Paper presented at ECMAST'99 - European Conference on Multimedia Applications, Services and Techniques, Madrid, Spain, 26-28 May, 1999

Protecting Intellectual Proprietary Rights through Secure Interactive Contract Negotiation

Carlos Serrão, José Guimarães

ADETTI / ISCTE, Av. Forças Armadas
1600-082 LISBOA, PORTUGAL

{Carlos.Serrao, Jose.Guimaraes} @ adetti.iscte.pt

Abstract. Protection of Intellectual Proprietary Rights is currently one of the most important barriers to electronic commerce of digital contents over networks. Authors and content providers understand the immense advantages of the digital world but show some reserve. However, technologies and techniques to protect IPR in digital content exist, their deployment in a coherent way is still in an early stage. In this paper, we describe the approach followed by the OCTALIS Project towards and effective electronic commerce of digital images. After describing briefly enabling technologies, the emphasis is on contract negotiation over Internet through a secure dialog between the Service Provider and the User.

1. Introduction

The trade of digital content through networks is an area that is receiving strong investments in research and development.

The problem is complex because digital content is possible to copy without any quality loss, thus the associated Intellectual Property Rights (IPR) are easily violated through unauthorised reproductions.

Authors, copyright owners and content providers in general face a crucial dilemma: profit from the immense advantages of exposing their work through digital mediums, or adhere to other business models and have higher costs to reach wide audiences.

In fact digital networks, like the Internet, provide the means to reach world-wide audiences with costs that can be considered inexpensive when compared with other types of media. However, the difficulty to protect IPR in digital content, to enforce them and to verify the correct usage of the content, is preventing the faster deployment of the electronic commerce of digital contents.

Electronic Commerce of any type of goods can be considered broadly under two main aspects: marketing and contracting [1]. While the first focuses on promoting company products and services to customers, the second focuses on negotiation of the terms and conditions of the contract and the monitoring of contract performance. In this paper, we will focus on the second aspect.

The work that is described in this paper was developed in the framework of Project OCTALIS – Offer of Content through Trusted Access LinkS[1]. It implements the OCTALIS model, including on-line contract negotiation of the usage terms and conditions for electronic commerce of digital images.

2. Approach and objectives

Technology and tools for protecting digital content, such as conditional access systems, digital labels and watermarks already exist. Some are still incipient, but the main problem is that they are mostly used in an isolate way, without establishing a common framework for solving the real problem: the effective protection of the Intellectual Proprietary Rights - IPR [2].

The OCTALIS Project [11] addresses an open architecture for secure content negotiation, delivery and protection, trying to solve some problems raised by the IPR protection. One of the goals is to protect the access to valuable information through the establishment of a secure contract negotiation scheme. The project provides a framework that has been successfully tested for protecting the Intellectual Proprietary Rights for interactive database access and broadcast services [2]. In this paper we will only focus on the first architecture.

The OCTALIS project inherits results from other R&D European projects, in order to fulfil some of the needs identified by the consortium. This is the case of OKAPI[2], which provided the kernel for the conditional access system, and TALISMAN[3] with technologies for invisible watermarking and labeling of images.

The OKAPI Project developed a security kernel, which ensures interoperability, openness, equity and user privacy. It aims at an evolution towards an open multimedia market.

The purpose of the TALISMAN Project is to provide standard copyright mechanisms to protect digital images against large-scale commercial piracy and illegal copying. With this purpose, TALISMAN defined an evolutive and open framework based upon a group of entities requirements (author's societies, content providers and broadcasters) allowing the integration of a hierarchy of effective solutions for protecting video and still image contents [3]. Technologies that have been developed include *labeling*, which is directly associated with the bit stream and *invisible watermarking*, a sophisticated undetectable system.

Other sources concerning IPR protection where also consulted, and there was a special emphasis on the use of standards, such as those that address embedded content description for digital images.

[1] OCTALIS ACTS Project AC242 is partially financed by the European Commission - DGXIII.

[2] OKAPI - Open Kernel for Access to Protected Interoperable interactive services, ACTS Project (AC051), partially financed by the European Commission – DGXIII.

[3] TALISMAN - Tracing Authors rights by Labeling Image Services and Monitoring Access Network, ACTS Project (AC019).

3. OCTALIS Common Functional Model

In order to evaluate and test the reliability and robustness of the solution proposed by OCTALIS, two field experiments were set-up. One of these experiments focused on the primary distribution network for broadcast television, and the second one focused on the interactive access to high value professional image databases through Internet. In this paper we will concentrate on this last experiment.

The experiment implements the Common Functional Model (CFM) defined in an early stage of the project. The CFM, shown in Fig. 1, represents a multimedia chain and its actor's, together with a copyright and IPR protection mechanisms flow, from the content creator to the final user.

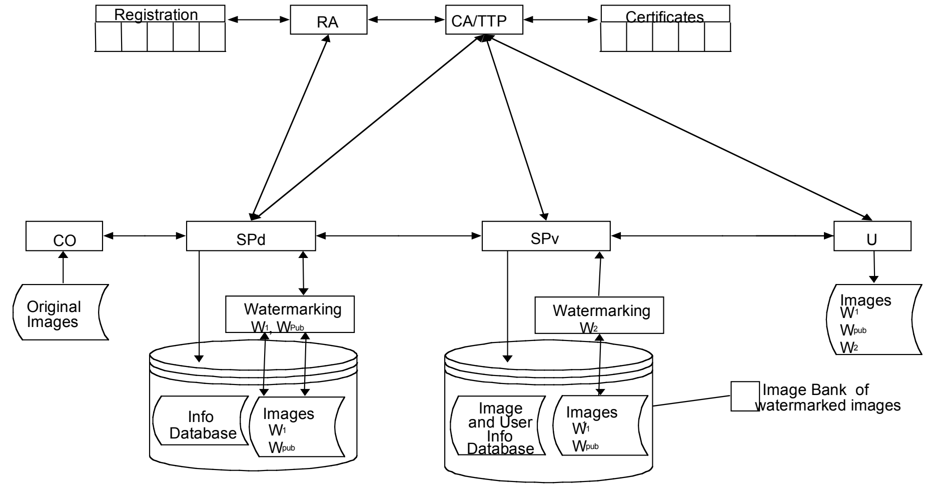


Fig. 1. OCTALIS Common Functional Model.

OCTALIS defined a set of different entities across the multimedia chain, establishing the necessary mechanisms for conditional access and copyright and IPR management [4]. These entities are shown in Fig. 1 and briefly described in Table 1.

It should be noted that the CA and the RA entities might not perform their main task on-line. In fact, it is even desirable to avoid security breaches.

Content flows in the CFM have implicit a set of procedures necessary to manage content itself and associated IPR. We will describe these procedures in the following sections.

