DigiRight: Network of Excellence for a Framework for Policy, Privacy, Security, Trust and Risk Management for Digital Rights Management

H. Abie[1], J. Bing[2], B. Blobel[3], J. Delgado[4], B. Foyn[1], S. Karnouskos[5], P. Pharow[3], O. Pitkänen[6], and D. Tzovaras[7]

[1]*Norwegian Computing Center, Norway, {habtamu.abie, bent.foyn}@nr.no*
[2]*Norwegian Research Center for Computers and Law, Norway, jon.bing@jus.uio.no*
[3]*University of Magdeburg, Germany, {Bernd.Blobel, Peter.Pharow}@medizin.uni-magdeburg.de*
[4]*DMAG-TECN, Universitat Pompeu Fabra, Spain, jaime.delgado@upf.edu*
[5]*Fraunhofer Institute FOKUS, Germany, Stamatis.Karnouskos@fokus.fraunhofer.de*
[6]*Helsinki Institute for Information Technology (HIIT), Finland, olli.pitkanen@hiit.fi*
[7]*ITI, Center for research and Technology Hellas, Greece, Dimitrios.Tzovaras@iti.gr*

Abstract

In today's digital world there is an enormous and increasing amount of digital content. In the future world of ambient intelligence, digital content will be ubiquitous and people will interact with it in all areas of their lives, a situation that presents new challenges in the area of Digital Rights Management (DRM). While valuable information products need protection from theft and prying eyes, access to information and the ability to contribute to information products and to share information within communities are also essential to all citizens of the information society. The needs for security and privacy are predominant in such situations. All of this is making DRM crucial. Therefore, we proposed to establish a Network of Excellence for a Framework for Policy, Privacy, Security, Trust and Risk Management for DRM, DigiRight, which will consist of experts from various disciplines and will conduct and guide on-going and future high quality research.

1. Introduction

Today's wired and wireless digital world has yielded a massive and increasing amount of digital content. Indeed, in the future world characterized by ambient intelligence, digital content will be ubiquitous, and people will interact with it in all spheres of their personal life, social activities and work, even in situations where they may not realize it. All this presents us with new kinds of challenge in the area of DRM.

Information and communications technologies (ICT) provide us not only with evermore powerful means to develop and distribute information products, but also with means to copy-protect data and restrict its availability. On the one hand valuable information products need protection from theft and prying eyes. On the other hand, access to information and the ability to contribute to information products as well as to share information within communities, are essential to all citizens of the information society. While efficient business methods require collecting detailed information on transactions, business partners and customers, the need for privacy of all stakeholders must also be respected. The amount of sensitive information that must be securely stored, shared, or distributed within and between organizations is also rapidly increasing. Striking the balance between the appropriate level of security and the protection of user privacy and enabling users to control how personal identifying information is to be stored, distributed, and used, is crucial. All of this is making DRM crucial.

Digital Policy Management (DPM) is becoming a discipline in its own right, whose concern is the design, analysis, implementation, deployment and use of efficient and secure technology that handles digital information in accordance with the relevant rules and policies. These policies are based on the security requirements of digital information, which in turn are based on rigorous analysis of risks, its vulnerability, and threats to it. Thus, since the improvement in the implementation of policy depends on an improved risk management process, any DRM research must give full attention to the improvement of risk management process, and risk assessment methodologies. Consequently, security, trust and privacy policies must be developed and integrated into the DPM-enabled DRM system (DRMS). Furthermore, seamless interoperability of DRM solutions across fixed and wireless networks and infrastructures need to be addressed.

Therefore, we need to establish a Network of Excellence (NoE) [1] for a Research Framework for Policy, Privacy, Security, Trust and Risk Management for DRM, viz DigiRight [2]. It will consist of individual experts from various research institutes and organizations having expertise in the fields of technology, law, business, social science, ethics, policy-making, and security. As the issue is very complex, an NoE is needed in order to conduct and guide on-going and future high quality research. The description of

DigiRight's relevance and potential impact may be found in [3]. The ubiquity of digital content means that DRM concerns almost everyone, from authors and publishers, to consumers, libraries, schools and educational institutions, infrastructure providers, hardware and software manufacturers [4], and governments and standard bodies. Therefore, any DRM related research must take into account both the complexity of disciplines and the concerns of the various stakeholders.

This paper describes the DigiRight NoE, which will meet these requirements and has been submitted under the Sixth Framework Programme for the first IST Call. Section 2 and 3 describe the DigiRight objectives and integrated DRM research framework, respectively. Section 4 describes the scenario methodology for making the goals operative, and the plan to establishing a virtual DRM research Center, and section 5 concludes.

