



<http://virtualgoods.tu-ilmenau.de/2004/>

Reviewed Papers

Virtual
Page
Numbers

Session 1: Watermarking for Virtual Goods

1. **StirMark and profiles: from high end up to preview scenarios** 1-12
Andreas Lang, Jana Dittmann,
http://virtualgoods.tu-ilmenau.de/2004/virtual_goods_2004_LANG_DITTMANN.pdf
2. **Synchronization of Video Watermarks for Oblivious Detection after Geometrical Distortions** 13-23
Uwe Wessely
<http://virtualgoods.tu-ilmenau.de/2004/wmsync-VG04.pdf>
3. **Complexity Optimization of Digital Watermarking for Music-On-Demand Services** 24-35
Martin Steinebach, Sascha Zmudzinski
http://virtualgoods.tu-ilmenau.de/2004/watermarking_music_on_demand_steinebach_vg2004.pdf

Session 2: Culture and Business for Virtual Goods

4. **On-line music distribution: a case study** 36-46
Francis Rousseaux, Alain Bonardi, Romain Poncelet
http://virtualgoods.tu-ilmenau.de/2004/On-linemusicdistribution_a_case_study.pdf
5. **Secure Music Content Standard - Content Protection with CodeMeter** 47-58
Marcellus Buchheit, Rüdiger Kügler
http://virtualgoods.tu-ilmenau.de/2004/SecureMusicContentProtection_VG2004.pdf
6. **Towards a Secondary Market for Virtual Media - A Theoretical Approach** 59-71
Lutz Niehüser, Johannes Bräutigam
<http://virtualgoods.tu-ilmenau.de/2004/SecondaryMarket.pdf>

Session 3: The Value of Virtual Goods

7. **Modelling the eVerlage Payment Protocols** 72-83
Uwe Petermann
<http://virtualgoods.tu-ilmenau.de/2004/EVerlagePaymentProtocols.pdf>
8. **How to Pay in LicenseScript** 84-90
Cheun Ngen Chong, Sandro Etalle, Pieter Hartel
<http://virtualgoods.tu-ilmenau.de/2004/ceh04vgoods.pdf>
9. **Personalized Previews: An Alternative Concept of Virtual Goods Marketing** 91-100
Patrick Aichroth, Stefan Puchta, Jens Hasselbach
http://virtualgoods.tu-ilmenau.de/2004/personalized_previews.pdf

Session 4: Digital Protection and Digital Rights for Virtual Goods

10. **Enabling Digital Content Protection on Super-Distribution Models** 101-112
Carlos Serrão, Joaquim Marques
<http://VirtualGoods.tu-ilmenau.de/2004/VG2004-EDCP-SD-OSDRM.pdf>
11. **Licensing Structured Data with Ease** 113-124
Yee Wei Law, Cheun Ngen Chong, Sandro Etalle, Pieter Hartel, Ricardo Corin
<http://VirtualGoods.tu-ilmenau.de/2004/law04licensing.pdf>
12. **Interoperability Challenges for DRM Systems** 125-136
Andreas U. Schmidt, Omid Tafreschi, Ruben Wolf
http://VirtualGoods.tu-ilmenau.de/2004/Interoperability_Challenges_for_DRM_Systems.pdf

INTEROPERABILITY CHALLENGES FOR DRM SYSTEMS

ANDREAS U. SCHMIDT[†], OMID TAFRESCHI^{*}, RUBEN WOLF[†]

ABSTRACT. Large scale Digital Rights Management (DRM) systems are close to deployment in various areas. However, interoperability problems associated with DRM based content distribution systems encompassing many business models, consumer use cases, content and device types, have not been regarded in detail. On grounds of an analysis of these issues we argue that comprehensive DRM poses very special interoperability challenges, and advocate the utility of intermediary roles for viable DRM solutions.

1. INTRODUCTION

For a time, the transition of markets to the Internet seemed to prophesise doom for intermediary businesses like wholesalers, agents, retailers, warehouses, and so on. In fact, the prime economical role of intermediaries, namely to reduce transaction costs through a combinatorial reduction of necessary contacts between buyer and seller, was lost since the cost of a single electronic transaction would eventually tend to zero. That deemed a compelling argument for the case to many, and the phenomenon-to-be was aptly named *disintermediation* [1]. But new business ideas apparently unfolded quicker than this effect — there is no need to name the prominent examples of Internet auction houses and book resellers. The Internet became an enabling technology for these new business models, spurring the inverse process of *reintermediation* for a wide range of distribution channels for physical goods.

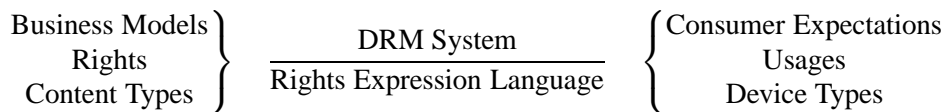
The distribution of virtual goods [2] over any kind of electronic network and based on sophisticated DRM systems seems to be bound to repeat this story. The virtual non-existence of video on demand systems operated directly by Hollywood studios and the thus far limited success of music portals owned by record companies are telling. In stark contrast is the successful launch of intermediary services like Apple's iTunes portal, and more recently myCokemusic.com. Although these relative successes can be attributed in part to better usability and less restrictive licence conditions [3], they also bespeak a more fundamental problem: A user navigating the portal of a single owner of digital content will always see only a fraction of the media world he is interested in. The arising need for content federation (the integrated access to content from various sources through a single point of contact, beyond the trivial level of meta search-engines) is perhaps the most commonplace instance in which the interoperability of DRM systems becomes an important issue, if not an enabling factor.

In the following Section 2 it is analysed how DRM's pretence to enforce usage policies for virtual goods over the whole value creation chain, together with demands of content owner and consumer, factor into the complexity of the interoperability problem, and we show that DRM systems have specific traits increasing the practical import of it. Section 3 exhibits the problem's imprint on what are to be the informational fundaments of DRM systems, that is, the various brands of rights expression languages (RELs). It is shown that the advanced capabilities of these languages can entail fastidious DRM tasks, not all of which are covered by the functional roles of the classical DRM architecture presented in Section 4. We proceed with an advocacy of content distribution systems based on DRM models and architectures with central roles for intermediaries — what we call *intermediated DRM* (IDRM) — and the high level tasks that will fall to such an intermediary. To further corroborate the argument for IDRM, some non-technical issues are highlighted in Section 5, where we also point to the enabling character of intermediaries for completely new business models for the diffusion of protected virtual goods. Section 6 offers an outlook to the probable advent of IDRM solutions in various domains, most notably for mobile applications.

