# Digital Rights Management in Information Publishing

Salden, A.H.; Goedvolk, E.-J.; Ter Doest, H.; Kersemakers, R.; Slijp, D.; Prins, J.E.J.

*Published in:*
International Conference on Law and Technology (LawTech 2002), Cambridge, MA, USA, November 6-8, 2002

*Publication date:*
2002

# Digital Rights Management in Information Publishing

Alfons H. Salden, Ernst-Jan Goedvolk and Hugo ter Doest

Telematica Instituut, P.O. Box 589, 7500 AN Enschede, The Netherlands
Phone: +31-53-4850470/438/481, e-mail: {salden, goedvolk,terdoest}@telin.nl

Rob Kersemakers and Dion Slijp

Océ-Technologies B.V., PO Box 101, 5900 MA Venlo, The Netherlands
Phone: +31-77 3595013/5166, e-mail: {rke,dfsl }@oce.nl

Corien Prins

Tilburg University, Center for Law, Public Administration and Informatization,
P.O. Box 90153, 5000 LE Tilburg, The Netherlands
Phone: +31-13 466 3088/8199, e-mail: J.E.J.Prins@uvt.nl

## ABSTRACT

We present a business and technological solution to digital rights management (DRM) issues that could arise with increasing document management capabilities of application service providers (ASPs) offering future networked business-to-business (B2B) Information Publishing services. Document management concerns indexing, querying and retrieval in the author-publisher relationship. In the publisher-ASP-subscriber relationship, however, it concerns mainly presentation, i.e. printing and viewing of document content. On the basis of an ASP business model we identify critical DRM aspects that future B2B Information Publishing service providers have to face in the light of the above mentioned technological advances. We elaborate on technologies that might resolve related DRM issues. Furthermore, we discuss legal implications of such technological advances, e.g. conflicts between intellectual property rights enforcement and privacy protection due to those advances. Subsequently, we specify digital rights of enriched document content by extending the Open Digital Rights Language (ODRL). Finally, we enforce digital rights of enriched document content by implementing an ODRL-compliant DRM services on top of our Information Publishing service.

## KEY WORDS

Information publishing, business model, DRM, ODRL

## 1. INTRODUCTION

Information Publishing is aiming at realising a web service that offers a business as well as technological solution for electronic publishing and document management between publishers and companies or among companies exclusively [1]. As DRM is an essential business aspect in Information Publishing, we investigate in this paper how to integrate DRM with our existing business as well as how to realise DRM service components that actually enforce digital rights conform an accepted specification language. We focus mainly on enforcing digital rights that arise due to technological advances in the area of document management systems. In addition we discuss legal implications of those technologies, in relation to privacy laws in particular.

Both Information Publishing companies and E-publishing companies [1, 2] have almost similar networked business models [3]. They all provide electronic document content over heterogeneous networks. They both support creation and publishing, marketing and distribution, and transaction of document content.

However, they significantly differ in their value proposition, business organisation and revenue model. That of E-publishing companies concerns in general the provisioning of business-to-consumer (B2C) services from a single publisher to a large customer base. Information Publishing companies on the contrary offer advanced B2B document management services to many publishers as well as a large customer base of companies. The business organisation of E-publishing normally involves the arrangement of services between one publisher and one customer. Besides similar arrangements Information Publishing also includes arrangements between various third parties that support sophisticated services such as legal and financial clearing. Outsourcing of secondary business processes to those third parties is nowadays common for networked businesses. Information

Publishing as well as E-publishing companies [1] could gain a lot of competitive advantages over their competitors by adopting an ASP business model [4]. Such a model brings them in the reach of a larger customer base through economies of scale yielding higher revenues and possibly profits, which allow them in turn to focus on their core business, which is service innovation (i.e. business differentiation followed by integration) and customisation. The revenue models of both type of companies differ in the applied exploitation strategy. In E-publishing the whole document content is sold in the form of e-books. In Information Publishing, however, even the usage of modified fragments of document content is licensed by publishers to companies, or among collaborating companies. However, both type of publishing enterprises make use of billing, accounting and payment services for financial settlement of the selling of e-books or licensing of document usage, respectively. However, in Information Publishing on-line payment would be not so common as in E-publishing. Only if companies are assigned specific quota for document content or service usage, it is conceivable that an ASP providing the advanced Information Publishing services would ask banks or clearing houses about the financial credibility of companies.

DRM aspects of a networked B2B Information Publishing will occur over the complete value chain ranging from the initial submission of electronic content by authors, the subscription by companies, to content delivery, i.e. viewing and printing of content. Analogous for E-publishing [2] the question arises how to describe Information Publishing in terms of parties (including Certificate Authorities), the roles they play and the interactions between them, and analyse this all in terms of DRM. This means that we have to identify in our value chain the right holders of intellectual property rights, their offered services, their (digital) rights and obligations, their legal liability and financial accountability under European Union and international laws and regulations. In the context of specifying such DRM aspects languages, models and architectures are indispensable [5, 6]. Furthermore, it means that we have to define where and how licensing will take place, to pinpoint vulnerable interactions (risks) with respect to rights management [7, 8], and to propose countermeasures to cope with these risks [9]. The latter measures boil down to enforcing permissions of viewing and printing, modification, storage, distribution and duplication of content. These permissions could be laid down in (paper or electronic) contracts [10] that additionally comprise constraints to e.g. user and device, requirements of e.g. payment, user authentication and tracking, and contextual conditions such as those related to geographical regions.

The above document content usage permissions and other DRM issues initially stated in a contract should subsequently be translated to and enforced in the digital DRM domain of an Information Publishing service. A number of standards are currently being developed and deployed that support the specification of digital rights independent of the type of content. ODRL developed by the Open Digital Rights Language[1] (ODRL) Initiative and eXtensible rights Markup Language[2] (XrML) that recently has been adopted by OASIS, seem serious candidates for application in Information Publishing.

An evaluation of these standards against our Information Publishing requirements shows that ODRL is the most promising candidate for our purposes. Authors, publishers, Information Publishing service providers, ASPs and subscribed companies all have high expectations that in essence boil down to easy, secure and profitable integration of innovated document management services with those of their own. ODRL is an open language and therefore extensible. It allows us to readily meet those expectations and to resolve complicated digital rights issues among the parties that are caused by the advances made in document management technologies and the imposed legal constraints.