2. The DigiRight objectives

The overall goal of DigiRight is to develop a synergy Research Framework for Policy, Privacy, Security, Trust and Risk Management for Digital Rights Management with an ultimate goal of establishing a virtual DRM research Center. The purpose of the DigiRight research Framework is to

1. integrate the traditionally separated DRM research communities across Europe (both at national and regional level) in the fields of technology, business, law, ethics and social science (all of which are important operative factors in the uptake of DRM), and to structure the way DRM research is carried out in the research community and amongst practitioners by networking together teams of experts in these fields;
2. stimulate joint scientific research projects to gain insights into the fundamental issues and challenges associated with future DRM systems, exchange of research personnel, harmonization of DRM technologies and solutions, and learning programs at the European level;
3. create a self-sustainable set of knowledge-spreading activities through liaison with end-user communities, industries, standard bodies and governmental organizations, and a solid two-way technology transfer between the industries, standard bodies, and governments;

The final goal is to establish a virtual DRM research center with the aim to develop solutions, guidelines and standards to protect, manage access rights (including the evolution, emergence and negotiation of the new rights of the e/m-society) to, control usage of, and distribute trustably tangible and intangible digital assets without risking users' privacy, and hence to stimulate the development and use of European digital content on the global networks promoting the linguistic diversity in the Information Society. In particular, we shall address the new challenges presented by new broadband access networks and mobile telephony, thus enabling content providers and technology companies to publish information on any Internet platform, from the web to wireless devices, to Internet appliances and broadband television. Through all this, we aim to build customers' trust and confidence so that the Intellectual Property Rights (IPR) business will flourish on a global scale.

3. DigiRight: An integrated DRM research framework

The primary feature, which assures a coherent integration, is the well-defined collective goal, which can be simply stated as DRM. The topic itself, DRM, is an extremely motivating goal for researchers and an attractive product for the public. However, the research necessary to achieve this goal is, by its nature, highly complicated and diverse, and can thus not be conducted without steps being taken to integrate it and bringing together relevant, complementary researchers. The necessity of a well-coordinated large and diverse research group to achieve this goal strongly discouraged researchers for a long time.

DigiRight will therefore network experts in the different disciplines necessary for a holistic view and understanding of DRM. For each discipline a task force has been created, a task force of experts within each discipline, who will be responsible for on-going and future high quality research into those aspects of the discipline concerned, which are relevant to DRM. The task forces will co-operate with each other on joint research using common concepts, methodologies and tools that will be developed and synthesized from components taken from jurisprudence, the social sciences, business theory and economics, and science and technology. This integration of interdisciplinary approaches and ensuing technologies will provide the Network with a common background and basis for combined research, and facilitate the exploitation of the synergy of the various projects, areas of expertise and stakeholders. Intellectual property (IP) asset creation, IP asset capture, IP asset management, and IP asset usage [5] control and tracking will be handled effectively as common domain platform services. Standards will be developed to allow interoperability so as not to force DRM users to encode their works in proprietary formats or systems.

DigiRight will concentrate mainly on technology. In this connection it is important to note that the object is not merely to develop and implement DRM technology, but also to ensure that it is widely used. This will require a reliable and secure infrastructure, and will depend on users' (citizens, businesses, communities) trust and confidence in the technology which provides them with controls fine-tuned for the balance of, on the one hand, privacy and security, and, on the other,

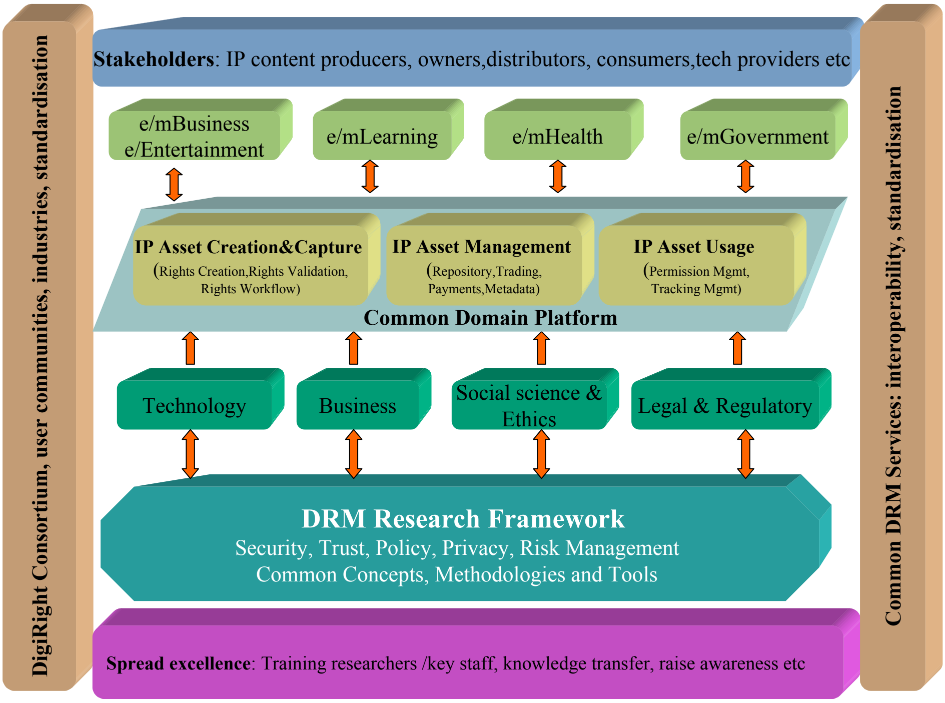
DigiRight Consortium, user communities, industries, standardisation
Stakeholders: IP content producers, owners,distributors, consumers,tech providers etc
e/mBusiness e/Entertainment
e/mLearning
e/mHealth
e/mGovernment
IP Asset Creation&Capture
(Rights Creation,Rights Validation, Rights Workflow)
IP Asset Management
(Repository,Trading, Payments,Metadata)
IP Asset Usage
(Permission Mgmt, Tracking Mgmt)
Common Domain Platform
Technology
Business
Social science & Ethics
Legal & Regulatory
DRM Research Framework
Security, Trust, Policy, Privacy, Risk Management
Common Concepts, Methodologies and Tools
Spread excellence: Training researchers /key staff, knowledge transfer, raise awareness etc
Common DRM Services: interoperability, standardisation