Addresses: [†]Fraunhofer-Institute for Secure Telecooperation, Dolivostraße 15, 64293 Darmstadt, Germany; ^{*}Technische Universität Darmstadt, Fachbereich 20, FG Sicherheit in der Informationstechnik, Wilhelminenstraße 7, 64283 Darmstadt, Germany.
e-mail addresses: [†]{aschmidt,rwolf}@sit.fhg.de; ^{*}tafreschi@sec.informatik.tu-darmstadt.de.
Paper URL: http://VirtualGoods.tu-ilmenau.de/2004/Interoperability_Challenges_for_DRM_Systems.pdf

2. COMPLEXITY FACTORS FOR INTEROPERABLE DRM

In a division between *content owner* as the entity which sets rights for content and wants them enforced when content is distributed according to a business model, and *consumer* as the one who is willing to acquire content and to use it, a coarse categorisation of factors escalating the complexity of a comprehensive DRM task can be given as shown below.



This can be understood as follows: Various business models may be formulated using a multitude of (combinations of) rights terms, in reference to a number of content types. In turn, individual expectations of consumers may be fulfilled through different usages of the content on a number of device types.

From this elevated perspective, even the concrete entities of content and device types are understood as generic terms comprising categories such as entertainment/educational, media formats (audio/visual/textual and others) and underlying data formats on the one hand, and on the other hand devices for public use vs. private ones, mobile and stationary devices, and finally brands, makes, and models. More often than not, expectations about the variable range of the six factors are encoded in informal business and/or technical requirements [4, 5]. Let us consider two more concrete examples.

Consumers of protected content have considerable requirements. Especially with respect of content usage, portability of content as one aspect of usability is of high interest. Users want to use the purchased protected content on all devices their, as it usually is for non-virtual goods. In turn, the desired usages may vary between those devices conditioned by their respective capabilities. Yet, since portability of content conflicts with the base idea behind strong DRM,¹ DRM solution providers have to find ways to balance both the consumer's and the content owner's requirements. From the content owner's side, a very important top-level requirement is the ability of a content distribution system to support *price discrimination*, as was stated clearly in [6]: "A successful business model should not force copyright holders to charge the same price to all buyers ...". The most familiar example of price discrimination is the sequential marketing of movies in theatres, pay-TV programmes, through DVD/video rentals, and finally by DVD sale. These business plans are often based on the ability to sequentially but separately release a work in various forms. Content type and licence model will vary over this temporal sequence, which in fact consists of a number of subsidiary business models implicitly or explicitly targeting distinct customer groups. No DRM system is known that could support price discrimination schemes of this complexity in the digital realm.

So far the above factors provide a purely combinatorial measure for the space of situations an interoperable DRM system has to deal with. But do these numbers count? There might be boundary and side conditions which limit the practical attainability of some situations, e.g., incompatible combinations of content and device types, or usages and business rules. But although the three abstraction levels are surely interdependent on both sides, no one-to-one relation between, say, business models and usage rules exists. Simple multiplication of these quantities yields in any case an upper bound for the extension of the DRM task space. More important here is the often neglected issue of the *fine granularity* of usage rules that can be formulated with RELs (see below), and of individual usage desires in a mass market with millions of customers. More than the individual factors enumerated above, this is what powers the fundamental *tension field* in which a DRM system operates. That the restrictions imposed by usage rules and consumer expectations are often in conflict, is a commonplace. What raises this to a serious problem is the binary decision logic of classical DRM, which is derived from the established methods of access control: If a user action is not allowed it is simply blocked. Innocuous as this might be from the viewpoint of content protection, it exhibits the tendency of DRM systems to frustrate customers. For, the finer the granularity with which allowed usages are delineated, the more likely is an individual's usage demand to fall outside of their scope. Classical DRM has no means to direct the user to an allowed action which is adjacent and similar to its desired one.²

¹Strong DRM refers to copy protection of content, while weak DRM refer to content tracking, and tax and royalty systems.

²Of course, if either the fine granularity of rights is not utilised, or the individuality of usages is grossly neglected, the DRM tension field remains a potentiality.

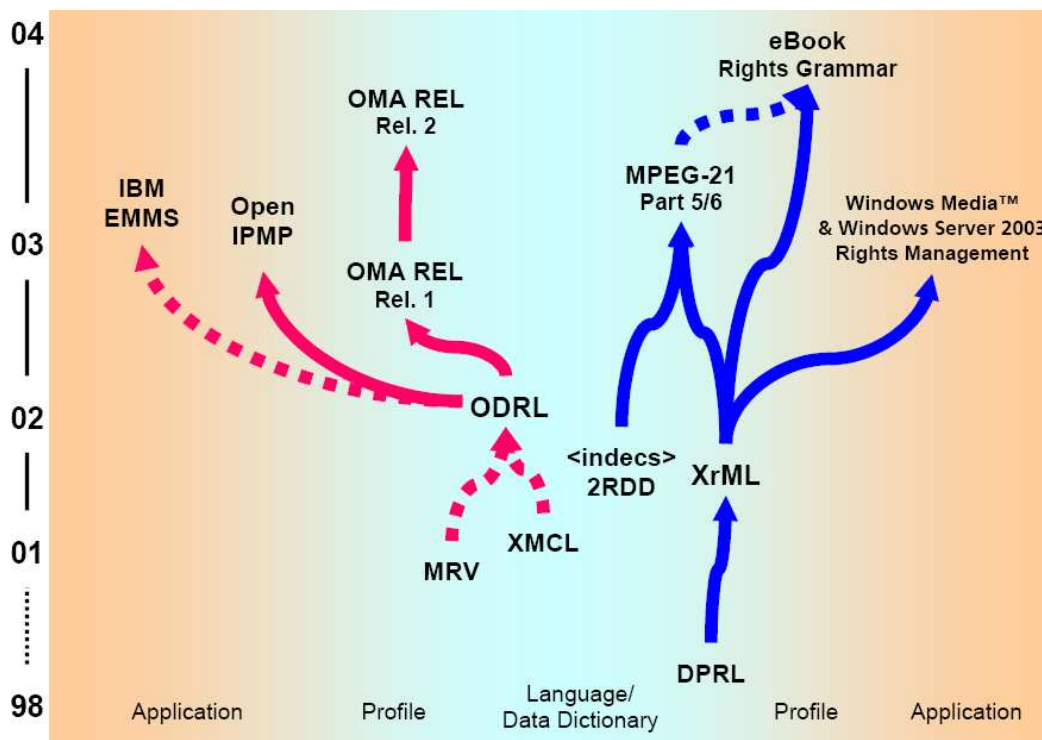


FIGURE 1. A Genealogy of Rights Expression Languages.