To facilitate automatic processing and enforcement of digital rights expressed in ODRL, DRM-specific software components must be implemented that offer their services via ODRL-compliant interfaces. Furthermore, we have to show how extended ODRL specifications can be stored efficiently in an XML database in combination with enriched document content. Last but not least we have to demonstrate an ODRL-compliant extended DRM service for Information Publishing focusing on permissions of usage, i.e. display and printing; re-use, i.e. modification, excerpts, annotation and aggregation; temporal constraints of viewing such as date-time or interval; and requirements with respect to payment of content-usage, such as post-pay, pre-pay and per-use.

Our paper is organised as follows. In section 2 we give an account of our adopted ASP business model for Information Publishing. We stipulate the particular value proposition, business organisation and revenue model of our business model. In section 3 we study DRM aspects of Information Publishing from a business as well as a technological perspective. We study in detail the legal implications of DRM solutions to enforce digital rights of document content that are enriched by the latest document management system technologies. In this context we consider conflicts with privacy legislation due to those advances made in both DRM and document management system technologies. In section 4 we extend ODRL to enable digital rights specification of enriched document content. Furthermore, we implement DRM specific software components that are compliant to ODRL to enforce those rights. We conclude discussing in line with the legal implications of technological advances in document management and DRM some open problems

[1] http://www.odrl.org/
[2] http://ww.xrml.org/

that Information Publishing companies are confronted with.

## 2. INFORMATION PUBLISHING

The value proposition of Information Publishing [1] is twofold. On the one hand, publishers could be offered a low cost solution for electronic publishing of document content delivered by authors to subscribers, i.e. companies (among collaborating companies is also a possibility). This fact in turn could bring a large customer base of companies within reach of the publisher, i.e. economies of scale, compared to the traditional way of publishing, in which one has a considerable logistic overhead. In addition, Information Publishing service providers could offer additional sophisticated services like storage and printing facilities to its customers. On the other hand, Information Publishing could offer companies a broader range of high quality electronic and business specific publications that can be viewed on-line or printed on-demand at a competitive price over heterogeneous networks (see **Figure 1**). Furthermore, service innovation and customisation could be guaranteed as the Information Publishing company would be able to focus on its core business.

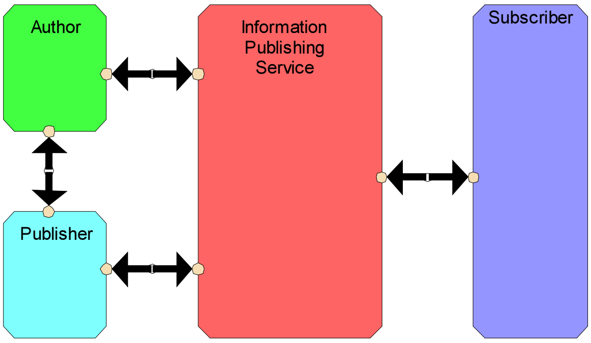


**Figure 1: Information Publishing Value Network**

In the case of networked Information Publishing the document content is provided via viewing and printing services for electronic publications and documents. The document has been structured and extended with meta-data by categorisation components integrated with the document management system. These components enriching documents could be licensed by the Information Publishing service provider to the subscribers. Functionality of the Information Publishing service that then could be licensed includes search functionality to find the right publications and summary services to generate business relevant abstracts of publications. Besides the document content management services also access, viewing, printing and transaction rights on the Information Publishing service can be sold or rented to a subscriber such that he or she has access to either all publications or a particular transacted subset. The content and services can be sold on subscription or license basis, per unit of usage of viewing and/or printing service, or can funded by third parties such as advertisement companies on the Information Publishing portal. Furthermore, if the Information Publishing service provider is a broker that mediates between publishers and subscribers, it can make a margin from each subscription that is sold. A networked Information Publishing provider that adopts an ASP business model can generate income from the services it provide to both publishers and subscribers. Publishers pay for using the e-publishing service to distribute their publications, subscribers pay for viewing or printing documents and/or usage of the document management service. In order to charge publishers and subscriber, it is necessary to make their service offerings and requests explicit. This summarises briefly some possible exploitation strategies that can be worthwhile to consider in a revenue model.

As stated above for reasons of economies of scale and service customisation and innovation, the Information Publishing service could be outsourced to an ASP. The Information Publishing service provider could then still be platform administrator and service creator, i.e. the service provider could still fulfil the administration role of the Information Publishing platform and be the developer of the new services. In this way the service provider would stay in control of the functionality (services offered) and the quality of service offered. The publisher could provide from its own repository or that of a Data Centre (probably located at the ASP-site itself), document content of the authors to the subscribers. Furthermore, the service provider could offer advanced document management services on top of the ASP platform to both publishers and subscribers. The Bank could then offer the necessary financial services to all the parties involved in the service delivery. Thus the service provider could play the role of process controller, platform administrator, print shop provider and service creator. The third party ASP could provide other services like storage to the publisher, network access and connectivity to all other parties. As in this case the service provider could innovate and deploy themselves next generation document management services, it would be more than plausible that they also will look after the integration of extended DRM and alike services for those document management services (see section 3).

The advantage of the above hypothetical business model is that the secondary business processes are outsourced to the ASP and not the service provider's core business. This scenario could be the most realistic for the Information Publishing service provider, since in that case he could concentrate on its core business, i.e. innovating and deploying printing, viewing and document management services, and simultaneously attain high customer base retention values. In **Figure 2** the actor diagram related to our specific business organisation shows how the Information Publishing service provider has aggregated several of those roles leaving the ASP with the responsibility for enabling access, connectivity, and delivering storage and computational resources. Note that the responsibility of access control and alike may still lie with the Information Publishing service provider. Thus ASP provides merely the network infrastructure to the other parties involved in the value chain.