Figure 1 – DigiRight research framework

accessibility and usability that they need. It will also require correct attention to be paid to privacy, policy, security, trust and risk management in DRM, and must be addressed from technological, business, legal, ethical and societal perspectives. Figure 1 depicts the DigiRight DRM research framework with some of its major components.

3.1. Technology

The overall objective of the Technology Task Force is to contribute to common DRM research methodology, integrating and spread of excellence activities from the technology perspective. This will involve among other things:

- identify and analyze the relevant technological challenges and solutions to DRM application scenarios in question;
- bring forward existing and lacking knowledge in technology;
- describe the technology requirements, solutions, and obstacles;

The Technology Task Force will concentrate on the following seven central aspects: privacy, policy, security, trust management, risk management, protection mechanisms, and information representation semantics.

Privacy enhancing technologies: The need for privacy is predominant in any core business. The next generation of DRM will cover the description, identification, trading, protection, monitoring and tracking of all forms of rights of usage over both tangible and intangible assets, and would manage rights holders relationships [5]. The ability of this next-generation DRMS to track and monitor will lead to a need for more efficient mechanisms for the protection of personal privacy, protection that the DRMS itself must ensure. Although there are those who claim that this is a red herring on the basis that such privacy is protected and guaranteed by law, it should be pointed out that unscrupulous manufacturers and individuals may be technically capable of violating privacy undetected and therefore unpunished.

The aim of this activity is to investigate approaches to protecting the privacy of individuals, groups, and even companies and governments, and strike the balance between tracking usage and user privacy, and enable consumers to control how personally identifying information is obtained and used [6, 7, 8]. Essential challenges are:

- Personal information privacy: What personal information can be shared with whom;
- Digital assets privacy: Whether digital assets can be exchanged without anyone else seeing them;
- Anonymity: Whether and how one can send messages anonymously, and whether this should be permitted or is desirable;

- Anonymity vs. Accountability: How accountability and anonymity can be balanced to allow user control as much as possible, community norms when users' desires conflict, and government regulation when the norms of the communities differ [9];
- Provide controls fine-tuned for the balance of, on one hand, privacy and security, and, on the other, accessibility and usability that users need;

Digital Policy Management (DPM): DPM's concern is the design, analysis, implementation, deployment and use of efficient and secure technology that handle digital information in accordance with the relevant rules and policies. Brose et al. [10] have also proposed a systematic approach to integrating security policy design into the system development process. The aim of this DPM activity is to investigate different trust and privacy policies that must be developed and integrated into the DPM-enabled DRMS. This digital policy can for example be embedded in a mobile software component, which may provide services helping authenticate and authorize use of the digital content and regulate what the user is allowed to do with the content. For the DRM policy part of the NoE, an architecture [11] is proposed in which the intellectual property rights owners (e.g. content providers) are associated to a broker that is in charge of exploiting (selling) their content rights, and, once those are sold, of controlling that the rights are respected; i.e., no illegal copies are circulating on the Internet.

Security architecture and infrastructure services: The problem of protecting digital information from unauthorized distribution is the concern of many rights holders, content providers and distributors. The function of this activity will be the investigation of DRM-enabling security architecture and infrastructure services as a basis for DRM applications. The aim of the security infrastructure is to enable valid users to create, distribute, store, manipulate and communicate information objects across organizational boundaries with the required level of security [12].