3. RIGHTS EXPRESSION LANGUAGES AND INTEROPERABILITY

A Brief Genealogy. The history of data formats for the expression of digital rights and licences is short, yet already shows signs of consolidation. This can be ascribed mainly to two factors. First, the IT industry has at an early stage recognised the need for interoperability in DRM, and, driven by converging interests, major players forced streamlined standardisation procedures such as the Open Mobile Alliance has carried out and is still pursuing. Second, the standardization was fertilised by the adoption of open standards, in particular XML as a syntactic foundation of RELs.

Rights Expression Languages based on XML have a common structure. They consist of an XML grammar (a Schema), also called the language concept [7], that describes the basic grammar for the expression of rights terms and conditions, and their relation to the assets in question and the parties involved. The language concept is complemented by a rights data dictionary (RDD) which is a thesaurus containing the vocabulary that can be used in rights, together with a description of its semantics. Such an REL can then be turned into a domain-specific language profile by choosing a subset of grammar and RDD, and possibly defining additional, custom semantics. Finally, such a profile or the REL itself becomes implemented in applications.

Figure 1 shows the two existing main stems of XML based RELs ordered along the structural lines sketched above and a coarse timeline. The information in this diagram is taken from various sources, good starting points are [8, 9]. Sprouting from two base standards, Open Digital Rights Language ODRL [10], and eXtensible rights Markup Language XrML [11], two viable plants evolved, which we now describe in that order. ODRL is an open standardization initiative aiming to develop a freely available REL for DRM. Its latest release version 1.1, dated from August 2002, has thus also been co-published by the W3C as a Note, although the chartering of a DRM/Rights Language activity remains an open issue within the W3C. ODRL is influenced by RealNetworks' eXtensible Media Commerce Language (XMCL), an earlier version of which merged with to Nokia's Media Rights Voucher (MRV) to form the ODRL standards track in the fall of 2001. XMCL is still under independent development as an open standard [12]. Main industrial promoters of ODRL are RealNetworks and Nokia, and the latter company was perhaps also a driving force behind the choice of ODRL as a basis for the language profile defined in OMA DRM Releases 1 and 2 as a proper restriction of the ODRL 1.1 language concept and data dictionary [13]. The OpenIPMP Open Source Rights

Management Project developed by ObjectLab [14] provided one of the first DRM reference implementations comprising ODRL. The proprietary REL used in IBM's Electronic Media Management System EMMS also shows influences by ODRL. The submission of ODRL as a candidate for the REL incorporated in MPEG-21 failed (see below).

In 1996, Xerox PARC developed the Digital Property Rights Language DPRL. Version 2.0, in which the language format was changed from Lisp to XML, dates from November 1998, and was rechristened XrML after Xerox and Microsoft funded the joint venture ContentGuard. XrML reached stability with version 2.0 of November 2001 and version 2.1 of May 2002 has been submitted to OASIS with the explicit goal to serve as "the basis in defining the industry standard rights language". XrML, although now developed under the sole responsibility of the OASIS Rights Language Technical Committee (TC, see [15]), is still copyrighted by ContentGuard, and industrial use has to be licenced with that company. This issue, and other questions concerning ContentGuard's patent portfolio (alleged claims that would pertain to any rights language) have led to vivid discussions in the IT community. However, it can be speculated that a freely available version of XrML will appear under the auspices of OASIS, since Robin Cover, one of the prime critics of ContentGuard's licence on XrML, is a member of the OASIS Rights Language TC. The XrML language concept is complemented by a comprehensive data dictionary developed by the <indec>2RDD consortium based initiative, supported by a group of major content owners (MPA, RIAA, IFPI and others) and technology companies (in particular ContentGuard), and managed by Rightscom. The combination of XrML with <indec>2RDD was successful in its application to become the REL for the MPEG-21 [16] standard, where it is incorporated as Sections 5 (RDD) and 6 (language concept) which currently have Final Draft International Standard status (as of July 29, 2003). A language profile of XrML for a specific application domain will be defined by the Open eBook Forum (OeBF, see [17]) in their upcoming DRM standard for eBooks. The eBook Rights Grammar will be a close adaptation of the MPEG-21 REL and OeBF has set up procedures to ensure compatibility with that standard. Support for the MPEG-21 REL is to be included in OpenIPMP.

ODRL and XrML are competing approaches. They differ in spirit and availability, which is open source for the former, as opposed to copyrighted for the latter. Furthermore, the industry backing of the two languages is different, Nokia, other mobile communications industries, and RealNetworks support ODRL, while Microsoft, Xerox, and content providers such as MPA, RIAA and IFPI (through <indec>2RDD) promote XrML and its usage. The latter cartel has proven to be on the longer lever in two important cases: The selection of XrML/<indec>2RDD for MPEG-21 and the decision to use XrML in the forthcoming REL for eBooks. That XrML is also the basis for the Windows Media Series 9 DRM, and for the comprehensive document rights management in the Windows Server 2003, using two different language profiles, comes as no surprise.

XrML defines itself as "the digital rights language for trusted content and services". This definition neatly encompasses the primary difference between ODRL and XrML. Both rights expression languages contain concepts for rights holders, users, permissions, and constraints on permissions. XrML differs from ODRL however in specifying XML standards and technologies for the management of rights. It therefore requires trusted systems for implementations, providing end-to-end support for DRM, which requires that the serving system and the client system can actively communicate and support rights transactions between the two parties. XrML supports opacity in rights transactions. Constraints to rights, such as limits on the number of unregistered uses for software can be hidden from the end user in an encrypted location on the user's computer. ODRL, on the other hand, makes no assumptions about how rights will be managed and enforced.

For the present discussion of DRM interoperability the lesson learned from the REL evolution is that at least two conceptually different RELs are established and will coexist at least on the short to medium term. But also the base standards of ODRL and XrML are already subdivided into families of application domain specific profiles. That this may create interoperability problems has in part been acknowledged by standardisation bodies. In such cases it is a common proceeding to establish so called "liaisons" between these organisations, as for instance between MPEG-21, the open eBook Forum and the OASIS Rights Language TC, to monitor and where possible, harmonise their standards. While this might be helpful for sure, interoperability problems have proven themselves too pertinacious in the past to hope for universal solutions. Let us now turn to some specific examples.