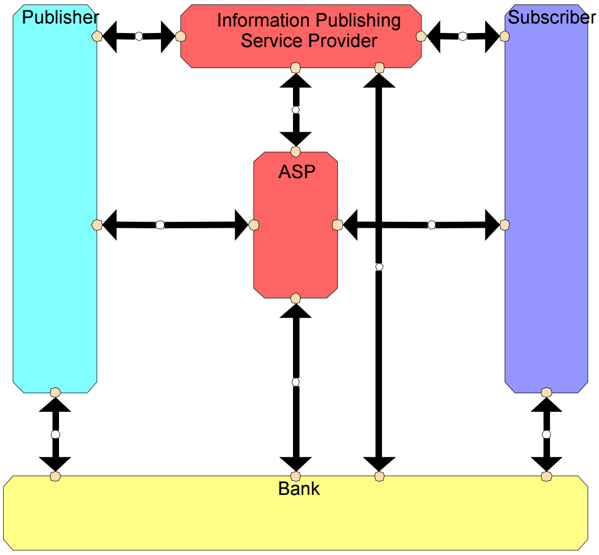


**Figure 2: Information Publishing  Actor Diagram**

## 3. DIGITAL RIGHTS MANAGEMENT

In the following technology is leading our Information Publishing business model. This means that the technological advances made in the area of document management and presentation technologies heavily influence the adopted Information Publishing business model. Novel technologies offer new business opportunities asking for other value propositions, business organisations and revenue models (see also section 2). One of the critical success factors for Information Publishing service providers to attain a competitive advantage over their competitors by innovating document management  services, is to set up a proper DRM service on top of such document and presentation services. Issues like who is the rights holder in case of sophisticated transformations of document content should be resolved, e.g. issues regarding further structuring of document content, constraining transactions like viewing and printing of documents, summarisation of documents whenever carried out by one of the parties in the Information Publishing value chain (see also section 4).

Legal aspects of Information Publishing translate to business requirements and subsequently to technological requirements. Furthermore, choosing a particular solution for DRM may be in conflict with many other legal issues like privacy – advances in Information Publishing may considerably complicate those matters. In the following paragraphs we elaborate on those matters.

### 3.1 BUSINESS REQUIREMENTS

In DRM one is faced with national, European and international laws, directives, regulations and arbitrage policies to prevent analogue and digital copyright and other rights infringements (see Internet Digital Rights Management[3]). DRM focuses not only on security, encryption and watermarking in order to prevent unauthorised exploitation of content, but also on description, identification, trading, protection, monitoring and tracking of usage rights. With regard to this DRM aims to safeguard the interests of copyright holders of digital content. DRM systems implement measures like copy control, access, control, usage metering and traceability to prevent the unauthorised use, copying and/or manipulation of copyrighted material (see also section 3.2).

In Information Publishing the issues, described above, boil down to various networked business requirements (see also section 2). In an ASP solution to Information Publishing security management and DRM should enable the protection of the copyrights held by publishers on the documents they distribute, store and transact using the Information Publishing service. Critical issues in Information Publishing with regard to DRM are storage at the repository of the publisher, Data Centre or ASP; distribution among the actors; viewing, printing and copying by the Subscribers, and other transactions on the publications by the actors involved.

For E-publishing as well as Information Publishing almost similar DRM requirements (see section 1) are valid during their business process steps.

*Creation and publishing step:*

- A rights specification language that is used to express the terms of the contract between parties,
- Encryption of digital content to securely distribute document content among parties.

*Marketing and distribution step:*

- Secure electronic packaging for document content and related items,
- Authentication of document content via digital signatures or certificates,
- Encryption of document content during transaction,
- Information Publishing business model aspects related to e.g. revenue model expressed in terms of the rights specification language.

*Licensing to Subscriber step:*

[3] http://www.idrm.org

- Allowed terms of sale or license expressed in terms of the rights specification language,
- Authentication of parties in transaction,
- Authorisation of transaction,
- Non-repudiation of origin and receipt of transaction,
- Financial clearing of transaction under agreed terms,
- Consumer information clearing for marketing purposes under agreed terms.

*Document transaction step:*

- Access and processing tools to unlock document content,
- Trusted environment for accessing and using document content consistent with digital rights,
- Facilities for printing, viewing, lending, giving away and distribution of document content in line with digital rights,
- End-to-end document content protection in particular on the Subscriber's printing or viewing device.

*Subscriber support step:*

- Facilities for parties to deliver value-adding services to the Subscriber such as document content categorisation (including summarisation tools), retrieval and authoring services (for modifying of document content) besides extended standard support services including virtual libraries, backup/restore services and archival services.

In the following we make the legal aspects of transactions on documents explicit together with the importance of contracts to enforce permissions to do so. Furthermore, we address the protection of intellectual property rights at the repository of a publisher, Data Centre or ASP. Last but not least we address the protection of intellectual property rights during distribution of publications.

### 3.1.1 TRANSACTIONS

Information Publishing may result in several transactions or transformations by subscribers or providers on documents, namely:

- Consultation and viewing of documents,
- Printing and sharing of documents,
- Modification and subsequent multiplication and distribution of transformed document content, e.g. aggregated summaries.

These transactions are subject to either intellectual property rights or data bank rights. Intellectual property rights apply, if the transactions still preserve enough originality of the primal documents. Data bank rights apply, if the transactions concern factual data sets such as name, address and city. To assess the legal implications of those Information Publishing actions we first of all give an account of the involved general intellectual property rights issues, namely their reach and the involved actors. Finally, we consider legal aspects of contracts allowing transactions on documents.

From a copyright-contract perspective [11] a publisher in Information Publishing is:

- Intellectual property right holder (possibly on behalf of the creator) of a work,
- License holder on the basis of a license with a third party allowed to sub-license.

Subsequently, the Information Publishing service provider can sub-license, on the basis of a contract, the usage of a work to (a representative of) subscribers. In this chain of sub-licenses the permissions, responsibilities and accountabilities in case of intellectual property rights infringements should be arranged by contracts [8]. In particular, the Information Publishing service provider should preferably not be kept accountable for intellectual property rights infringements by the publisher, nor should the subscriber be kept liable for those by the Information Publishing service provider. In the sequel we elaborate on intellectual property rights and related contracts.