Entity	Description
CO Copyright Owner	Represents the creative people contributing with content. For the purpose of the work described in this paper (digital images) they represent artists, like painters, ceramists, etc., as well as photographers, either as reproducers of the formers work or representing themselves with their own original works. We also include in this class an agent that may act a representative of artists in those aspects concerning IPR.
SPd Service Producer	Represents an entity that takes charge of preparing the artistic work to be made available in a digital format. Their task includes the interface with a RA (see below) for the purpose of image registration and the insertion of IPR information in the image by watermarking (see below). Each SPd has a database holding information about the images that were produced. This database is important for IPR tracking.
SPv Service Provider	These entities are responsible for the provisioning and distribution of images through networks. They also have a role in the IPR management flow, since they are responsible for the contract negotiations for each image, and by the insertion of another watermark (buyer’s fingerprint) in the image. They also manage a database important for the IPR aspects, as we will see later in this paper.
U User	Represents common people interested in buying a digital image through a network (Internet).
RA Registration Authority	It is a task of these entities to provide “notary” services for digital images registration. This entity is internationally accredited (see below). They receive the original image together with associated information, namely IPR information, and perform a registration by assigning it a universally unique identification number, according to the SPIFF specification [5]. As we will see later, this entity also manages a database important for the IPR flow.
CA Certification Authority	Entity that is responsible for issuing certificates to all the other players. These certificates will be necessary to the on-line transactions. The model does not preclude the existence of multiple CA entities due to the role of the TTPs (see section 3.1).
TTP Trusted Third Party	Trustworthy entity that manages conditional control. Contributes to the establishment of a Secure Authenticated Channel (SAC) between the User and the SPv.

Table 1. Actors in the Common Functional Model.

3.1. Entities certification

One of the basic pre-requisites normal in conditional access systems is the certification of the involved entities. Two entities are responsible for this functionality in the CFM: the CA and the TTP.

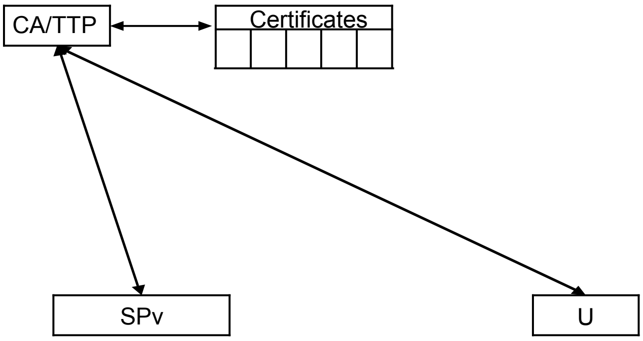


Fig. 2. Certification process.

The CA issues digital certificates for both the User and the TTP. It is normally available offline.

The TTP certificate is obtained from a CA and stored in the TTP database.

The User certificates are inserted into an Access Control Unit[4] (ACU), which, accordingly to the model, can be obtained by a person (the real user) in a store[5]. Public information corresponding to each ACU is forwarded off-line to all TTPs that hold a certificate issued by that CA. When acquiring an ACU, the real user receives a pin-code that will be necessary to initiate transactions.

This mechanism of distributed security allows a TTP to trust User's certificates obtained from diverse CAs.

The SPv certificates are obtained off-line from a TTP and stored in a database. A TTP has the possibility to register multiple SPvs and a SPv can be registered in multiple TTPs, ensuring a true interoperable solution and allowing the different TTP registered Users to be trustworthy at different SPvs and vice-versa.

[4] The ACU is a tamper resistant device fundamental to the OKAPI kernel (see section 4.4.), it is normally a smart-card however, since smart-card readers are not yet a standard peripheral on normal personal computers, an emulation based on a diskette and associated software was developed. Conceptually there are no differences between the smart card and the diskette based ACU, both are tamper resistant (the former by hardware, the later through content encryption) and protected by a pin-code.

[5] In the case of the emulation diskette, it can be obtained on-line through an interactive process at http://ra.adetti.iscte.pt.

3.2. Original images deployment

Images are delivered off-line to the SPd with the corresponding contractual terms for licensing and copyright and IPR information (see Fig. 3). Whenever it becomes necessary, it is assumed that the SPd is in possession of the technical means (e.g.: high-quality image scanner, software) to produce digital images from the original physical image and generate pertained information necessary for the SPv to accomplish an effective negotiation of contracts and licensing agreements.

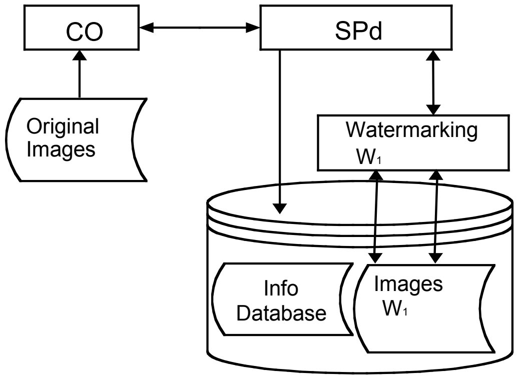


Fig. 3. Original image delivery process.

It is a task of the SPv to introduce a first approach to IPR management, by producing a digital image signature and embedding it in the image as an invisible watermarking. Relevant information for IPR purposes, namely the value that was watermarked in the image, is stored in the SPd database.

This process will allow at a later stage, if necessary, to enforce IPR in case the image is illegally reproduced.

Accordingly to the CFM notation, this watermark is designated as the first *private watermark* (W_1).

3.3. Images registration

An internationally accredited Registration Authority is responsible for performing image registration. This authority is defined in ISO/IEC 10918-4 as REGAUT and is in charge of producing and delivering unique identifiers, or *License Plates* (LP). The *License Plate*, together with other information about the image and its IPR, build sets of Directory Entries that constitute part of the SPIFF[6] format (see section 4.1).

[6] SPIFF (Still Picture Interchange File Format) is a standard approved by ITU-T and ISO/IEC to include metadata (data about data) information inside an image file. Annex F of document ITU-T T.84 | ISO/IEC IS 10918-3 "Digital Compression and Coding of Continuous-Tone Still Images" specifies the SPIFF format.

In the CFM, a SPd submits images to REGAUT, who issues an LP for each image. This LP is used by the SPd to embed a second *public watermark* in the submitted digital image (W_{pub}) thus identifying the entity that has the trusted repository of IPR information about the image.