Examples for Interoperability Tasks. The generic trend towards content federation in portals, distribution centers, and catalog systems, and the diversity of the business models of the owners of diverse content types renders scenarios foreseeable in which a content distribution system based on DRM has to cope with a multitude of RELs and licence models expressed in them. Let us assume for the sake of concreteness that a content owner comes with complex rights formulated in (a profile of) XrML while the DRM system's target REL, i.e., the REL that the rights enforcement components can process, is less capable.

For starters, consider the most basic task conceivable. The above mentioned diversity is of import also for the data formats underlying rights and content transport, entailing the most primitive interoperability problem of DRM systems and tied to their communication architecture, independently of the rights language used. Namely, *repackaging and format conversion* is needed if the content comes as a *secure container* [18], i.e., a cryptographically protected package containing the asset and the rights, yielding access only to authorised parties. The WMA format of the Windows Media Player is an example. Distribution through a system that operates on the client side with separate rights and content, like, e.g., the OMA Release 1 and 2 standards for the mobile domain envisages [19, 20], requires the distributor to have reading access to the container in order to separate content from rights. While the content format might be easily converted, the rights in the secure container must in this case address two parties: The distributor must be granted the right to issue rights to the content to a user. Such a semantics is in fact encoded in the **Issue** XrML core right concept [11, Section 5.4.2]. The user rights may then be transformed into the target REL as appropriate, or transferred as a separate piece of content with unlimited access rights, leaving rights processing to the device in a form of rights tunneling. An alternative to repackaging is of course tunneling of secure containers, disregarding the DRM architecture of the distribution system.

For a second example, note that *location based rights* can be expressed with fine granularity using the **Territory** concept from the XrML standard extensions [11, Section 6.1.11]. Yet, while for instance ODRL itself contains a single element `pLocation` to specify the physical location within the context of an entity, this is not semantically bound to the location at which rights can be exerted as in XrML, and less capable profiles of ODRL may not even contain that expressivity. Many business scenarios from the educational (classroom) and entertainment (theatre) domains are imaginable in which content is to be distributed to devices at specific locations only. If a content distribution system was to enforce such rights it would necessitate a geographical position information provider to check for locations in the allowed domain and reissue grants in the target REL upon success. This requires two separate agreements between DRM system operator³ and content owner: First and necessarily, they must agree that locations are specified based on, or at least within the resolution of, the DRM system's positioning information provider. Second, they need to specify how the remaining permissions are to be translated in the given context. For instance, unlimited rendering rights on the content owner's side may translate into time limited rights, to cater for the latency time with which the system checks a device's location. In addition, there is an emerging requirement from content providers for support of DRM in business-to-business (B2B) scenarios [21]. In B2B, the buyer may be an enterprise, organisation, institution or some other group of individuals, while the consumer of the material is a set of individuals of this group. The main point here is to grant rights to a set of individuals as part of a single financial transaction. Many new business models are conceivable, such as support for unlimited access to the content at a fixed price for a fixed period by any number of individuals, or by a specific number of individuals to be determined by an authority within the purchasing entity. The specification of location based rights and the use of the individual's location information during DRM enforcement allows controlled rendering of protected content by individuals within the purchasing entity and thus to fulfill the organisation's requirement for flexibility and portability of protected content.

Payment functionality is often regarded to lie outside the scope of DRM proper, and therefore payment expressivity is not contained in certain REL profiles.⁴ Payment primitives are numerous in the XrML standard extensions [11, Section 6.2]. A typical example is the **PaymentPerUse** condition concept, meaning that a right may be exercised upon payment of a fee for each use. An analogous construct is available in the ODRL data dictionary. Such a constraint could be implemented using a payment service provider's external charging functions, such that, in the simplest case, for each payment acknowledged by the user and registered by

³As a self-evident example, the operators of cell based mobile networks have rather direct access to information about the geographical location of devices by cell addressing, or even finer using triangulation in areas with dense cell distribution.

⁴The OMA DRM Release 1 REL is an example, although ODRL has such semantics.

the billing system, a right for a single use of the content is issued. Given the delay between registration of a due payment and its settling, an accord between content owner and DRM system operator might be required in such scenarios, to establish a separate business relation in which the operator guarantees for a certain due amount and/or number of user payments.

A last example: XrML already in its core allows an issuer of a right to revoke the signature associated with a right using the **Revoke right** concept [11, Section 5.4.3]. This allows, amongst others, the construction of business scenarios such as “Offer valid for a limited (unspecified) time”. Many systems for the dissemination of revocation information (for instance, certificate revocation lists in PKIs) involve a periodic polling for new revocations. To support this, the XrML core contains the **RevocationFreshness** condition concept, that sets an upper bound on the latency allowed for the gathering of revocations. An XrML processing unit of the DRM system could again deliver the functionality for enabling scenarios involving this kind of *revocation pull*, for which it has to periodically interact with content owner’s system and keep track of the validity of affected signatures.

Further conceivable scenarios and tasks are manifold, including PKI and identity management, rights mediation, price formation, logging and report generation, as well as general database, cache, and service functionalities, and many more. We conclude with a preliminary categorisation of four generic tasks arising in the transition between content owner’s rights language and the target DRM system, in order of ascending complexity.

- **Content and Rights Reformatting** is the simplest possible task. It consists of transformation of the digital content format to the specific one for the target devices, and a fixed, pre-defined transformation of rights expressions to the target REL.
- **Data Management** tasks require functionality of a transient or persistent storage of rights related data, and of structured access to them. A paradigmatic instance arises when a distributor has to implement certain PKI functionalities in order to process the digital signatures contained in licences. Other licences might require reports on rights exertion being sent back to the content owner [11, Section 6.1.5].
- **Condition Evaluation.** Conditions in rights of the content owner’s language may not be conveyable to the target REL. In such a case, it becomes necessary to check the validity of such conditions based on additional information which can be internal or external to the DRM system. In case of success, rights in the target REL that reflect the original ones as closely as possible must be generated deterministically.
- **Dynamical State Evaluation** becomes necessary as a top level extension of the previous task in complex cases, when a right’s condition depends on an authoritative piece of data representing a system state. The Location Based Rights example above falls in this class if the state (geographical location of the device) is continually tracked during the exertion of rights by the user, and the rights are revoked upon failure.