In order to achieve DRM solutions that are interoperable and standard-based as well as applicable in different domains, a common infrastructure platform for the DRM technology and enabling basic security services is required at both the application level and infrastructure level. Openness and interoperability lead to a seamless inter-connection and co-operation of security services. Communication security services comprise strong mutual authentication and accountability of principals involved, integrity, confidentiality and availability of communicated information as well as some notary services. Application security services concern accountability, authorization and access control regarding data and functions, integrity, availability, confidentiality of information recorded, processed and stored as well as some notary services and audit. DigiRight will address content qualities that can be managed semi-automatically properties such as integrity, confidentiality, authenticity, and trustworthiness in DRM. Specific challenges include:

- Research on the application of cryptographic technologies / Public Key Infrastructure (PKI) for the IPR protection;
- DRM-enabling security infrastructure as a basis for DRM applications;
- Design, analysis, and implementation of an advanced architecture and related security protocols for a distributed DRM in seamless environments;
- Integration of Biometrics and Smart Cards for DRM applications;

Trust Management: Trust is an essential factor in any business-transaction systems including DRM systems. To wit providers need to establish trust and confidence in their products and services, and consumers need to protect their privacy and information and assess the trustworthiness of their providers. Lack of trust in the ability of DRM infrastructure to protect IPR is a significant barrier to growth in the IPR business transactions. Usage Tracking is essential for providing trust for content providers. At the same time, the user must be able to trust that a service will not violate his/her privacy, and be sure that the service quality is the agreed upon one. Understanding user concerns related to trust and confidence has a key role in the work of DigiRight. In addition, DigiRight will engage in standard setting operations, which help to define a DRM architecture, which meets the security and dependability concerns of the users. Thus it is essential to facilitate the cross-disciplinary investigation of fundamental issues underpinning trust models by bringing together expertise from technology oriented sciences, law, philosophy and social sciences. Activities include:

- Develop formal social cognitive theories of trust and reputation, and explore the role of reputation in the evolution of altruism and co-operation in human societies;
- Apply the trust models to agent societies [13];
- Test theory-driven hypotheses about the effects of different types of reputation systems by means of simulation–based and natural experiments, also in view of optimizing existing online reputation reporting systems;
- Facilitate the emergence of widely acceptable trust management processes for open DRM systems and applications;
- Explore the role of attitudes towards a DRM-based transaction, which is defined as the overall evaluation of the desirability of a DRM-based transaction with an agent. The aim is to develop a trust model that will help each user to judge whether authenticity and provenance evidence of the transaction make a digital content sufficiently trustworthy;

- Model and simulate human factors regarding trust and security to understand the real background of the trust phenomenon;

Risk Management: Risk management holds the key to security: A security policy is necessary to support the security infrastructure required for the secure movement of sensitive information across and within national boundaries [15]. To ensure the secure operation of this kind of infrastructure, it is necessary to have some well-founded practice for the identification of security risks as well as the application of appropriate controls to manage risks. The risk management process provides a framework for identifying risks and deciding what to do about them. Risk management is not a task to be completed and shelved. It is an ongoing process (with well-defined steps [16, 17]) that, once understood, should be integrated into all aspects of an organization's management.

Trust management also relies on risk management: quantification of trust based on systematic methods for threat identification and risk analysis may offer better evaluations of DRM transaction. Risk in the digital environment is typically influenced by the organisational structure and circumstances [18] that affect human interaction (situational trust), beliefs and inclinations (human centric trust), and confidence on technology infrastructure in place (computer centric trust). Risk management thus allows us to combine risk with trust in order to form a security policy [18]. Furthermore, DRM and content distribution industry related companies would require risk management strategies and tools to protect vital assets. The application of risk management disciplines will help identify, assess and control risks relevant to the distribution of digital content. Sound risk management will help create a sense of confidence and safety about an operation. In an environment where the threat of unnecessary risk is reduced, services can be more creatively provided to clients and better results can be achieved, hence company/institution safety and security.

Consequently, the essential challenges are:

- Building appropriate balance between trust, privacy, policy and risk management for DRM with a balanced legal framework that takes account of the change in the academic, political, economical and socio-cultural model while at the same time safeguarding fundamental rights, freedoms, fair-use, and private-use in the digital world.
- Future possible risks related to information in digital form must be managed in advance in several ways [19].
- Research regarding risks and threats specifically related with digital rights management, in order to enhance the risk management procedure and ensure its completeness and research to manage risks involved in participating in DRM transactions thereby building trust in those transactions.
- Risk management methodologies for IPR protection development – especially the creation of knowledge bases with specific risks and control for addressing the risks.
- Research on DRM scenarios to qualitatively and quantitatively support appropriate decision making for minimization of risks, based on system dynamics based modeling and simulation.