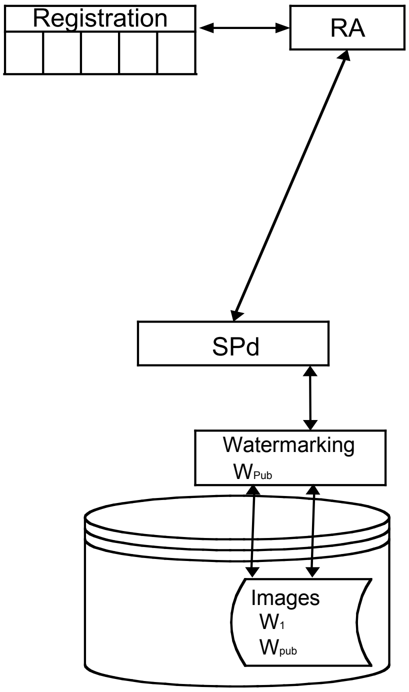


Fig. 4. Image registration processes.

As described before, the LP is world-wide unique for each image, therefore each image can be registered only once. This LP contains information about the REGAUT ISO country code, a unique JURA[7] identifying number and a sequential number for each of the registered images (e.g.: PT-98-1023).

3.4. Images provisioning

Once W_1 and W_{pub} watermarks have been introduced in the original image, the SPd produces several resolution levels for the same image. These levels constitute the pyramidal representation designated as JTIP (see sections 4.1. and 5).

It is the set of different resolutions, together with copyright and IPR information that is delivered off-line to a SPv.

[7] JURA - JPEG Utilities Registration Authority, http://jura.jpeg.org.

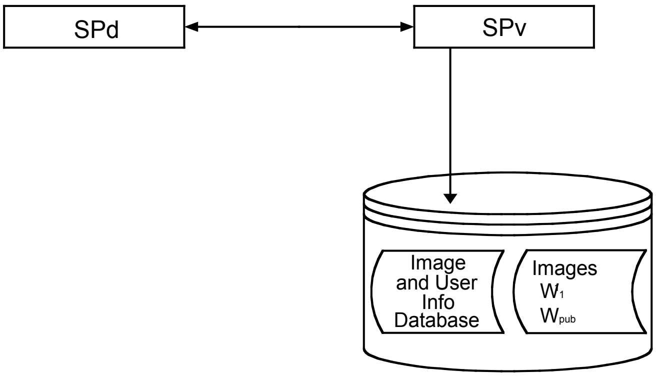


Fig. 5. Images provisioning process.

A database at the SPv location holds different levels of the images, resulting from JTIP, which include low-resolution reproductions adequate for web browsing. Images are displayed along with their copyright and technical information. For each available resolution, technical and copyright information is also showed.

The contractual terms for licensing are also stored, in order to allow the future on-line contract negotiation that is described in section 5.

3.5. Images acquisition

Images can be acquired on-line through Internet. The establishment of a Secure Authenticated Channel (SAC) between the User and the SPv is necessary for the secure download of images (see Fig. 6). The OKAPI kernel provides the necessary authentication and cryptographic features needed to fulfil the security requirements.

The ACU (see section 3.1) plays an important role by securely storing User secret information and certificates. Through this device the User can be authenticated to the OKAPI/OCTALIS system and therefore allowed to securely negotiate an image with the SPv.

This action and the subsequent image download are accomplished through a special application that calls the OKAPI security kernel through its API.

Before sending an image to a User a new invisible watermark is inserted. This watermark is obtained from the identification of the User, which is stored in the ACU and was previously sent during the process of establishing the SAC.

In the CFM this watermark is identified as the *second private watermark* (W_2), and corresponds in fact to a fingerprint of the User buying the image.

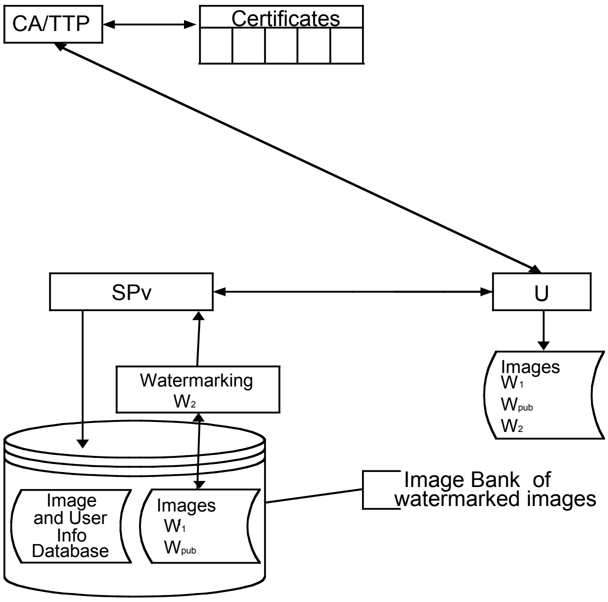


Fig. 6. Contract negotiation and image acquisition.

4. IPR protection

The OCTALIS system uses four different mechanisms for achieving IPR protection: standard image formats JTIP and SPIFF, REGAUT license plates, watermarking and the OKAPI kernel.

4.1. Standard image formats JTIP and SPIFF

The JPEG Tiled Image Pyramid (JTIP) format is an extension of the JPEG standard. This format defines a pyramidal tiling methodology to produce multiple resolutions of an image (pyramidal approach), and store higher resolution levels in different files (tiling approach).

The two lower resolution levels, A and B in the pyramid (see Fig. 7), are used at the ODISS site for web browsing. Higher resolution levels, including C (see Fig. 7), can be considered as having commercial value thus subject to licensing contracts.

Levels below C are tiled and stored in different files having the same dimensions as in C level. The purpose is to optimize downloading in case an error occurs during transfer. In this case it is only necessary to retransmit the file corresponding to the damaged tile. This is important considering that a professional image can have several hundreds of megabytes if stored in a single file.

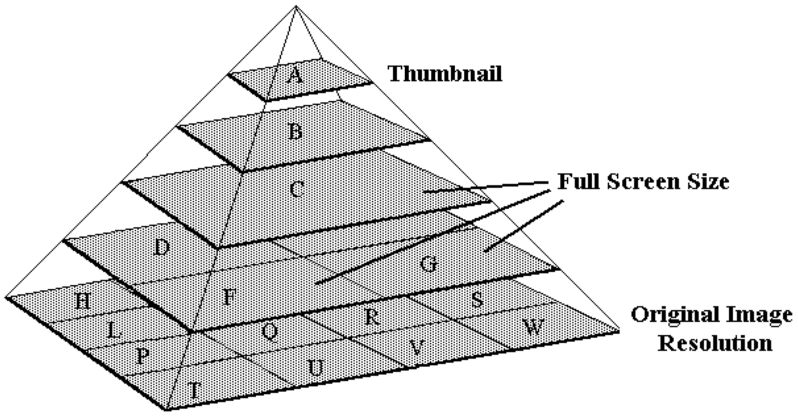


Fig. 7. JTIP format used in OCTALIS.