All conceptual levels are affected, ranging from basic data formats, syntax, grammar, and vocabulary to semantic questions, which in not even extreme cases may demand separate legal accords between content owner and the DRM system’s operator to fix the semantics of the language transition. In order to be prepared for REL interoperability, a minimal requirement would be the presence of middleware able to process source and target language. Again of course, a real problem arises only if content owners in their business models actually exploit the flexibility of advanced RELs, the capabilities of which would otherwise lie idle. It becomes clear that one could be confronted with a transition between similar, yet distinct, universes. We reiterate what has by now become a commonplace: XML is an enabling technology for interoperability, and not *per se* the solution of interoperability problems. At this point it is appropriate to emphasise the delineation of the domain of automation from areas where human decision must prevail, For instance, it has been a general critique of RELs that they solely take the perspective of content owners [22], and are thus unable to cope with complex user expectations of usability and fair use. However, when it comes to judgements about the latter notoriously elusive notion⁵ any attempt to automation seems to be doomed.

⁵The widespread term stems from the US legal domain and denotes a generic set of limitations to copyright, considered to be in the public’s interest. A decision on fair use has to be made case by case, for which actually rather clear cut criteria are formulated in

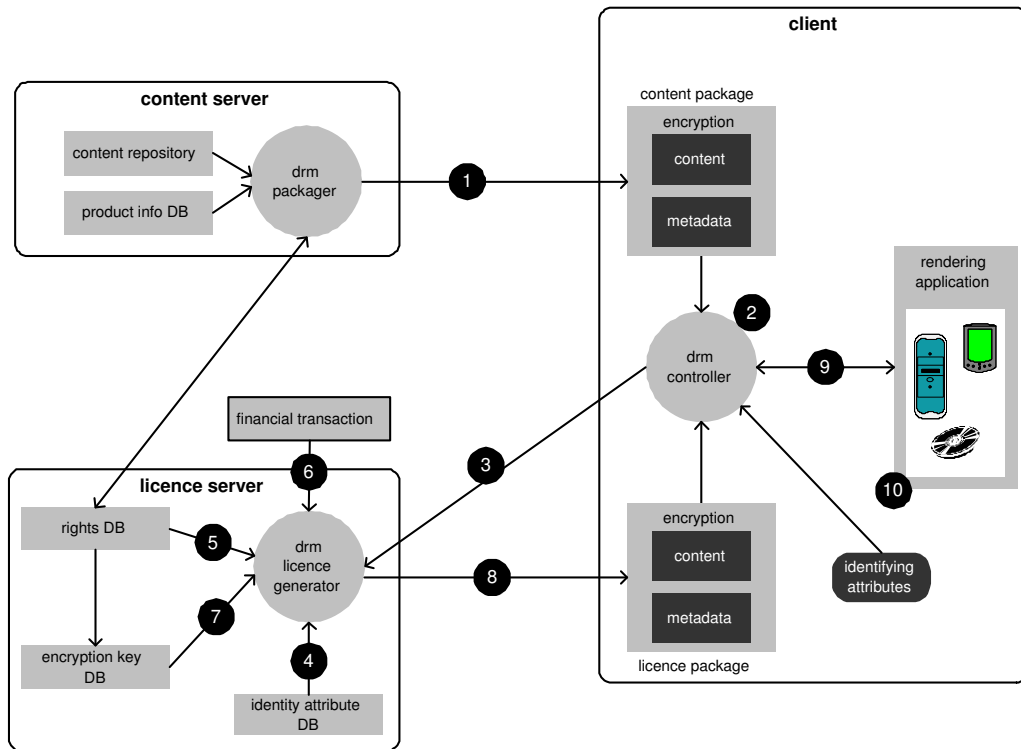


FIGURE 2. A Reference Model for DRM Platforms

4. INTERMEDIARIES FOR INTEROPERABLE DRM

Classical DRM Architectures. Due to their heterogeneous character, there can not be a single accepted model for DRM solutions. Several models with different views [23, 24] have been developed. Most sophisticated among them is the one proposed by Rosenblatt *et al.* [4] which is depicted in Figure 2. The process flow of this model can be outlined as follows:

1. User obtains content.
2. User attempts to use/render the content in some way. This triggers the DRM controller. Once activated, the DRM controller gathers information necessary for generating a licence. This includes identity information for the user and/or client device and information from the content package, including the content identifier.
3. DRM client makes rights request.
4. The licence server verifies the submitted client identification or attributes credentials against an identity database.
5. The licence server looks up rights specifications (rules) for the content.
6. A financial transaction is launched, if none has been recorded and the rules require it.
7. The licence generator compiles rights information, client identity information, and encryption keys, and creates a licence, which is itself encrypted or at least tamper proofed.
8. The licence is sent back to the client.
9. After the licence is generated and any authentication steps are completed, the DRM controller can decrypt the content and release it to the rendering application.
10. Finally, the rendering application plays or shows the content to the user.

None of the aforementioned interoperability tasks can easily be met by an architecture relying solely on the reference model above. Its focus is on a straightforward DRM process and does not leave much space for enhancements and complex manipulations of the content.

the law (17 U.S. Copyright Act 107), see [3, 25]. In the European domain a related concept is known as “making available” rights — another interesting story, see the many sources in [26]

The shortcomings are the result of certain unspoken assumptions. For instance, the issues of content and rights reformatting are not addressed by the model, since the simplistic model of the content server is assumed to yield a unique output format and relies on a predetermined set of input formats. However, as far as regards the input formats, no consolidation has been achieved and is even unlikely to occur given the heterogeneity of content owners' business models and content types. Consequently, content and rights reformatting remains a complex and a dynamically changing task. Accomplishing this task is at the tenets of a viable DRM system. An analogous problem exists on the side of output formats due to the heterogeneous and rapidly changing technical environments in which content is consumed. Similar critiques arise from the other three complex tasks of Section 3.

A Central Role for Intermediaries. The reader will surely have noticed that in the discussion above in Section 3 an intermediary was already present, if only in the form of a placeholder (the "distribution system") for the interoperability nexus ensuing from data formats and RELs. One might ask whether the described tasks in fact warrant an IDR architecture that is centered around an intelligent intermediary, or if not many interoperability problems may be shifted to other parts of a standard DRM architecture, e.g., the devices in the simplest case. The example of location based rights however clarifies that this is not an universal solution on the short to medium term. Not only would a device have to be equipped with an autonomous location system (if it is not based on the network) like GPS, which would be rather costly. But more importantly, a trust relation would have to be established between that system and the content owners, e.g., via digital signatures and certificates, requiring in any case a separate infrastructure. Thus the time does not seem quite ripe for device side DRM interoperability solutions. We therefore turn now to IDR architectures and their integrative advantages. But before doing so, we should derive from our analysis so far at least a tentative definition of what we mean by this frequently used term "IDR".