Protection mechanisms: watermarking, encryption and fingerprinting - technical solutions are required to restore some control over the identification of original content, the monitoring and tracking of the use, and the management of distribution/communication channels. There are techniques to identify original content such as hash codes in digital files, watermarks in images and hidden sound codes in music files, and encryption to secure communication and distribution. This activity will investigate protection techniques including:

- Watermarking (1D / 2D / 3D multimedia data), combining watermarking with indexing;
- IPR protection of data between Internet and mobile telecommunications systems, using encryption and watermarking;
- Accountability mechanisms. Accountability is a more challenging goal for distributed or peer-to-peer systems or networks with a transient population of users, where it is hard to identify user identities and obtain information about their past behavior in order to predict their future performance;
- Reputation mechanisms. The notion of reputation can be employed in a variety of mechanisms as a means of providing fairness and balanced use of resources;

Information representation semantics: In order to improve the management of rights in the digital environment (DRM), there is a need for a common language for DRM representation in the open and global framework provided by the Web. This kind of language is aimed to help building a reliable Web where IPR can be managed in an open, global and adaptable form, so people can share, sell, buy, etc. content subject to DRM, depending on their needs. A semantic approach seems a more flexible and efficient way of achieving these activities than a syntactic one.

Using metadata for referencing multimedia material is becoming more and more usual. This allows better ways of discovering and locating this material published in the Internet. Several initiatives for establishing standards for metadata models are being carried out at the moment, but each focuses on their own requirements when defining metadata attributes, their possible values and the relation between them. For someone who wants to seek and buy information (multimedia content in general) in different environments, this is a real problem, because he/she has to face different metadata sets, and so, must have different tools in order to deal with them. A DRM ontology can put into practice this approach, endowing agents with more complete background knowledge, which allows them to work quite autonomously.

The idea of this NoE is to facilitate the automation and interoperability of DRM frameworks integrating both parts, called Rights Expression Language and Rights Data Dictionary. This can be accomplished using ontologies. They can provide the required definitions of the rights expression language terms in a machine-readable form. Thus, from the automatic processing point of view, a more complete vision of the application domain is available and more sophisticated processes can be carried out.

3.2. Business processes and models

Connector in the field of business processes and models is the detailed analysis of all involved acting parts. On the one hand there are the rights holders, which are a heterogeneous group with acting parts such as authors, agencies, and publishing houses, which follow different aims and are connected on to each other in complex relationships. On the other hand, the target markets are also highly heterogeneous. In this area of tension varying business models are formed, which are distinguishable by achievement and revenue. According to the Oxford dictionary process is a method of producing goods in a factory by treating raw materials. A business model [20] is a description of how a company intends to create value in the marketplace. It includes unique combination of products, services, image, and distribution that a company carries forward, and the underlying organization of people and the operational infrastructure that they use to accomplish their work.

The objective of the business models task force is to be able to analyse and study business models' aspects of the scenarios in question. This activity should identify relevant research and results for the selected scenarios in order to bring forward existing and lacking knowledge. The product of this task force should be a report with analyses of what could be done from the business models' side of view to realise the scenarios, and where the major obstacles are believed to be. The main research challenges to be addressed in this activity are negotiation, contracting, and production processes, publication, and data models.

Negotiating: The negotiation protocol, that it is part of the "Service Request" phase in an e-commerce model, has three sub-phases: Initial offer, co-operative contract production, and payment. In the Contract production sub-phase, the most complex and important one, there are several alternatives over which to work. First, the selling entity initiates the protocol with an initial proposal of digital rights conditions, normally taken from a pre-defined subset. After that, the buying entity has three alternatives: Accepting the offer, making a counter-offer and rejecting the offer. After the initial proposal, the negotiating entities elaborate the contract, using the negotiation protocol, from the sequence of offers and counter-offers until a final agreement is reached, forming then the final electronic contract.

Contracting: By DRM negotiation we mean the process in which, at purchase time, the buyer of some multimedia content and the rights owner (or representative) negotiate the conditions (concerning rights) in which that material is sold. This process, run through a protocol with some interchange of information, is equivalent to creating an electronic contract. It could be also seen as a joint editing of a structured document (the contract), following pre-specified alternative rules. The electronic contract, that should be electronically signed, has two parts:

- Mandatory part: It contains the minimum information necessary to formalize an electronic contract.
- Optional part: It contains optional information related to any kind of contract.

Production processes, publication, data models: Publishing houses and media companies are developing the opportunities of expanding their own competitive position with the aid of innovative products and services, and for acquiring entirely new business segments. At the same time, they are confronted with a lack of systematic processes and methods, which bear in mind issues of DRM. Such processes are essential above all to develop successful products and services. The aim is to allow publishing houses and media companies to prepare and design content for publication in a manner, which is manageable by typical midsize companies. This demand results from changing possibilities of data storage and the big expectations in the field of media products.

The question is therefore, how production processes and DRM can be integrated in this complex field of media production. For that reason a model for reference processes and a model of production have to be developed. These models consider co-operation within publishing houses as well as co-operation between companies; they should allow multiple uses of content through standardized asset management and support the use of integrated information systems along the production processes.