The Still Picture Interchange File Format (SPIFF) is the official replacement for the JFIF file format for storing JPEG data. It is a generic image file format defined by ITU and ISO/IEC for the storage, compression and interchange of colour or grey-scale, continuous-tone images, and bi-tonal image data [6].

Four major sections compose SPIFF files: *header*, *information directory*, *image data* and an optional section containing *indirect data*. The relative position of these sections is shown in Fig. 8.

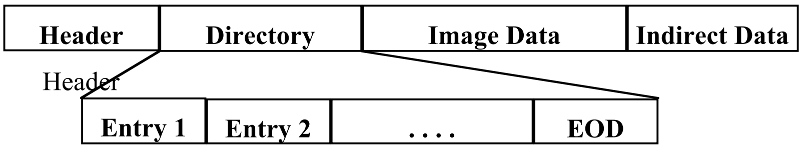


Fig. 8. Sections in a SPIFF file.

A brief description of the content of each section is provided in Table 2.

Header	This section is typical of most image file formats and contains the necessary information to decode the image data.
Directory	A list of information entries. The directory may be thought of as a second header containing information important for IPR and copyright management. The License Plate is stored in the Directory. An entry is used by OCTALIS to store the result from the on-line contract negotiation (see section 5.3.4).
Image Data	This section is dedicated to the image information, which should normally be a JPEG coding.
Indirect Data	Place to store additional data when a Directory Entry is too large.

Table 2. SPIFF sections content.

4.2. REGAUT License Plates

An image Registration Authority is defined in ISO/IEC 10918-4. It is in charge of delivering unique identifiers to be inserted inside image files for identification and copyright protection of contents. As stated in the scope of this standard, due to the fact that a very large number of registration applications are foreseen, the PTSMCR[8] authority will delegate the task of certifying such Registration Authority to the National Bodies [5].

This mechanism allows a National Body, on behalf of the PTSMCR authority, to deliver a certificate of validity to the registrant upon receipt of the input form duly completed and checked. The information contained in the input form is then disseminated to users. Multiple REGAUT allocations are possible inside a given country, provided that the registrants fulfil the exploitation conditions. A collective right society, an image agency, a public or private institution may apply for qualification as a REGAUT.

To become a National Body and receive a REGAUT Identification number, an organisation can apply to the JPEG Utilities Registration Authority (JURA) [7], meeting the following criteria:

i) Unique - it must not duplicate a REGAUT ID already defined:

ii) Correct submission - the syntactically and technically correct submission of SPIFF files produced by the applicant, along with all appropriate explanations;

iii) Suitability - the applicant must be a well-known institution recognised as a professional in the digital imagery domain. Furthermore, this institution must be willing to fulfil its obligation as a Registration Authority.

After a trial period using a temporary REGAUT number where all the necessary requirements must be fulfilled (both technical and legal) by the applicant, the definitive REGAUT is issued, and the organisation is accredited as a valid image Registration Authority, capable of issuing *License Plates*.

A *License Plate* contains information about the Registration Authority:

i) ISO country code;

ii) REGAUT Identification: the unique number assigned by JURA[9];

iii) A sequential number assigned by the REGAUT to each image that is registered.

4.3. Watermarking

An invisible watermark consists in a pattern of bits inserted into a digital image, audio or video file identifying uniquely the media copyright information (author, rights, etc.). The name comes from the faintly visible watermarks imprinted on stationery that identify the manufacturer of the stationery. The purpose of digital

[8] PTSMCR are the JURA items. P - JPEG and SPIFF profiles; T - SPIFF tag; S - SPIFF colour space; M - APPn marker; C - SPIFF compression type; R - Registration Authority.

[9] In Portugal an existing REGAUT is PT-1098.

watermarks is to provide copyright protection for IPR in digital formats. Unlike the printed watermarks, which are intentionally visible, digital watermarks are designed to be completely invisible or, in audio clips, inaudible. Moreover, the actual bits representing the watermark must be scattered throughout the file in such a way that they cannot be identified or manipulated. The watermark should be robust enough so that it can withstand normal changes to the file, such as reductions from lossy compression algorithms [3].

The OCTALIS CFM uses three different invisible watermarks: two private watermarks (W_1, W_2) a one public watermark (W_{pub}). Table 3 shows the purpose for each of these watermarks.

W_1	The first private watermark W_1 corresponds to the digital signature of the image. It will allow to prove if the image has been changed from its original
W_{pub}	The public watermark W_{pub} corresponds to the License Plate. It will contribute to establish the copyrights on an image, based on the entity that registered the image.
W_2	The second private watermark W_2 corresponds to the fingerprint of the User that licensed the image. It will allow tracing the responsibility for eventual unauthorised reproductions.

Table 3. Watermarks in OCTALIS.

4.4. OKAPI kernel

The OCTALIS system relies on the OKAPI security kernel to provide security for applications in open environments. It extends the normal functionality of an operating system for securing communications at the application level, ensuring authentication, privacy and integrity of the communications [9].

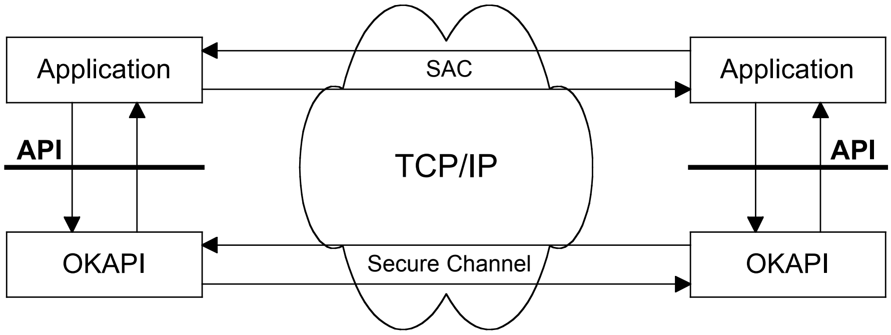


Fig. 9. Secure communications enabled by OKAPI.

Software developers can access the security kernel through an API (see Fig. 9). The API allows the design and implementation of non-proprietary and interoperable solutions for conditional access to multimedia services. Through the API, developers of conditional access systems can establish a Secure Authenticated Channel (SAC) between Users and SPv to achieve secure transactions over insecure channels.

Authentication is enabled through the infrastructure provided by the CAs and the TTPs (see Fig. 1 and Table 1).

Security is enabled through the use of public key cryptography and smart cards to store secret parameters.

5. Contract Negotiation

Like in the real world, establishing the conditions of an on-line digital contract satisfying all the involved parties is not always an easy task. Electronic Commerce can be considered in two main aspects [9]: marketing and contracting. While the first focuses on promoting the products and services to customers, the other focuses on negotiation of the terms and conditions of contracts and the monitoring of contract performance.