Tentative Definition: *An intermediary in a DRM system is an entity which offers services that strive to provide to content owners optimal revenues by a broad diffusion of their content under optimal enforcement of the associated licence terms, while aiming at offering to the final consumers an optimal content selection, approximation of usage preferences, and value proposition.*

This abstract, economical definition is neutral with respect to business models but sets certain limits and minimal requirements. For instance, a network service provider functioning as a mere bit-pipe for a DRM system is not an intermediary, since he does not offer value proposition mediation. On the other hand, the definition is flexible enough to comprise a wide range of cases. In particular what is optimal depends entirely on the business model of the content owner and the consumer's preferences. That means that the generic placeholder "value proposition" subsumes ancillary goals like price, privacy, quality of service, usability, etc., while on the other hand "enforcement" would cover anything from legal provisions and accords to cryptographic content protection and measures based on hardware. The latter term is also meant to denote an intermediary buying content for lump sums and offering it on his own terms, which might well be much more liberal as the example of Apple's iTunes service shows [3]. Minimally, the licence terms under which content is provided should be available in electronic form to remain in the realm of *digital* rights management.

Some proposals for IDR have been made in the literature, yet if not under the latter term. For instance, Sobel [6] would like to see network service providers as retailers for virtual goods in a rather strong inter-mediating function. They are thought to provide uncontrolled access to content allowing copying and redistribution. The trafficking of goods should in this model be traced by watermarking and fingerprinting and be charged to the responsible users accordingly by the network operator, conveying the content owners their fair share. Though in our view the exclusive reliance of this model on watermarking and fingerprinting is doubtful, it nicely shows the strengths of IDR. In fact, despite its similarity to a flat taxation, the model gives content owners the full discretion over the price proposition and enables price discrimination.

IDR Characteristics. Now coming to basic characteristics of IDR, we first focus on content and rights reformatting, a fundamental prerequisite and therefore of representative character for IDR. Remember that content federation and its counter part *demand federation* are the incitements for our discussion of content and rights reformatting. Here, demand federation refers to building one single demand aggregated from several separated demands, potentially different with respect to content types and rights formats. For

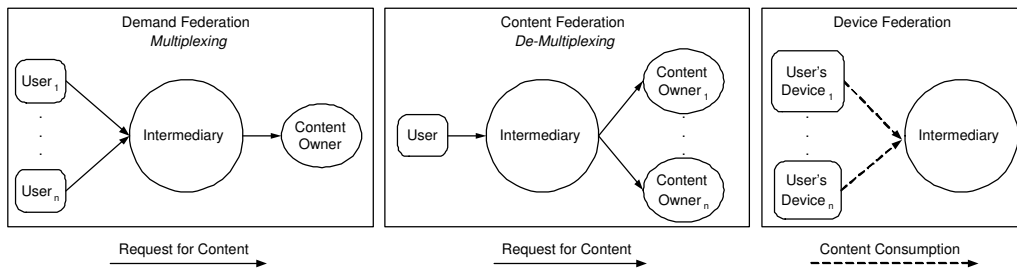


FIGURE 3. Federation Tasks within IDR Scenarios

example, two users could have different preferences regarding the number of consumptions for a certain content. The aggregation of these two demands could be a typical task for an intermediary. To accomplish it, he has to perform several sub-tasks which necessarily include content and rights reformatting.

Identification and production of data formats and the unique identification of the content type may still be done by an isolated component. But in the complex world of open systems, reformatting tasks cannot be performed without exploitation of external resources. Schemata, in particular for specific REL profiles, have to be fetched and interpreted. Likewise, the system must be able to understand the numerous schemes for unique content identifiers and metadata which are core components of DRM in general [27]. Additionally, if asymmetric cryptography is applied in a IDR solution, certification and validation authorities come into play, which is also relevant for data management tasks.

More challenging tasks of condition evaluation and dynamic state evaluation also require the involvement of external resources such as trusted time sources and providers of geographical location information. If a user desires portability of content between devices and the content's licence grants a limited number of consumptions, the usage information of all devices has to be compiled at a single point for evaluation. Since this can not be performed on the client side, it is another task for an intermediary, which in this case links to the devices as information sources for IDR.

We identify the most important characteristics of IDR: The intermediary collates information from external sources for DRM processing. This is an enabling factor for intermediaries' core functions as a multiplexing and demultiplexing unit located between users and content owners. Multiplexing in this context refers to demand federation whereas demultiplexing is understood as content federation, see Figure 3. As the figure depicts, there is a further aspect of multiplexing, i.e., subsuming several user devices for portability in a kind of "device federation".

5. NON-TECHNICAL MERITS OF INTERMEDIATED DRM

Many authors have argued on a general level that the acceptance of DRM systems might benefit from a limited relationship between content owner and consumer [3, 25] — a genuine feature that is provided by IDR. To the numerous arguments supporting this view, some of which are reiterated below, we can add one conclusion from our analysis at the end of Section 2: An intermediary can weaken the DRM tension field. Just as intermediaries in classical markets are effective in reducing the number of necessary transactions in the value chain, IDR has the potential to slash the size of the DRM complexity space. The intermediary can "shield" a number of the possible situations at both ends of the chain from each other by various means. He can do that by abstraction, generalisation, pre-negotiation, and proper mediation. Examples abound, from the primitive case of an intermediary buying content for a lump sum and reselling it on his own terms, over grouping of content and customers, to enabling portability of content between devices by registering them with an authority (see below). The terms offered by the intermediary might well be more liberal than the ones a content owner would be prepared to offer in his own right, maybe due to an existing trust relationship between the intermediary and its customer base — in other words the intermediary may vouch for the consumers.

It appears as a general drawback of current DRM concepts that demands can only be formulated from one, namely the content owner's, side, as mentioned in Section 3. Let us digress briefly to offer the most manifest suggestion: To equip the user with a machine readable language and data format to formulate his

usage preferences for virtual goods, an approach that would be very similar to the set of standards known as P3P [28] for the expression of user's privacy preferences and their automatic negotiation with web sites and applications⁶. If such a thing were in existence and widespread usage, the DRM tension would be weakened enormously. If furthermore automatic mediation between rights terms and usage preferences were possible, one might even speculate about the onset of disintermediation in the DRM domain. Luckily for potential intermediaries, the complexity of rights and usage preferences in the real world set natural limits to automation in this respect. Moreover, the main practical problem inherent to P3P systems [29, 30] (see also [31] for a thorough assessment of the efficacy of P3P) applies also in the present context. Users would have to set up and manage, and therefore to reflect seriously, on their own preferences. Not a thing which is easily initiated with someone who just wants to consume content as wanted. Again one might think about the automatic generation of user preferences as is already done today for marketing purposes but this is a prospect that is bound to raise the eyebrows of privacy keepers.