3.3. Legal and regulatory, private and public policies

The objective of this activity is to analyze and study legal and societal aspects of the DRM scenarios in question. The Task Force should identify relevant research and results for the selected scenarios in order to bring forward existing and lacking knowledge. The most important research challenges in the area of legal, regulatory, policy and societal aspects are the following four central aspects.

Data protection: The task will be to identify IPR in the terms of elementary actions which require the consent of a right holder, i.e. to "copy", to "public performance", to "systematically access and extract elements from a data base", *etc.,* [13,14]. There are also fundamental unsolved issues related to IPR in new kinds of information products. Within this task, we are going to integrate the participants' excellence in understanding which intellectual property rights are applicable to different information products and which parts of the products are protected. For data protection, one will have to identify in which way to obtain a relevant consent from a data subject, or alternatives in obtaining the right for the processing of the personal data involved. This will especially be a challenge in the health care sector, where the data will be of sensitive nature, but is also of growing significance in the telecom sector. Though coordinated by the data protection directive, different national statues have implemented the provisions rather differently, especially with respect to sensitive data, of which processing in many jurisdictions is subject to license from a national data protection authority. Therefore, the inter-legal issues (jurisdiction and choice of law) have to be included.

Content policies: Content policies are developed on the basis of the recent directive coordinating national copyright and related rights. "Content" is a facile term covering a variety of material in different legal categories, copyrighted material, material subject to neighboring rights, especially the rights of performing artists, producers and database builders. Content is usually the part of an information product without which the product has no value. The other parts, like metadata or programs, however, may add value to the content. It is not possible to precisely define the concept of content. As there can be tremendously many kinds of information products, also content can differ a lot. It can be nevertheless described as the actual payload of the information product. For example, a computer program as such can be an information product. On the other hand, as a part of a multimedia product, it does not necessarily need to be something without which the product has no value, but is merely a value-adding auxiliary part. Therefore a program may or may not be content. It should be noted that not only commercial publishers produce information products or content, but using modern information technology it will become more common that authors themselves distribute their works and the end-users, on the other hand, contribute to the content. Often the subject for trade is not content, but the legal position related to the content, allowing the purchaser to exploit the content according to terms specified in a license, which also will include remuneration.

Ethical aspects: Legal rules may not be sufficient for business models to operate, but will have to be bolstered by more restrictive ethical rights. Especially for data protection, one should make explicit the trade practices. The identification of human individuals is one of the most difficult ethical issues. Technically, it is difficult to reliably relate any physical identification to a human being. However, that is a small problem compared to legal and ethical issues related to privacy, anonymity, and identity. In general, everybody should be able to remain anonymous and to keep privacy. On the other hand, a human being may act in a large number of roles. A person at work, at home, at leisure activities and so on has many roles that should be distinguished. For example, usage rights like private use or fair use are often different depending on the role and a license may only cover certain role-based usages. Therefore it is hardly possible to build solutions that in general rely on human beings direct identifications. Instead, most systems need to depend on indirect user identification based on for example device identification.

Consumer rights and expectations: There are latent but growing tensions between the actors involved, especially where DRM may restrict the use of "content" with respect to end user equipment (only authorized DVD-players). An example of consumer protection issues related to DRM is one with rights description languages (e.g. ODRL, XrML). It is possible to describe very complex sets of rules using those powerful and expressive languages. A rights description resembles a computer program. For a human, it can be very difficult to understand what those complex sentences mean. However, when somebody buys an information product, it is essential what rights are licensed or assigned. Even if the customer gets the right data, but does not get the rights needed, the customer does not get what was expected. In accordance with consumer protection laws, it is important to inform a consumer in advance what is to be sold. It must be possible to cancel the transaction if the consumer does not get what was anticipated.

3.4. Societal questions

A balancing act of the rights of the provider or right holder and the end-user must be made in the perspective of the society, where promotion of electronic trade may be a separate policy objective. The European Commission has announced that bringing every European online and into the digital age, creating a digitally literate Europe, and ensuring that the whole process is socially inclusive will be the key objectives in bringing an information society for all the Europeans. This raises important societal aspects on DRM. DRM systems that unnecessarily prevent people from accessing information or increase the digital divide between population groups are not welcome. Instead, future DRM systems should actively help to achieve the above goals.

One of the key issues in the societal area is the rise of user communities. Users themselves contribute to content and share information and resources. A topical example is gaming communities in which players around the world develop the games and play them together. Another example is open source movement: software engineers without any formal organizations create programs together and distribute them freely. This model will enlarge and cover many walks of life.