It is normally a difficult task to establish a generic model of digital contract for use on the Internet, considering that geographically distributed jurisdictions have different rules about the contents and legal establishment of a digital contract. Such a model should consider several aspects in order to develop a formal representation of electronic contracting:

i) Represent several different trade scenarios, specifying the temporal sequence of the inter-organisational document exchanges for a given transaction;

ii) Be computable, allowing for fully automated computer-to-computer trade transactions;

iii) Be customisable to fit very specific contracting situations, while yet retaining the legal and control qualities of the generic version;

iv) Friendly end-user interface, whereby the terms, rules and procedures of the trade scenario can be easily read and understood by the contracting parties (as well as judges, arbitrators).

Generically a contract should define the following aspects [10]:

i) **Parties**: the certified identity of two or more parties. Usually it should be possible to distinguish who originated the contract. The Copyright Owner must be clearly identified. In the case of shared copyright, all the copyright owners must be specified;

ii) **Validity**: a data interval specifying when the contract will be valid (or a starting date and duration). One of the most sensitive points is the electronic contract validity according to the agreed jurisdiction (country, state, or community);

iii) **Clauses**: one or more description items, which constitute the actual body of the contract, specifying the terms in the contract. These clauses can include, for example: privacy and sub-license conditions;

iv) **Jurisdiction**: the law governing the contract;

v) **Allowed or possible operations**: to each of the intermediary entities in the exploration chain and, if possible, over each of the specific work components, including commercial conditions (sold units, time limit, …);

vi) **Signatures**: by all the **parties**, specifying agreement to honor the **clauses** of the contract during the **validity** period of the contract, in respect with its **jurisdiction**.

Considering the electronic contract clauses and the legislation gap that exists in most of the countries, both contracting entities must define specific own laws in order to fill this gap. The established electronic contract between the contracting parts must at least contain the following clauses: transmitted rights, remuneration, access warranty, work integrity, end of contract, offence compensation, end of contract consequences, and adopted legislation.

Contract information should be described in a language that is understandable to all parties: this is the information that is signed and will be retrieved during an eventual dispute resolution.

In OCTALIS the subject of contracts are digital images.

The rights associated with a digital image can vary accordingly to the terms expressed by the Copyright Owner (CO in Fig. 1). This system supports a wide range of hierarchical terms, providing the capability to define terms and conditions of the contract through an on-line negotiation. Once the buyer (User in Fig. 1) is satisfied with the contract that defines the image usage conditions, digital signatures will authenticate the business and the contract is established.

A demonstration Internet site (http://odiss.adetti.iscte.pt) implementing the on-line contract negotiation has been developed in the framework of the OCTALIS Project [11]. The site represents the SPv in the CFM model (see Fig. 1) previously described.

Throughout this section we will describe in detail the relevant aspects of the negotiation and measures aiming at contract enforcement.

5.1. IPR provisioning

In section 3 we introduced the notion that each image in the data bank would be available in different resolutions. The main purpose for this set of resolutions is to allow the buyer to select the option that best fits into his business needs, and pay accordingly.

As described in the business model adopted by OCTALIS, the CO must address a Service Producer (SPd in Fig. 1) who will produce a set of different resolutions corresponding to the different JTIP levels (see section 4.1). Each file is produced using the SPIFF format, which contains in the same file the image data and additional information concerning IPR (see section 4.1).

One of the important aspects in IPR is the unique registration number assigned by a Registration Authority (RA in Fig. 1). This number will be designated *License Plate* and relates the image, with its Author and Copyright Owner. Thus, before producing the SPIFF files for each JTIP level, the SPd must address a RA, providing it with all relevant information concerning IPR, in order to register the image and obtain a *License Plate* (see section 4.2).

Now the SPd can effectively produce the different image resolutions corresponding to the JTIP levels. Each file produced accordingly to the SPIFF format will contain specific standardised Directory Entries (see section 4.1) to accommodate the *License Plate* and other information such as image descriptions, IPR, date of registration, etc. Though resolutions are different, the original registered image is the same, thus information will be common to all SPIFF files.

5.2. Contract Terms definition

Naturally, each resolution of the same image, hence JTIP level, has a different commercial value, and possibly different associated contractual terms. Thus the terms and conditions must be established.

It is a task of the SPd in conjunction with the CO to define the Contractual Terms and deliver them, together with the SPIFF files, to a Service Provider (SPv in Fig. 3). The SPv will store all information in its image bank and provide the infrastructure that will enable the on-line contract negotiation, and the inherent electronic commerce of the images.

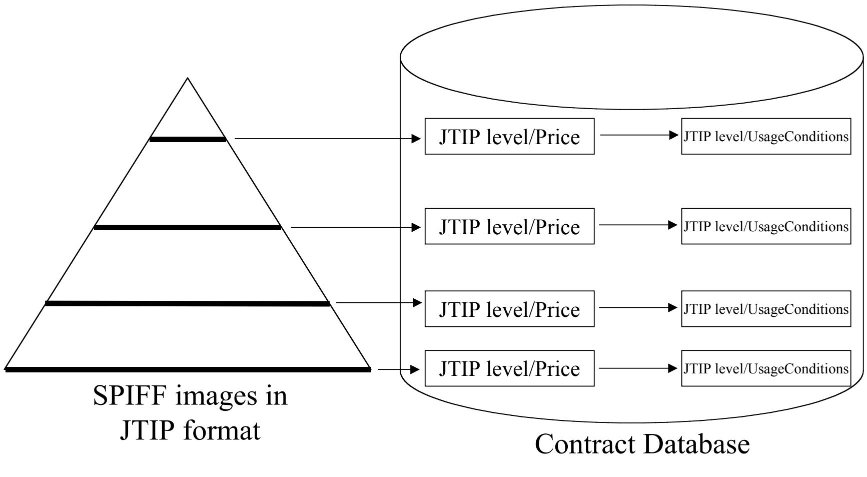

JTIP level/Price
JTIP level/UsageConditions
JTIP level/Price
JTIP level/UsageConditions
JTIP level/Price
JTIP level/UsageConditions
JTIP level/Price
JTIP level/UsageConditions
SPIFF images in JTIP format
Contract Database

Fig. 10. Image contract database.

The system allows the storage of the Contractual Terms and Contractual Conditions that will be proposed to the buyer. Both contractual aspects are organised on a per resolution basis, as shown in Fig. 10.

5.2.1. Database model

The number of Contractual Terms for each image resolutions is unlimited, meaning that CO and SPd can define any terms that are reasonable and store them in the SPv database.

The structure adopted for the database allows the insertion of new terms or conditions at any time, without compromising contracts that were previously established for that same image resolution.