Coming back to the advocacy of IDRМ, a recurring issue of utmost importance is *customer privacy*. This is already true for Web Services [32] and the more for DRM systems with their ominous trend to indiscriminate accumulation of usage data (see [33] containing also a critical discussion of the suitability of P3P for privacy purposes in DRM systems). The limiting of the relation between content owner and user in IDRМ appears as a general advantage in this respect and has two distinct aspects. First, the intermediary again gains a federating function, this time with respect to content owner's various privacy policies⁷ which might otherwise be hard to assess and confounding to the user [3]. Since in fact intermediaries are legally required to disclose a unified privacy policy to the consumer when they offer an IDRМ service, they will have to negotiate a common denominator between the content owner's policies. That they will foster the interests of the consumers in doing so is made plausible by the second aspect of privacy in IDRМ. The intermediary might well maintain a pre existing economic and trust relationship with the customer base, e.g., if he is an Internet Service Provider (ISP) or Mobile Network Operator (MNO). This also diminishes the need for collection and distribution of user data for use in the DRM system, e.g., through usage of the ISP's/MNO's identity management and accounting systems — positively advantageous in the sense of data austerity. Even DRM systems based on watermarking technologies could profit from IDRМ with respect to privacy. The intermediary can serve as an escrow for the information in the watermark which would otherwise be public and attributable to an individual (pseudonymity). Another somewhat antipodal aspect of privacy in IDRМ is the issue of *lawful inspection/interception* (LI) by governmental authorities. Here, a caveat can arise with respect to the actual deployment of IDRМ systems, in that the intermediary could be required to provide access to distributed content in clear form, e.g., to identify content violating criminal law and track its usage. The intermediary himself must then necessarily be able to obtain content unencrypted, which rules out certain distribution models. As the discussion of the conflicts between privacy and LI is ongoing, this question must be regarded as unsettled for the moment. On a positive note, if an intermediary would provide a pragmatic solution for LI, this would appear as a service to content owners, relieving them from that burden.

Enabling content portability will be one of the key functions of IDRМ (see Section 2) and requires certain organisational measures. To that end, DRM solution providers developed so called domain concepts. A domain is a set of devices that share protected content (and also the respective rights to render the content). A user can define a domain of its personal devices and thus use the purchased content on those devices. Even if DRM enforcement is usually performed on the device itself, current domain management concepts typically require the devices to be online in order to register to or unregister from domains. Domains may either be managed by content providers themselves or, with observance of content federation, by trusted third parties responsible for managing domains of multiple content providers. This is advantageous from a consumers' perspective, since then they may not need to register their particular domains for each content provider. In the mobile domain, the Content Management License Administrator (CMLA [34]) consortium was recently founded. Besides the focus on robust DRM implementations through licensing of DRM devices, it provides the trust management for all involved server-side parties, such as content providers, content owners, device manufactures and service providers. CMLA would be a good candidate for domain management by

⁶A modification of existing rights expression languages to that end was suggested in [22].

⁷The availability of such policies is a general legal requirement for service providers both in the US and the EU domain, although a minimal one. EU policy goes further in imposing generic privacy guidelines.

extending the current scope to client side trust management features, since CMLA has already existing trust relationships with server side parties.

The aforementioned aspect of demand federation facilitates a new range of business models, which belong to the category of powershopping. Mediation is the foundation for powershopping, consequently intermediaries have to be in place. Intermediaries typically perform the tasks of aggregation, discovery, and matching [35]. However, since protected content and its usage rights can be complex and multi-attributive, consumer demands may differ greatly. Consequently, the task of demand federation is not restricted to the collection of several demands, but also means analysing their details with respect to both required data formats and desired usage rights. In particular, the latter are subject to consumers' preferences. For example, one user may wish to keep the purchased content forever, whereas another user wants to consume the same content only one time. The task of the intermediary is to aggregate this two demands into one by harmonising the two different rights requests. After purchasing the content and usage rights the intermediary has to generate two usage rights matching the consumers request. This simple example makes clear which value added services can be offered by an intermediary. The introduction of an intermediary can also be beneficial for content owners since it allows them to implement price discrimination models and thereby increase their revenues. Another positive side effect is that IDRMs leads to the creation of electronic communities, where intermediaries can provide diversification with respect to content owners in order to provide value to members and protection of privacy as described above, see also [36].

6. OUTLOOK

Let us conclude with a not so farfetched speculation on where DRM intermediaries will have their first appearance on a large scale, apart from the apparent onset of economic success for online music portals like iTunes and myCokemusic.com. Here we see network operators, i.e., ISPs and MNOs in a good starting position (for instance, T-Online has just recently started its Video on Demand service). The mobile case seems most interesting to us. For the mobile market, the present is a time of significant changes, characterised by the transition to third-generation (3G) technology based on high-bandwidth networks. Yet, the penetration of the mass market by the new products faces economic obstacles which are considerably steeper than were those at the beginning of the first mobile revolution in the early 1990ies. To name a few: Exceedingly high UMTS licence costs, massive investments for new network infrastructure, prohibitive final consumer prices for 3G Smartphones, and the established and widespread mobile technology, leave solid arguments for the consumer to change to 3G networks wanting. In particular, a lack of high valued content for the 3G market persists since content owners are hesitant to distribute such content without proper protection against piracy [37]. One of the most promising strategies to open the 3G mobile mass market could be to emulate the successful procedure of the present mobile market. Here, MNOs act as handset retailers by offering subsidised long term bundle contracts consisting of handset purchase and network access. But given the circumstances described above, MNOs need a viable perspective to market success to enter into such deals, and it is here that *MNO-centric IDRMs solutions can become an enabling technology*. An MNO could offer to content owners a secure distribution channel and added value (high quality content) to final consumers, i.e., the desired arguments to change to 3G. The MNO can thus obtain serious estimates about potential revenues in the 3G mass market on which he can base calculations for subsidised device contracts.

MNOs are in fact in an optimal position to become IDRMs service providers, foremost due to their huge customer bases. But also large parts of an MNO's existing infrastructure for ID management, payment, and interfaces to financial clearing systems can be "recycled" for IDRMs purposes. They can, along with a mobile network's ability to yield location information about devices, serve as information providing components for complex DRM scenarios. Also at the standardisation front, major industries are approaching interoperability specifications for mobile DRM at a high pace, most notably in the efforts of OMA [13, 19]. Dedicated DRM solution providers are already on the mobile bandwagon, e.g., Digital World Services and LockStream have already carried out a number DRM projects for MNOs [38].