*INTELLECTUAL PROPERTY RIGHTS*

Copyright law provides that, the author or creator of a document or the publisher, who owns and provides its enriched document content via the Information Publishing service, are in principle holders of the corresponding intellectual property rights. In line with this law, a processor of a document, provided he got permission of the intellectual property right holder of the original document content to transform the document, can become right holder of the transformed document content, if this content possesses enough originality of its own. Such a situation may arise quickly if the advanced document services for B2B Information Publishing can offer companies aggregations of business specific summaries of more than one publication (see section 4). The exclusive rights of reproduction and distribution of an enriched document will then belong to the intellectual property right holders of that enriched document.

For transactions on document content permission of the intellectual property right holder is needed. In the Information Publishing context such a permission can be granted by paying a certain fee and should be regulated by a particular license to view, print and transform document content. The transactions on the document are then depending on the chosen revenue model limited to (see also section 2):

- A fixed number of viewing and printing sessions;
- A fixed time of viewing;
- Authorised subscribers;

- A definite set of purposes for transformation like generating summaries and translations.

A license for transactions on document content is then commonly laid down in a contract [10] between subscriber, Information Publishing service provider and publisher [12].

In this context the creation and exploitation of multimedia require enforcement of usage permissions of all the intellectual property right holders whose works are being aggregated [7]. In order to prevent that Information Publishing service provider and subscribers are being kept legally and financially accountable in case of intellectual property rights infringements before that the transactions on the documents, which were provided by the publisher, even could take place, the contracts have to stipulate that only the publisher in those cases is responsible and thus liable and accountable. In this respect in particular one-stop-shops that manage data about works and related conditions of usage, and clearing houses that manage rights, licenses and contracts all together, could help in resolving liability and accountability issues as well as prevent unintended intellectual property rights infringements.

*CONTRACTS*

From the perspective of the Information Publishing service provider there are two contracts needed, namely:

- A contract with the publisher,
- A contract with (a representative of) the subscriber.

The contract between the Information Publishing service provider and the publisher should state or handle the following issues:

- Information Publishing service provider is permitted by publisher to sub-license subscribers,
- Access control implemented by the Information Publishing service provider on behalf of the publisher is issued to subscribers through e.g. authorisation,
- Transaction control implemented by Information Publishing service provider on behalf of publisher is issued to subscribers through e.g. a limited viewing time,
- Monitoring capabilities of the actual transactions on the documents are provided by the Information Publishing service provider to the publisher through e.g. a logging system,
- Non-liability of Information Publishing service provider is assured by the publisher in case of (unintended) intellectual property rights infringements by publisher or third parties.

The above type of contract needs to supplemented with technical specifications concerning its life span and other conditions of non-repudiation.

The contract between the Information Publishing service provider and the subscriber should cover the following business issues:

- Subscriber is permitted by the Information Publishing service provider to view, print and copy documents for his/her own use,
- Access control implemented by the Information Publishing service provider on behalf of the publisher is issued to subscribers through e.g. authorisation,
- Transaction control implemented by the Information Publishing service provider on behalf of publisher is issued to subscribers through e.g. a limited viewing time,
- Monitoring capabilities of the actual transactions on the documents are provided by the Information Publishing service provider to the subscriber through e.g. a logging system,
- Non-liability of subscriber is assured by the Information Publishing service provider in case of (unintended) intellectual property rights infringements by Information Publishing service provider, publisher or third parties.

### 3.1.2 STORAGE

For Information Publishing the service provider stores not only information about intellectual property right protected works and their authors in data banks. It also stores information about the transactions on those works, e.g. the usage by the subscribers, at these centres (for related implications of the entanglement of DRM and privacy issues see section 3.3). Concerning the intellectual property right the question rises whether, when and which intellectual property right issues occur on the content stored at data centres.

Since 1996 there exists a European directive for safeguarding of legal rights of databases [Directive 96/9/EC, OJ L 77]. Under the system of database protection, the structure of the database as well as its content fall within the ambit of the copyright law, provided they qualify as original. The content of the database that lacks sufficient originality, however, falls under the sui generis system of the database law [13]. Art. 7 of the European Database Directive stipulates that if one of the parties- in our case the Information Publishing service provider – has made a substantial investment in either the obtaining, verification or presentation of the contents of the database (thus content collection, access control, maintenance, update and publishing), then the database rights fall exclusively to him or her, i.e. in our case to the Information Publishing service provider. The database rights thus does not retain in the party actually setting up (but not making the investment for) the database (possibly the ASP) on which the Information Publishing service provider is operating. The rights holder of the content on the database then has the exclusive right to permit the extraction and re-utilisation of substantial parts from that content [art. 8 Database Directive]. By means of a licensing agreement permissions for usage of content on data banks can be granted to third parties. The agreed terms that govern the rights and obligations of the parties in a contract, can be effectuated analogous to the intellectual property rights under transactions, namely, through licenses and transfer of rights.

### 3.1.3 DISTRIBUTION

In Information Publishing the ASP will play a crucial role in service delivery. Therefore, it is important to consider whether and to what extent the ASP can be held liable for unlawful distribution of content that is protected by copyrights or database rights and for unauthorised access and use of personal data protected under privacy law.

The answer to these questions is highly dependent upon the context, since matters of liability are to be decided upon the specifics of the individual situation. In any case, the degree in which the ASP is actually involved in deciding upon the content of the Information Publishing process is important for deciding his liability [14]. Clearly, such involvement is not easy to assess, and therefore determining liability is nontrivial and subject to a case by case approach (see also section 5 for a possible technological solution). As a consequence, the measures that must be taken by the ASP to protect copyrights and guarantee privacy cannot easily be defined (see also section 3.3)

Section Four of the European Directive on Electronic Commerce [Directive 00/31/EC, OJ L 178] gives us a bit more context in that it makes a distinction between mere conduit, caching and hosting intermediaries. For each type of service provider, conditions are specified to limit liability. For hosting service providers such as ASPs, which seem relevant for Information Publishing, dispensation is given if the provider does not know or does not need to know that activities or content are unlawful. However, if the ASP or Information Publishing service provider comes to know about unlawful content or transaction, it is required that he removes the content and disables access or functionality.