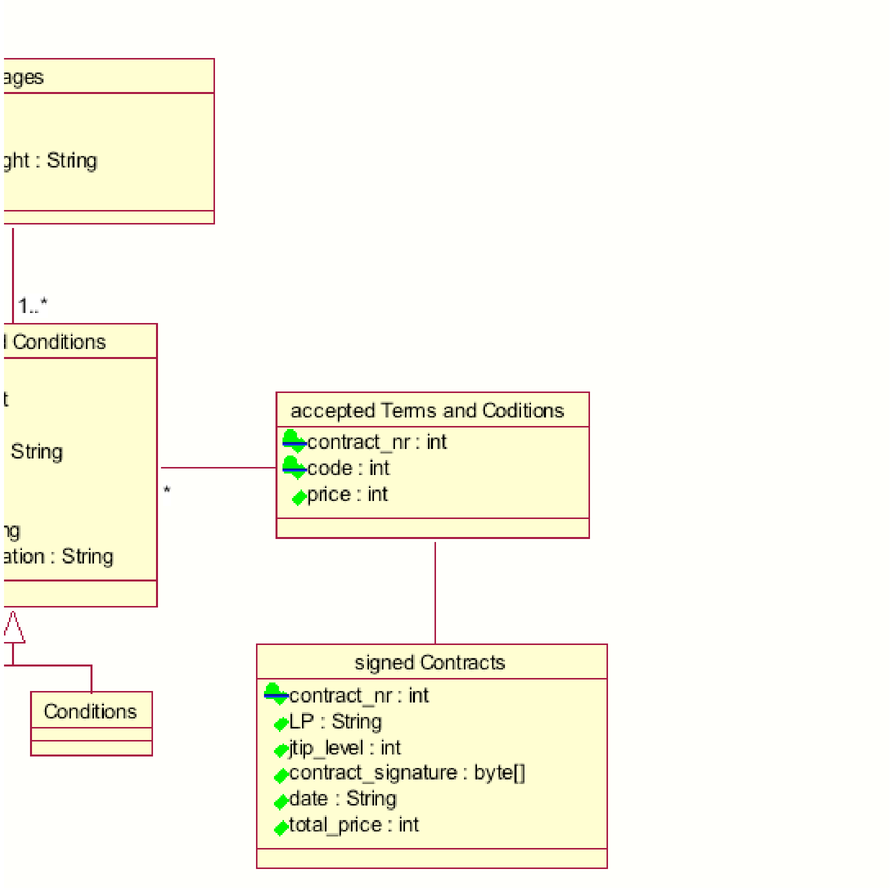


Fig. 11. Basic UML model.

A simplified UML model of the database is shown in Fig. 11.

Each Contractual Term has a *price* tag, and an *item* tag. Both are used in the contract negotiation, as described in section.

Terms can be negotiable or non-negotiable. This characteristic is defined through the *item* tag: a term that has a single tuple for a certain item number, is implicitly a non-negotiable term. Non-negotiable terms are imposed to the User and the system does not allow them to be removed. The price value can be negative to accommodate situations of discounts.

Table 4 shows some possible Contractual Terms, and how they can be related through the *item* tag.

Code	Contractual Term description	Price	Item
1	To be used in web pages	10	1
2	To be used in books	100	1
3	To be used in newspapers or magazines	1000	1
4	Not allowed in outdoor advertising	0	2
5	Can only be used once	0	3
6	Can be used an unlimited number of times	100	3
7	Image can not be edited	0	4
8	Rights granted for a period of 3 months	100	5
9	Can be used immediately	1000	6
10	Can be used only after 20/05/1999	500	6
11	Can be used only after 20/07/1999	-50	6

Table 4. Examples of Contractual Terms.

In addition to the Contractual Terms, the database also supports Contractual Conditions (see Fig. 11), which are normally associated with payment and delivery aspects.

A structure similar to the above has been adopted. Table 5 shows some possible Contractual Conditions.

Code	Contractual Conditions description	Price	Item
1	On-line immediate payment	0	1
2	Payment upon invoice	50	1
3	Payment upon invoice (30 days credit)	100	1
4	Image secure download	0	2
5	Image sent in CD-ROM through surface mail	10	2
6	Image sent in CD-ROM through air mail	20	2

Table 5. Examples of Contractual Conditions.

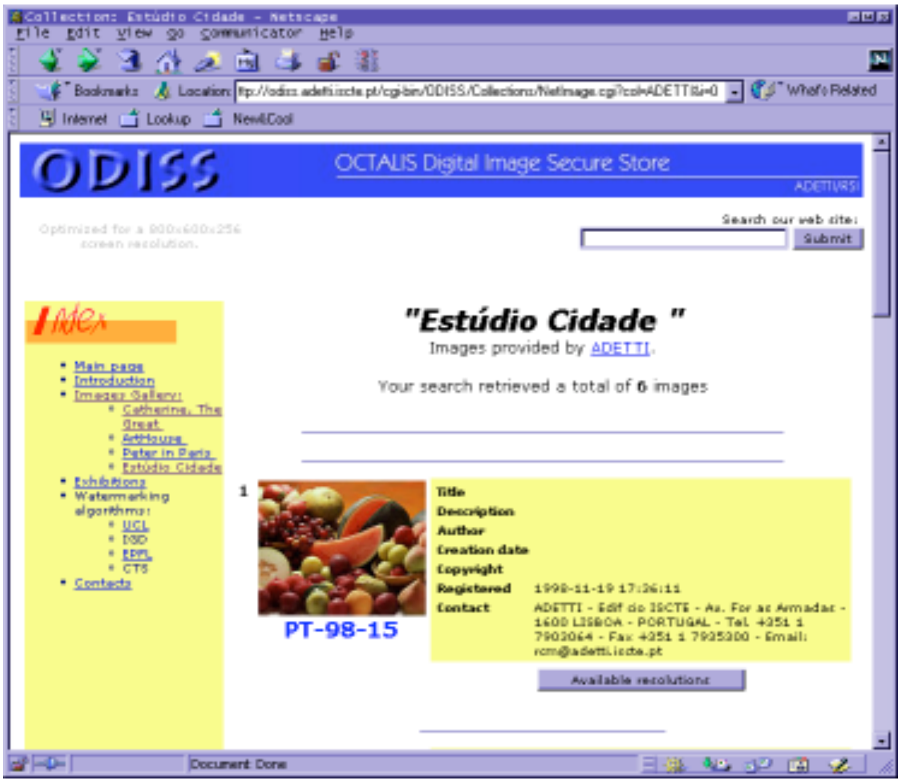
5.3. Establishing an On-line Contract

The process of establishing an on-line contract defining the usage terms and conditions for a digital image starts with the selection of the image.

5.3.1. Browsing the image bank

In the ODISS demonstration site http://odiss.adetti.iscte.pt there are two possibilities of selecting an image: i) searching by keywords or ii) browsing through thematic or artist collections.