Whether mobile and other DRM solutions live up to fulfill the promising prospects of intermediated DRM and exhaust its possibilities to the mutual benefits of content owners, consumers, and not the least themselves, remains to be seen.

REFERENCES

- [1] Rolf T. Wigand: *Facing the Music: Value-Driven Electronic Markets, Networks and Value Webs in Economic Integration of Digital Products*. In: [26], pp. 250–270.
- [2] Patrick Aichroth, Jens Hasselbach: *Incentive Management for Virtual Goods: About Copyright and Creative Production in the Digital Domain*. Virtual Goods 2003.
http://virtualgoods.tu-ilmenau.de/2003/incentive_management.pdf
- [3] D. K. Mulligan, J. Han, A. J. Burstein: *How DRM-based content delivery systems disrupt expectations of “personal use”*. In: Proceedings of the 2003 ACM workshop on Digital Rights Management, Washington DC, October 27, 2003, pp. 77–89.
- [4] B. Rosenblatt, W. Trippe, S. Mooney. *Digital Rights Management: Business and Technology*. M& T Books, New York, 2001.
- [5] Rob Koenen: *Intellectual Property Management and Protection in MPEG Standards*. Workshop on Digital Rights Management for the Web, World Wide Web Consortium, INRIA – Sophia Antipolis, France, 22–23 January 2001.
- [6] Lionel S. Sobel: *DRM as an Enabler of Business Models: ISPs as Digital Retailers*. Berkley Technology Law Journal, **18**, no. 2, 2003. <http://www.law.berkeley.edu/journals/btlj/articles/vol18/Sobel.stripped.pdf>
- [7] Susanne Guth: *Rights Expression Languages*. In [26], pp. 101–112.
- [8] XML Cover Pages. <http://xml.coverpages.org>
- [9] DRM Watch. <http://www.drmwatch.com>
- [10] The Open Digital Rights Language Initiative. <http://www.odrl.net>
- [11] XrML The Digital Rights Language for Content and Services. eXtensible Rights Markup Language (XrML) 2.0 Specification, Parts I–V. <http://www.xrml.org>
- [12] XMCL - the eXtensible Media Commerce Language. W3C Note 19 September 2002.
<http://www.w3.org/TR/2002/NOTE-xmcl-20020919/>
- [13] Bill Rosenblatt: *Open Mobile Alliance Announces Version 2.0 of DRM Standard*. DRM Watch, Feb. 5, 2004.
<http://www.drmwatch.com/standards/article.php/3308861>
- [14] openIPMP Open-Source Rights Management. <http://openipmp.com>
- [15] OASIS Rights Language TC. http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=rights
- [16] The MPEG Home Page. <http://www.chiariglione.org/mpeg/>
- [17] Open eBook Forum. <http://www.openebook.org/>
- [18] G. Spenger: *Authentication, Identification Techniques, and Secure Containers — Baseline Technologies*. In: [26], pp. 62–80.
- [19] Open Mobile Alliance. <http://www.openmobilealliance.org>
- [20] Frank Hartung: *Mobile DRM*. In: [26], pp. 138–149.
- [21] Reed Elsevier: *Position Paper*. Workshop on Digital Rights Management for the Web, World Wide Web Consortium, INRIA – Sophia Antipolis, France, 22–23 January 2001. <http://www.w3.org/2000/12/drm-ws/pp/reed-elsevier-honious.html>
- [22] Deirdre K. Mulligan, Aaron J. Burstein: *Implementing Copyright Limitations in Rights Expression Languages*. In: Proceedings of the 2002 ACM workshop on Digital Rights Management.
- [23] Renato Iannell: *Digital Rights Management (DRM) Architectures* In: D-Lib Magazine, Volume 7, Number 6, June 2001.
- [24] Qiong Liu, Reihaneh Safavi-Naini, Nicholas Paul Sheppard: *Digital rights management for content distribution* In: Proceedings of the Australasian information security workshop conference on ACSW frontiers 2003 - Volume 21, 2003.
- [25] John S. Erickson: *Fair Use, DRM, and Trusted Computing*. Communications of the ACM **46**, no. 4 (2003) 34–39.
- [26] Eberhard Becker, Willms Buhse, Dirk Günnewig, Niels Rump (eds.): *Digital Rights Management - Technological, Economic, Legal and Political Aspects*, Lecture Notes in Computer Science 2770, Springer-Verlag, 2003.
- [27] Norman Paskin: *Identification and Metadata*. In: [26], pp. 26–61.
- [28] Platform for Privacy Preferences (P3P) Project. <http://www.w3.org/P3P/>
- [29] Electronic Privacy Information Center/Junkbusters: *Pretty Poor Privacy: An Assessment of P3P and Internet Privacy*. June 2000. <http://www.epic.org/reports/prettypoorprivacy.html>
- [30] James H. Kaufman, Stefan Edlund, Daniel A. Ford, Calvin Powers: *The Social Contract Core*. In: Proceedings of the conference WWW 2002, May 7–11, 2002, Honolulu, Hawaii, USA, pp. 210–220.
- [31] Harry Hochheiser: *The Platform for Privacy Preference as a Social Protocol: An Examination Within the U.S. Policy Context*. ACM Transactions on Internet Technology, Vol. 2, No. 4, November 2002, pp. 276–306.
- [32] Donna L. Hoffman, Thomas P. Novak, Marcos Peralta: *Building Consumer Trust Online*. Communications of the ACM **46**, no. 4 (1999) 80–85.
- [33] Joan Feigenbaum, Michael J. Freedman, Tomas Sander, Adam Shostack: *Privacy Engineering for Digital Rights Management Systems*. In: Tomas Sander (Ed.): *Security and Privacy in Digital Rights Management*, ACM CCS-8 Workshop DRM 2001, Philadelphia, PA, USA, November 5, 2001, Lecture Notes in Computer Science 2320 Springer-Verlag, 2002, pp. 76–105.
- [34] Content Management License Administrator Initiative. <http://www.cm-la.com>
- [35] Astrid Meck: *Shopbots, Powershopping, Powersales: New Forms of Intermediation in E-Commerce — An Overview*. Beitrag 203, Volkswirtschaftliche Diskussionsreihe, Universität Augsburg.
- [36] Ai-Mei Chang, P.K. Kannan, Andrew B. Whinston *Electronic Communities as Intemediaries: the Issues and Economics*. Proceedings of the 32nd Hawaii International Conference on System Sciences 1999.
- [37] NetLight Consulting AB: *The Business Case for Mobile DRM*. Stockhol, September 2002. <http://www.netlight.se>
- [38] See the Websites <http://www.dwsco.com>, <http://www.lockstream.com/>