Therefore, in Information Publishing the following business requirements must be fulfilled:

- The ASP does not take the initiative to distribute content, publishers, Information Publishing service provider and subscribers do,
- The ASP does not decide to whom content is distributed,
- The ASP does not select or modify content or personal details on its own initiative.
- If the ASP or Information Publishing service provider knows of illegal content distribution or access he must take action to prevent that he is held liable.

### 3.2 TECHNOLOGICAL REALISATIONS

The word ‘rights’ in “Digital Rights Management” is a bit confusing. It suggests that DRM has solely to do with legal rights and legislation (which are country specific). Specification of legal rights is only one part of DRM. DRM in addition deals with usage rights, also called permissions (which are not country specific) of users over digital content. So besides managing and protecting permissions, a DRM system must, like any other system, observe the legal rights of its users. Therefore in this paper we will apply the following definition:

*Digital Rights Management is the process of defining, managing and enforcing the usage rights of digital content. The function of DRM also includes that the legal rights are observed of and by all participants engaged in the electronic commerce and digital distribution of content.*

DRM systems allow content providers to distribute content over the Internet in a protected format. Content is encrypted and packaged. The decryption key is usually stored in a license, which is distributed separately. A clearinghouse can be used to authenticate the consumer's request for a license. The protected content can be easily distributed over the Internet, placed on document servers or a Web site for download, since only licensed customers are allowed to actually view the content. DRM systems are useful when digital information is deemed important or sensitive enough to be protected by law. This includes cases when digital content needs to be available to certain people and kept away from others; digital content will be used differently by different kinds of users; digital content needs to be tracked or audited as it moves through a process or organisation.

Digital Rights Management systems should help to enable:

- Confidentiality of content during transport and storage. Protection of digital content by scrambling or encrypting content DRM enables authors and publishers to protect content while sending it over an unsecured network to an unsecured storage device,
- Integrity of content (or content authenticity) to assure that the content is not altered during transport or storage,
- Authentication of the sender and receiver of the content to assure the publisher that the consumer is who he claims to be (a credible consumer) and to assure the consumer that the content he obtains is really published by publisher,

- Authorisation to access the content by the intended (and authenticated) recipients,
- Non-repudiation of the transaction to assure that consumer has really ordered a piece of content (origin) and that publisher really delivered it (receipt).

In general the function of a DRM system is to define, manage and protect the rights over digital content (in this case documents). The translation of this general function into more detailed (and workable) system functionality can be described as follows [15]:

- Packaging of content for exploitation:
  - Definition and declaration of content usage rights in a rights language,
  - Protection of content in order to keep this content confidential during transport and storage (encryption is often used as a solution to provide this protection),
  - Enabling of content tracing (watermarking is often used as a solution to enable this),
  - Enabling fraudulent user tracing (adding a user specific watermark is often used as a solution to enable this),
  - Packaging the above-mentioned into one identifiable digital item.
- Unpackaging of delivered content for usage by means of decryption and extraction of that packaged content by the end-user.
- Usage control of protected content:
  - The interpretation of usage rules and rights associated to the protected content (this is done by the content-viewer on the end-users device),
  - The request for a license to use the protected content,
  - (Payment for this license, this involves: user identification and authentication),
  - Authorisation to consume the content (this can involve the delivery of a license with a decryption-key to the end-user),
  - Exception handling (in case of violation of usage rights).
- Process monitoring of (un)packaging and usage control:
  - Logging of specific events,
  - Feedback of successful download/playback of the protected content, which involves monitoring or metering on the client side that presupposes that end-user has a trusted content-viewer,
  - Tracing for illicit content.

In the Information Publishing business model the above-described DRM system functionality is distributed over the systems of the different actors in the value network (see section 2), i.e. the publisher is responsible for content packaging, and distribution; the Information Publishing service provider is responsible for enriched content and license management, storage and distribution, and the subscribers system is responsible for control on unpackaging and display of the enriched document content (see **Figure 3)**.

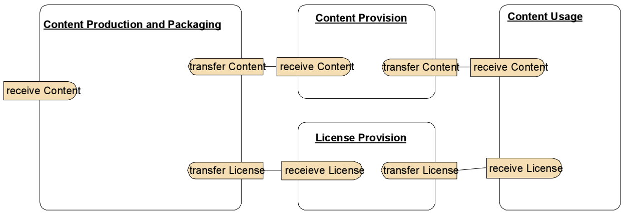


**Figure 3: Functional Architecture of DRM System**

The packaging of content on the publisher's system involves the declaration of content usage rights, the encryption of the associated content, and the generation of a license that contains the decryption key. The DRM client on the subscriber's system uses all this information to display the content. The client side is therefore the most critical part of the DRM system and it is obvious that the publisher needs to have confidence in, and control over, this client side. Besides content display an important part of the DRM functionality on the client side is concerned with the control on content usage (see **Figure 4**).

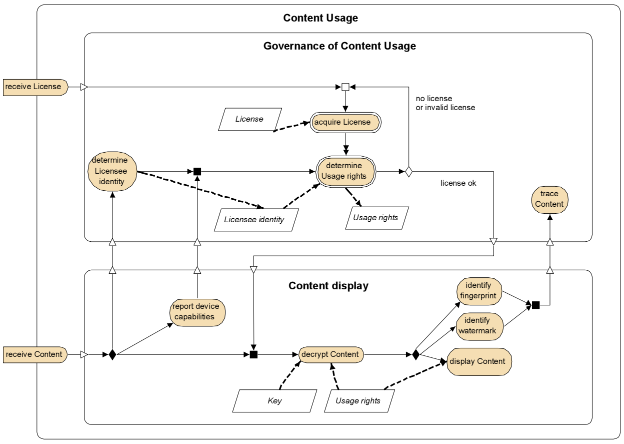


**Figure 4: Functional Architecture DRM at Client-Side**

When a subscriber opens a protected document the identity of the Licensee is determined. This Licensee is mostly a hardware device or software application that is coupled to the subscriber. The publisher or the Information Publishing service provider is aware of this coupling and should therefore also be aware of the legal implications of the monitoring process it performs at the client-side (see section 3.3. for possible conflicts that might arise with privacy concerning the usage behaviour of content). Next to this the capabilities of the content display (and editing) device are reported in order to make sure the device at the client-side can be trusted. Licensee identity and device capabilities are used in the process of determining usage rights as associated with the content and obtaining the proper license. If the license is valid, the key that is stored in it can be used to decrypt the content. Once decrypted the document content can be displayed in the trusted viewer or editor. The usage rights set the possibilities for this viewing and editing (see also section 4).