Once the image is selected, it is necessary to choose the resolution adequate for the User's application.



Location: ftp://odiss.adetti.iscte.pt/cgi-bin/ODISS/Collections/NetImage.cgi?col=ADETTI&i=0

OCTALIS Digital Image Secure Store

ADETI/URSI

Optimized for a 800x600x256 screen resolution.

Search our web site:

Index

- Main page
- Introduction
- Images Gallery:
  - Catherine, The Great
  - ArtHouse
  - Peter in Paris
  - Estúdio Cidade
- Exhibitions
- Watermarking algorithms:
  - UCL
  - IGD
  - EPFL
  - CTS
- Contacts

"Estúdio Cidade "

Images provided by ADETTI.

Your search retrieved a total of 6 images

1

PT-98-15

Title

Description

Author

Creation date

Copyright

Registered 1998-11-19 17:36:11

Contact ADETTI - Edif do ISCTE - Av. For as Armadas - 1600 LISBOA - PORTUGAL - Tel. +351 1 7903064 - Fax +351 1 7935300 - Email: rcm@adetti.iscte.pt

Fig. 12. Available resolutions for the same image.

The web page shown in Fig. 12 allows displaying of available resolutions for the image. The universal identification number, which was referred before as *License Plate*, is shown below the thumbnail image.

The approach followed in the development of this application allows the negotiation of several predetermined terms and conditions, defined by the CO. The purpose of the negotiation is to establish, upon input from the User, a contract defining the terms and conditions the User is willing to accept and comply with, for that particular image.

5.3.2. Contract negotiation

The Contract negotiation is performed on-line through a web page (see Fig. 13).

This page presents, on the left window, the terms that apply to the selected image. The right window proposes default terms to the User.

The User can accept or reject the default terms, by moving them from one window to the other, with the exception of non-negotiable terms.

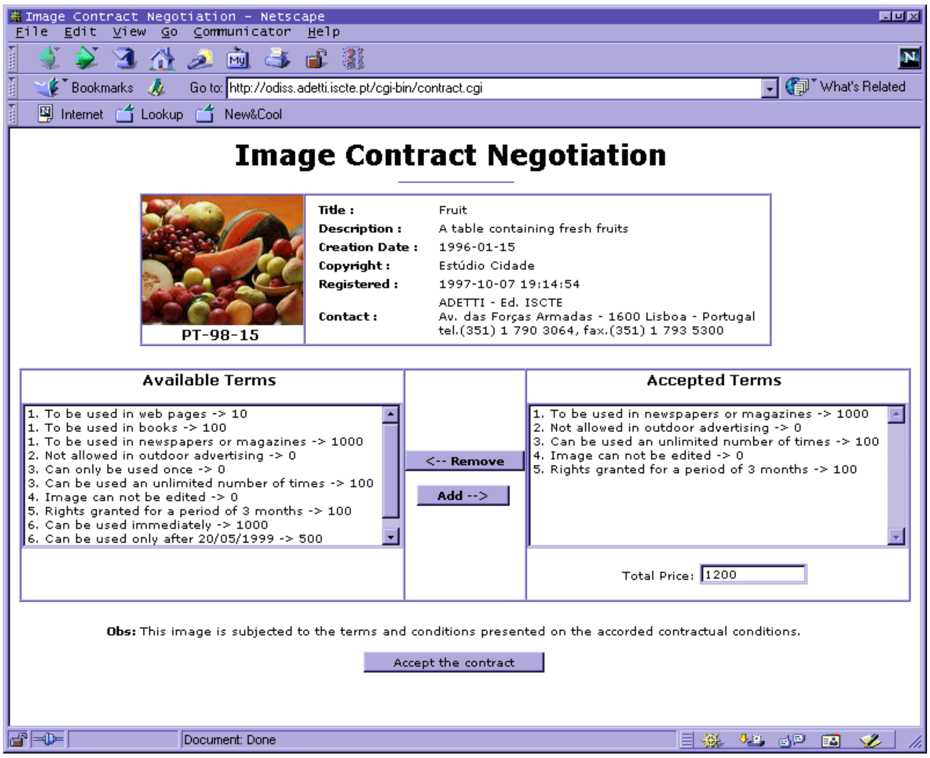


Image Contract Negotiation - Netscape
File Edit View Go Communicator Help
Bookmarks
Go to: http://odiss.adetti.iscte.pt/cgi-bin/contract.cgi
What's Related
Internet
Lookup
New&Cool

Image Contract Negotiation

PT-98-15

Title :	Fruit
Description :	A table containing fresh fruits
Creation Date :	1996-01-15
Copyright :	Estúdio Cidade
Registered :	1997-10-07 19:14:54
Contact :	ADETTI - Ed. ISCTE Av. das Forças Armadas - 1600 Lisboa - Portugal tel.(351) 1 790 3064, fax.(351) 1 793 5300

Available Terms

1. To be used in web pages -> 10
1. To be used in books -> 100
1. To be used in newspapers or magazines -> 1000
2. Not allowed in outdoor advertising -> 0
3. Can only be used once -> 0
3. Can be used an unlimited number of times -> 100
4. Image can not be edited -> 0
5. Rights granted for a period of 3 months -> 100
6. Can be used immediately -> 1000
6. Can be used only after 20/05/1999 -> 500

Accepted Terms

1. To be used in newspapers or magazines -> 1000
2. Not allowed in outdoor advertising -> 0
3. Can be used an unlimited number of times -> 100
4. Image can not be edited -> 0
5. Rights granted for a period of 3 months -> 100

Total Price: 1200

Obs: This image is subjected to the terms and conditions presented on the accorded contractual conditions.

Fig. 13. Web page for the Contract negotiation

Each term belongs to an item family, which aggregates terms that are interrelated.

The User is free to choose the terms that best suite the intended usage for the image, provided that one term for each different item is present in the right window, when the Contract is submitted to the SPv server at the ODISS site.

The next stage is the negotiation of the Contractual Conditions. Since these Conditions are related to payment and delivery issues, they are defined by the SPv.

Establishing the Contractual Conditions is a procedure that follows steps similar to the Contractual Terms negotiation. The web page shown in Fig. 13 is again used to display on the left window the available conditions and the default conditions on the right window.

