with a discussion around ability to add a Copyright Authority enabling a better protection. This approach is quite conservative compared with the second one as it keeps existing rules and interests. The second one is more innovative and based upon an '*a priori scenario*' allowing protection of a work during its creation. Both approaches can be justified and applied in the future multimedia context. Next stage consists into better assessing and analyzing their relative impact and relationship in the actual copyright context, which is the objective of future TALISMAN project.

## References

- [1] CIS (Common Information System) document. Plan proposed by the BIEM/CISAC Information Systems Steering Committee - December 1994.
- [2] ACCOPI RACE Project m1005, Workpackage 2, *Common Functional Model*, June 95
- [3] G. Van Slype. The CITED approach. ESPRIT II CITED Project 5469, April 20, 1994.
- [4] G. Van Slype. Natural language version of the generic CITED model. ESPRIT II CITED Project 5469, June 28, 1994.
- [5] Esprit Project 8195: Copyright Ownership Protection in Computer Assisted Training (COPICAT), Workpackage 2 (Requirements Analysis), Deliverable 1, June 2, 1994. *Conference on Intellectual Property Rights for Specialized Information, Knowledge and New Technologies*, Vienna, Austria, August 1995.
- [6] Macq B., Quisquater J.-J.. *Cryptology for Digital TV Broadcasting*. Proceedings of IEEE. June 1995. pp 944-957.