It has to be remarked that we assume a DRM system in which the end user's system can be trusted because the publisher controls the client side of the DRM system and the content display. This assumption is not very realistic and often criticised [16]. It is also not realistic to expect that DRM systems can guarantee full protection of content; this is also shown by various successful attempts to circumvent the control of DRM systems. There is always an "analogue hole" in a DRM system, i.e. printing, photocopying and scanning of a protected document stays always possible. It is not as bad as it looks like in our case. In Information Publishing the DRM system is used to prevent unwanted usage or distribution of content in a B2B setting. The DRM system is used in a situation where a business relation based on trust exists. Therefore it is not very likely that professional subscribers to Information Publishing services will tamper large volumes of (transacted) document content with their DRM client in order to illegally copy, transact and distribute them.

### 3.3 LEGAL IMPLICATIONS

DRM gives holders of intellectual property rights the opportunity to implement new ways of formatting and distributing their works. However, in implementing these ways ample consideration should be given to the implications under copyright and database law in case the protected work is transacted or transformed (e.g. an abstract of the document is made, or the document's content is portioned). In particular having regard of the fact that various parties participate in the value chain and are thus potentially involved in transforming protected documents, different parties may become right holders to the different variations and formats in which a document is available. For example, the original author of a document may be right holder to this document, but the Information Publishing service provider holds the copyright in an abstract it has made on the basis of the original document. Also, the various participating partners should agree on the conditions under which documents can be transformed, viewed and printed. In other words, the parties should take careful consideration of contractual clauses that stipulate the various rights and responsibilities of the partners in the digital rights management system (see section 3.1). Technology could complement the contractual provisions in that it embeds copy control flags indicating whether copying, altering, viewing and printing of the document is authorised (see section 3.2 and section 4).

However, intellectual property rights are not the sole legal dimension that should be dealt with. In developing digital rights management in information publishing careful thought should be given to various other legal implications. Clearly the application of digital rights management for the protection of intellectual property rights is most likely to intersect and to conflict with other interests protected by law, such as the free flow of information, freedom of communication, innovation, free speech and privacy protection. Developments in the European Union as well as the United States show that the broader societal implications of innovation in the area of digital rights management are closely followed by policy makers.[4] If licensing by means of technological instruments such as digital rights management systems becomes a more common way of information distribution, it could lead to potential conflicts with the underlying goals of intellectual property law (i.e. balancing the interests of rights holders and society). Policy makers thus deliberate the possible impact of the introduction of digital rights management on the position of authors, publishers, end users and the public in general.

Aside from questions related to balancing the various interests at the level of national and international policy makers, the individual businesses that develop and implement digital rights management systems are also faced with the legal implications of their dealings. Depending on the specifics of the business model developed for the distribution of digital information, legal issues related to privacy, identity management, liability and security should be contemplated.

First, the very concept of digital rights management is that it links right holders and publishers with subscribers. It provides for a mechanism to e.g. monitor the exact actions of a subscriber in order to enable the assessment of payment due by the subscriber. Hence the system tracks an individual's usage of copyrighted material by registering the name of the subscriber carrying out a transaction, the time and data of this transaction, etc. (see section 3.2). The implication of tracking and logging such information is that these dealings come within the ambit of international data protection rules as laid down in the 1995 European Personal Data Protection Directive and

[4] National Research Council, 'The Digital Dilemma: Intellectual Property in the Information Age', Washington D.C. 2000. European Directive 2001/29, 22 May 2001, O.J. L 167/10.

implemented in the various member states.[5] Consequently, the legal rules require among others that subscribers are informed in advance about the personal data being processed and that the adequate (technical and organisational) security measures are implemented to protect the personal data within the value chain of the rights management system.

In linking right holders and publishers with subscribers, the Information Publishing service provider may contemplate diverse architectures and models for on-line identity management. Clearly, effective and efficient rights management stresses the importance of user identification and authentication, also in the light of combating identity theft. However, the interests of privacy protection emphasise possibilities for pseudonyms and partial anonymity. Thus, the need to control the dealings of an individual and identified subscriber should be balanced with the minimisation of data collection as well as the track of the individual's dealings. Here, an architecture which incorporates the use of digital signatures may offer solutions. This, however, raises questions about the legal validity of such signatures and the position of certification authorities. Will digital signatures be admitted as evidence and if so, what will be the evidential value of transactions identified by means of digital signatures? Uncertainty as to the status of digital signatures can be an obstacle to the implementation of an architecture incorporating digital signatures. Contractual solutions between the partners in a rights management system cannot remove these legal impediments completely. Therefore, digital (and more broadly electronic signature) legislation and regulations concerning related matters have been designed by different countries, international organisations and the European Union in order to meet the expectations and needs of the digital market.[6] Under the new legal rules, security parameters indicating authentication, confidentiality, data integrity and non-repudiation service levels along the information publishing chain remain of utmost importance. Hence, such parameters should be addressed while contemplating various architectures and models for on-line identity management.

Aside from the organisational and technological implications of the applicable legal rules, consideration should be given to the formulation of contractual clauses that stipulate the various rights and responsibilities of the partners in the digital rights management system. Publishers, Information Publishing service provider, ASP and subscribers should thus address liability parameters in case intellectual property rights are infringed during the distribution and use of works within the value chain. The Information Publishing service provider can for example be liable whenever it permits unlawful changes and adaptations in copyrighted material. Also, accountability and liability issues in case of e.g. network and application failures, or unauthorised transactions on document content should be dealt with in contractual provisions [10].

Summarising, we may conclude that various implications of applicable legal regimes (e.g. copyright and privacy) should be simultaneously addressed while contemplating architectures and business models for digital rights management. In addition, the various partners in the value chain should give careful consideration to the contractual dimension.