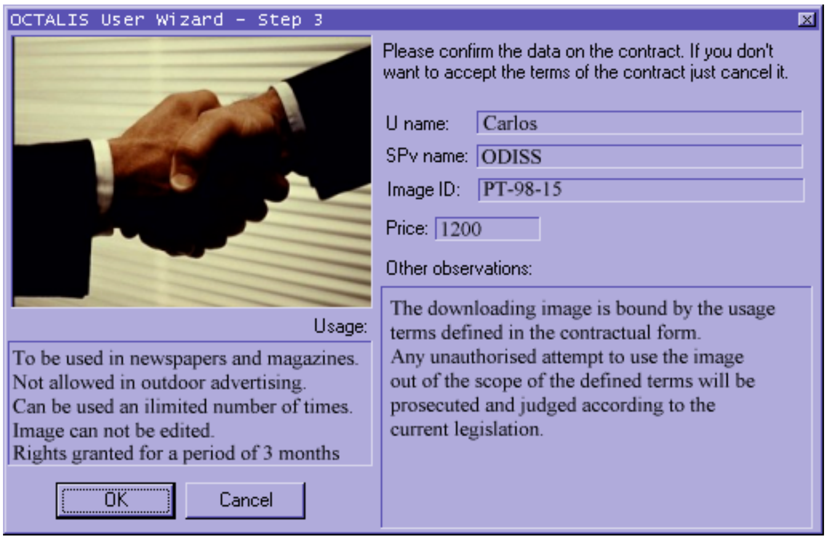
Once the User has accepted one condition for each *item* present on the left window, the negotiation is finished and the Contract is ready to be signed.

5.3.3. Contract signature and transaction security

The process of signing the Contract uses some of the features present in the OKAPI Conditional Access System to ensure Contract authentication and non-repudiation, as well as security in the transaction.

In fact all the Contract negotiation that we have been describing is accomplished through the exchange of secure messages between the User application and the SPv server. The Secure Authenticated Channel (SAC), which was previously established when the User started the OKAPI User Application, provides security for those messages.

In the process of establishing a SAC, the User and the SPv have already exchanged their public keys. Selecting the OK button, shown in Fig. 14, the User application signs the final Contract and sends it securely through the OKAPI enabled SAC to the SPv.



Please confirm the data on the contract. If you don't want to accept the terms of the contract just cancel it.

U name: Carlos

SPv name: ODISS

Image ID: PT-98-15

Price: 1200

Other observations:

The downloading image is bound by the usage terms defined in the contractual form.
Any unauthorised attempt to use the image out of the scope of the defined terms will be prosecuted and judged according to the current legislation.

Usage:

To be used in newspapers and magazines.
Not allowed in outdoor advertising.
Can be used an ilimited number of times.
Image can not be edited.
Rights granted for a period of 3 months

Fig. 14. On-line Contract signature.

A verification procedure takes place in the SPv server, ensuring those Contractual Terms and Conditions have not been tampered, and correspond to the image previously selected. Upon completion the SPv signs the Contract and sends it back to the User through the same channel.

5.3.4. Contract storage

The Contract is stored in two different places with different purposes: i) for administrative purposes, it is stored in the database and ii) for protection of IPR purposes it is written in a specific Directory Entry of the SPIFF file that will be delivered to the User.

Though it is easy to remove Directory Entries from a SPIFF file, or change their contents, the User is informed that tampering any information in the acquired file is not allowed, thus SPIFF entries should always accompany the image file.

5.3.5. Contract payment

Currently OCTALIS does not define a model for on-line payment. Integration with payment systems already existing is a possible and desirable evolution.

The fact that OCTALIS relies on the OKAPI security kernel to establish a SAC between the User and the SPv potentially provides the capabilities for diverse on-line payment forms.

5.3.6. Delivery of the image

Delivery of the contracted image can be accomplished through multiple channels.

As we have seen before, during the Contract negotiation the User is allowed to select the desired delivery channel, based on the possibilities previously defined by the SPv.

In case of on-line immediate delivery, the image will be sent to the User though the OKAPI enabled SAC. A protocol, using specific session keys negotiated between User and SPv, is established to encrypt the SPIFF file that is subject of the Contract, and send it across the network to the User.

6. Conclusions

The work developed in the OCTALIS Project demonstrates an approach to IPR protection through on-line negotiation of digital contracts that regulate digital content transactions.

Conditional access and watermarking technologies, together with the extensive use of standards provided the means to preserve IPR aspects over the Internet.

Several aspects contribute to an effective electronic commerce of digital images enabled by OCTALIS:

i) The CO can be assured that images will be used according to the licensed terms, furthermore the means to prove that the image is being misused are available;

ii) The User is assured that the origin of the image is from a certified image vendor (SPv) that the image itself is certified and that no one can intercept the image while the downloading process is in progress;

iii) The SPv is assured that the User has succeeded in establishing his identity towards the system and has the means to prove that the User signed a digital licensing contract for a certain image;

iv) In case of illegal copies the responsible entities can be identified and copyright information can be retrieved from the image;

v) Negotiation of the terms and conditions of a different licensing contract for each images and for each image resolution, with on-line price establishment.

An important aspect partially solved through the solutions deployed by OCTALIS is the insurance to authors and content owners that a User signs a contract on the licensing conditions they defined for their work.

However, there are other aspects related with legal issues that are not in the scope of the project. Technologies deployed provide the means to effectively define, trace and prove IPR over a digital content, but the possibility to enforce those rights depends on legislation that differs from one country to another. Digital signatures are not yet widely valid for document authentication and there is still much legal work to do until copyright violations on digital content can be effectively prosecuted.

References

1. *Standing Committee on Copyright and Related Rights – First Session*, WIPO – World Intellectual Property Organization, November 1998, http://www.wipo.org
2. Burnett, M., Jan, M., D10: Rights identification and management specifications, OCTALIS - AC242, April 1997
3. Delaigle, J-F, “D12 – Common Functional Model”, TALISMAN, March 1996
4. Arnold, M., Koch, E., D11: OCTALIS Trial Specifications, OCTALIS – AC242, July 1997
5. Digital Compression and coding of continuous-tone still images: Registration of JPEG profiles, SPIFF profiles, SPIFF tags, SPIFF colour spaces, APPN markers, SPIFF compression types and Registration Authorities (REGAUT), ISO/IEC DIS 10918-4.2:1997
6. Information technology – Digital compression and coding of continuous-tone still images: Extensions, ISO/IEC 10918-3.
7. JURA – JPEG Utilities Registration Authority, http://jura.jpeg.org.
8. Serret, X., Boucqueau, J., Mas Ribés, J., “D19 – OKAPI specific tools design”, January 1998
9. Lee, R. M., “Towards Open Electronic Contracting”, International Journal of Electronic Markets, Vol. 8, No. 3, 1998.
10. Marques, J., “Protecção de Direitos de Autor no meio digital e seu impacto no Comércio Electrónico”, Master Thesis, Mestrado em Gestão de Sistemas de Informação, ISCTE 1999.
11. OCTALIS – Offer of Content through Trusted Access LInkS, http://www.tele.ucl.ac.be/OCTALIS and http://adetti.iscte.pt/RSI/OCTALIS/CD-ROM.