## 4. DRM AS ODRL-COMPLIANT SERVICE

Nowadays, most DRM companies[7] offer integrated solution of a limited number of DRM aspects, such as storage and distribution security. As noted in previous sections DRM, however, involves more than security issues. For the implementation of DRM on top of novel Information Publishing service components, new standards, like XrML and ODRL, are indispensable. Both languages allow the expression of terms and conditions on the usage of digital content in an XML language. The XrML language, aka Digital Property Rights Language (DPRL), consists of a core specification, which allows the expression of permissions on content. An extension of the this core is available, which enables the expression of our business model for content usage in XrML. Unfortunately, XrML is ContentGuard proprietary. However, XrML is supported by the ContentGuard software development kit (SDK)[8] allowing easy development within the scope of XrML.

ODRL comprises an extensible open language and vocabulary (data dictionary) for the expression of DRM terms and conditions over any kind of content including permissions, constraints, obligations, conditions, and offers and agreements with rights holders. ODRL, roughly speaking, captures the capabilities of the XrML specification language and its extensions into one standard. In contrast to XrML ODRL also support refinements concerning constraints to the transactions that are carried out on document content (for example different policies for viewing and printing). It also has more refined capabilities to express our Information Publishing business model. This allows the definition of per-use, pre-paid and post-paid payment options for content usage, but also the distribution of rights and revenues with respect to content usage over the right holders can exactly be specified. Thus ODRL truly supports financial and legal clearing to ensure effective DRM and therewith Information Publishing service

[5] European Directive 95/46/EG, 24 October 1995, O.J. 1995, L 281/31.

[6] http://www.rechten.uvt.nl/simone/ds-lawsu.htm

[7] http://www.sealedmedia.com

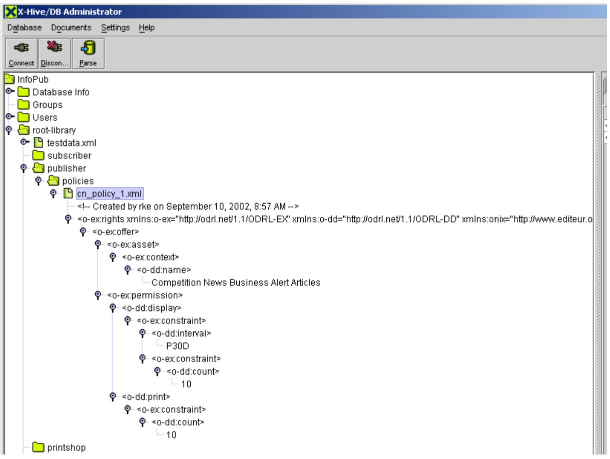
[8] http://www.contentguard.com

provisioning. The latter capabilities even extend the links between publishers and subscribers to other third parties.

For the implementation of our Information Publishing service we used ODRL as a technological instrument for expressing mainly permissions and constraints. The refinements made in ODRL are exactly in line with the accounting options available on our existing Inforamtion Publishing service platform [1], on which all services are developed and deployed. The platform provides non-repudiation on transactions and enables digital identification of users. Both properties are pre-requisites for credible usage of ODRL, and, even stronger, for credible support of DRM.

Normally, an ODRL policy is determined by a publisher and is enforced by an Information Publishing service provider during the usage of content by a subscriber (see section 2 and section 3). The actual enforcement of the policy is handled by a separate software component.

The ODRL policies defined on content (in our case mainly documents) in the system are stored in an XML database. This database serves as the storage back-end for all Information Publishing services and allows easy querying and manipulation of XML document. By using the mechanism of XLink[9], a single document or set of documents is bound to an ODRL policy that is stored in the database. We call this a template (see **Figure 5**). By using XLink a weak coupling is created between the policy and the document. Thus, it is allowed to attach different or new policies to the documents in the system after they have been published. When a document is used, the software component in charge of enforcing the policy retrieves the policy related to the document by resolving the XLink and applies it to the action the subscriber wants to perform.



```
InfoPub
  Database Info
  Groups
  Users
  root-library
    testdata.xml
    subscriber
    publisher
      policies
        cn_policy_1.xml
          <!-- Created by rke on September 10, 2002, 8:57 AM -->
          <o-ex:rights xmlns:o-ex="http://odrl.net/1.1/ODRL-EX" xmlns:o-dd="http://odrl.net/1.1/ODRL-DD" xmlns:onix="http://www.editeur.o
            <o-ex:offer>
              <o-ex:asset>
                <o-ex:context>
                  <o-dd:name>
                    Competition News Business Alert Articles
              <o-ex:permission>
                <o-dd:display>
                  <o-ex:constraint>
                    <o-dd:interval>
                      P30D
                    <o-ex:constraint>
                      <o-dd:count>
                        10
                <o-dd:print>
                  <o-ex:constraint>
                    <o-dd:count>
                      10
    printshop
```

**Figure 5: ODRL Specification Used in XML Database**

In essence the policy is a template bound to documents with certain rights on document usage. This implies that when a document is used, an instantiation of the template must be created for this document. This instance comprises the state of a certain policy applied to a document in time. However this introduces some redundant storage that may lead to inconsistencies.

XPath[10] (or the deprecated XPointer) can be used for addressing specific elements of a policy. XSLT can be applied for specific projections on ODRL policies, thereby, for example, enabling joining an instantiated policy and its template. This projection can be used to make decisions for enforcing the policy.

With regard to the granularity of rights enforcement in ODRL, we propose an extension to the language that also supports:

- Policies on sections of documents,
- Policies on pages of documents.

The Information Publishing service developed accounts the viewing and printing of separate pages and sections - you pay for what you read or print, not the complete document - [1]. ODRL however applies to documents, not to pages and sections. In a rather ad hoc way we have therefore applied segments of the ODRL syntax tree to the separate pages and sections of documents in the system, instead of applying ODRL to the whole documents only. In concrete, the agreements in ODRL on the usage of the content are now specified at a page/section level instead at the document level.

Besides the lack of support for document segments, no support for the expression of rights on transformations of the original content is available in ODRL. For example, the rights on a (machine generated) summary or translation of a document are not supported. For a transformed document, a new policy has to be defined, clearly identifying the right holders. However for these transformations a number of questions with respect to ownership of the generated content are still unanswered. Who owns the rights on the summary, besides the author of the original text, if it is machine generated? Do the additional rights belong to the software company that developed the summarisation tool or the individual that uses the software? And what if the software user needs to provide some sort of domain knowledge to the summarisation tool to create domain-specific summaries? For a discussion on these matters the reader is referred to section 3.3.

In our current use of ODRL and the use of it in general, the policy is not embedded in the document it belongs to (see also Ted Nelson[11]). However, embedding the policy

[9] http://www.w3.org/TR/xlink

[10] http://www.w3.org/TR/xpath

[11] http://xanadu.com

in the document content could ensure the proper use of the document according to the ODRL-policy, if the document is distributed by itself.

## 5. CONCLUSION AND DISCUSSION

As DRM is an essential business issue in Information Publishing we investigated how to integrate DRM in our business model as well as how to realise software components that specify and enforce digital rights of enriched document content. We analysed impacts of Information Publishing, in particular DRM and advanced document management and presentation, on other legal issues, such as privacy.

The above investigation and analysis show us that business model choices and legal norms are highly intermingled. DRM appears a key instrument in introducing new ways of formatting and distributing works protected by intellectual property rights. However, in preventing or favouring certain actions with copyrighted works, DRM also most likely intersects and conflicts with other interests protected by law, such as the free flow of information, freedom of communication, innovation, free speech and privacy protection. Thus it is of high importance that the business scenarios that apply rules and norms through technology are open and transparent, thus allowing public control over such technology. Proactive enforcement by means of technology and thus tracking, logging and hence controlling all - personalised - actions on an information publishing service should be counterbalanced with fundamental rights of individuals, such as privacy and the free flow of information. Hence, it is to be expected that one of the big themes affecting future developments on digital rights management is setting the borderlines between the different interests at stake.

Aside from this, the different partners in the DRM business model should give ample consideration (preferably by means of contractual provisions) to their respective rights and obligations as regards the use and transformation of copyrighted works.

The above legal remarks about the entanglement of business and law seem to suggest that resolving conflicts between intellectual property and other legal issues like privacy are hardly feasible. However, integration of document categorisation systems [17] and subjective legal systems [18] might cope with such entanglements in the realm of Information Publishing. The document categorisation systems could dynamically enrich documents and associate to them over their life-time digital rights and their allowed enforcement measures. Integrating such a categorisation system with a subjective logic system could then make explicit the particular DRM system components not jeopardising other legal aspects of Information Publishing like privacy.

## REFERENCES

[1] A. Salden, H. ter Doest, R. Kersemakers & D. Slijp, Information Publishing on FRIENDS[12], Proc. SSGRR 2002s Conf. on Advances in Infrastructure for e-Business, e-Education, e-Science, and e-Medicine on the Internet, l'Aquila, Italy, 2002.

[2] E. McCoyd, Digital rights management for E-books: publisher requirements (Association of American Publishers, Inc., 2000).

[3] F. Hoque, D. Kutnick and T. Trainer, E-Enterprise: Business Models, Architecture and Components (Cambridge University Press, 2000).

[4] C. McCaskill (Ed.), A Guide to the ASP Delivery Model, Application Service Provider Industry Consortium (ASPIC) Best Practices Committee, April 14, 2000.

[5] C. A. Gunter, S. T. Weeks & A. Wright, Models and Languages for Digital Rights, InterTrust Star Lab Technical Report STAR-TR-01-04, March 2001.

[6] R. Ianennella, DRM Architectures, D-Lib Magazine, 7(6), 2001.

[7] E. Carmel & E. Collins, The impact of international copyright management and clearance systems on multimedia markets, Telematics and Informatics 14(1), 1997, 97-109.

[8] L.M.C.R. Guibault, Copyright Limitations and Contracts. An Analysis of the Contractual Overridability of Limitations on Copyright, Information Law Series 9, 2002.

[9] A. Torrubia, F. J. Mora & L. Marti, Cryptography regulations for E-commerce and digital rights management, Computers & Security, 20(8), 2001, 724-738.

[10] S. Angelov & P. Grefen, A Framework for the Analysis of B2B Electronic Contracting Support, 4th Edispuut Conference - Multidisciplinary perspectives on electronic commerce, 2001.

[11] M. Nimmer, D. Nimmer, Nimmer on Copyright – A Treatise on the Law of Literary, Musical and Artistic Property, and the Protection of Ideas, (Mathhew Bender & Co., 1999).

[12] J.E.J. Prins, Contracting in an on-line marketplace, *Emerging Electronic Highways. New Challenges for Politics and Law*, (eds. V. Bekkers, E.J. Koops, J. Nouwt), Kluwer Law International, 1996.

[12] http://www.ssgrr.it/en/ssgrr2002s/papers/47.pdf

[13] E. Kindt, Ownership of Information and Database Protection, *A Decade of Research @ the Crossroads of Law and ICT*, (eds. J. Dumortier, F. Robben, M. Taeymans), Larcier Publishers 2001.

[14] E.J. Koops, J.E.J. Prins & H. Hijmans, ICT Law and Internationalisation. A Survey of Government Views, (Kluwer Law International, 2000).

[15] E. J. Goedvolk et.al., Digital Rights Management[13], State of the Art report the Uluru project, Telematica Instituut, 2002.

[16] B. Schneier, The Futility of Digital Copy Prevention[14], Crypto-Gram newsletter, 2001.

[17] A. Salden & M. Kempen, Business Information and Knowledge Sharing, In IASTED International Conference Information and Knowledge Sharing, IKS 2002, St. Thomas, Virgin Islands, USA, November 18-20, 2002, in press.

[18] A. Joesang & V.A. Bondi, Legal reasoning with subjective logic, Artificial Intelligence and Law, 8, Kluwer Academic Publishers, 2000, 289-315.

[13] https://doc.telin.nl/dscgi/ds.py/Get/File-18920

[14] http://www.counterpane.com/crypto-gram-0105.html#3