3.5. Application domains and stakeholders

There is a lack of communication between application domains. Practitioners in one domain are frequently totally ignorant of the activities of their peers in others, and are quite capable of producing the most exciting results without sharing them, and on occasion, after someone else has produced them without bothering to tell anyone. How often has the wheel been reinvented? This is due to the unfortunate fact that the results are neither disseminated through the right channels nor, more importantly, in a cross disciplines. The same concepts and ideas often apply in many different areas, and those few of us who have managed to abstract these concepts from one domain and apply them to the problems of another have often gained wonderful results.

Therefore DigiRight will pay special attention to inter-domain communication and co-operation as it meets those challenges highlighted by the Commission as top priorities for Europe in the coming years in the following domains **e/m-business, e/m-entertainment, e/m-learning, e/m-health, e/m-government,** and **e/m-generic-services** with the objective of ensuring that all stakeholders including producers, owners, distributors/retailers, users, technology providers enabling the delivery, and hardware and software companies enabling the consumption of intellectual property (IP) content, are all winners. Thus, in DigiRight all domains relevant to the information society will be represented by domain experts among the partners reflecting specific challenges, needs and solutions.

Therefore DigiRight will attempt to address any stakeholder in any business chain. DRM is a key part of the future platform for application and service provision. A DRM architecture that balances the interests of the various stakeholders will be a key enabler of new applications; an ill-balanced architecture is a showstopper.

4. DigiRight: Scenario methodology, integrating process, and a virtual DRM research center

4.1. Scenario methodology – making the goals operative

DigiRight aims at studying future systems that involve many disciplines whose systems do not exist today, so they cannot be observed directly. At first sight, it seems that, for instance, legal challenges related to the systems should be analyzed using the methods of legal science. However, the challenge is about forthcoming issues while legal science mostly uses court cases, statutes, and their preparatory works as its sources and derives theories by analyzing them. Thus it is hardly possible to tell almost anything about the future using conventional methods. Instead, future research provides us with more suitable methods. Especially scenarios are useful when we want to describe how the world will be like. In addition to providing us with adequate research method, scenarios are excellent means to integrate and communicate ideas, views and concepts. The participants will be able to share common understanding and disseminate outcome using clear, explicit scenarios. Scenarios used in other fields of science are typically quite broad. On the other hand, sometimes it is useful to create very small scenarios or use-cases. In this network, we expect the scenarios to be relatively narrow: they will merely describe a possible service that is grounded on participants' research, literature, existing services, and discussions with other experts. However, there may emerge needs to develop also very small or huge scenarios.

We do not claim that any of our scenarios would actually come true. Neither is their actual probability of being realized in the focus of work. Instead, they are to form a picture of possibilities and concerns that may exist in the future. In the network of excellence, scenarios will be used as means of integrating the excellence of various partners, defining research areas, accomplishing actual joint research work, and disseminating the conclusions. The scenarios will be updated and new scenarios will be created as we are making progress.

4.2. DigiRight integrating process

DigiRight aims at developing a synergy research framework whose purpose is to structure the way DRM research is carried out in the research community by networking together teams of experts in the fields of technology, business, law and social sciences. The provision of such a Framework is expected to become a critical instrument for attracting researchers and practitioners to DRM issues. DigiRight needs to address DRM from all sides, identify where there are obstacles to overcome in order to realize services that use DRM. It will achieve its goal through a number of carefully planned activities, which collectively bring a high degree of long lasting integration. Figure 2 depicts the DigiRight integrating process/cycle with the main activities and task forces.

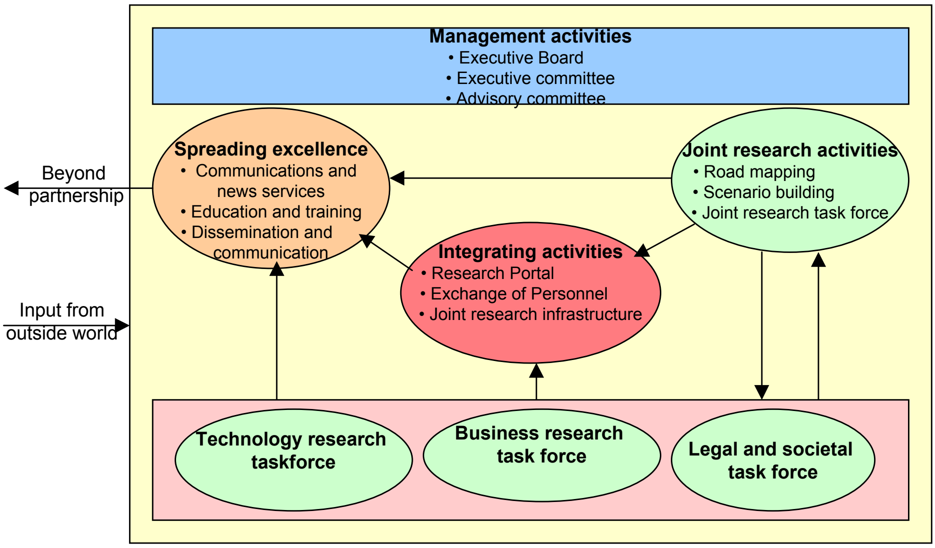

Figure 2 - Integration process

4.3. Establishing a virtual DRM research center

The objective of this activity is to ensure that the Network activities continue to be adequate for DigiRight to approaching a virtual organization that will continue to exist after the cessation of Community funding. This will first of all be a result of all the other activities in DigiRight. The reason for having this activity is to be able to address important questions from this side of view that might not be taken sufficiently into account in the other activities. Examples of important questions are:

- How to ensure that DigiRight becomes the preferred unit of co-operation within DRM research in Europe;
- How to create services that will secure the economic basis for funding when the EC financing is terminated;
- How to ensure sufficient anchoring of DigiRight in international organizations that run conferences, standardization work and other scientific activities and within the most important partners in DRM research;

The ultimate goal of DigiRight is to create one single virtual research organization in DRM issues across Europe in order to co-ordinate DRM research in the future. This virtual organization should span the different traditional borders of research such as technology, legal & regulatory, societal questions, and business processes and models.

5. Conclusions

In this paper we have described DigiRight, a Network of Excellence proposal for a DRM research framework, which aims to

1. integrating the traditionally separated DRM research communities across Europe (both at national and regional level) in the fields of technology, business, law, ethics and social science all of which are vital to understanding the issues related to future DRM and its use;
2. stimulating joint scientific research projects to gain insights into the fundamental issues and challenges associated with future DRM systems;
3. creating a self-sustainable set of knowledge-spreading activities through liaison with end-user communities, industries, standard bodies and governmental organizations;

The DigiRight NoE is an integrated approach to address the **trust** and **confidence** in communication, e/m-business, e/m-entertainment, e/m-learning, e/m-health, e/m-government, and e/m-generic-services, and the support to solve complex problems in science, society, industry and business objectives. It is our considered opinion and firm conviction that such an integrated research framework will be a much-needed shot in the arm for the understanding and uptake of knowledge-based digital economy.

Acknowledgements

The authors would like to express their gratitude to the DigiRight partners [2] for their contributions and efforts during the proposal writing, and Martti Mantyla for his review of the DigiRight proposal and for his useful comments.

References

[1] Research DG, European Commission, Provisions for Implementing Network of Excellence, Background document, Draft 2002 edition: 11 November 2002

[2] Network of Excellence for a Research Framework for Privacy, Policy, Security, Trust and Risk Management for Digital Rights Management, a proposal for network of excellence under FP6 for the IST Call 1, submitted to EC, 24/04-2003, http://digiright.nr.no/nuke/html/

[3] H. Abie, B. Blobel, J. Delgado, S. Karnouskos, R. Marti, P. Pharow, O. Pitkänen, and D. Tzovaras, DigiRight: Relevance to and Potential Impact on Europe's Need to Strengthen the Science and Technology Excellence on DRM, Mobile IPR, HIIT, Finland, August 27-28, 2003.

[4] M. Fetscherin, Present State and Emerging Scenarios of Digital Rights Management Systems, JMM – The International Journal on Media Management Vol. 4 – No.3, pp 164-171, 2002

[5] R. Iannella, Digital Rights Management (DRM) Architectures, D-Lib magazine, June 2001, Vol. 7, No 6, http://www.dlib.org/dlib/june01/iannella/06iannella.html

[6] J. Feigenbaum, M. J. Freedman, T. Sander, and A. Shostack, Privacy Engineering for Digital Rights Management Systems, November, 2001, http://www.pdos.lcs.mit.edu/~mfreed/docs/privacy-engineering.pdf

[7] J. E. Cohen, DRM and Privacy: http://www.law.berkeley.edu/institutes/bclt/drm/papers/cohen-drmandprivacy-btlj2003.html, 2003

[8] Electronic Privacy Information Centre. Digital Rights Management and Privacy: http://www.epic.org/privacy/drm/

[9] L. J. Hoffman and K. A. M. Carreiro, Computer Technology to Balance Accountability and Anonymity in Self-regulatory Privacy Regimes, Cyberspace Policy Institute, School of Engineering and Applied Science, The George Washington University

[10] G. Brose, M. Koch, and K.P. Lohr, Integrating Security Policy Design into the Software Development Process, Technical Report B-01-06, Institut fur Informatik Freie Universitat Berlin, Germany, November 13, 2001

[11] J. Delgado, I. Gallego, and X. Perramon, Broker-Based secure Negotiation of Intellectual Property Rights, ISC'01, LNCS 2200, Springer-Verlag, 2001

[12] H. Abie, A Rights Management Model for Distributed Object-Oriented Information Distribution Systems, Proceedings of the IFIP WG6.7 Workshop and EUNICE on Adaptable Networks and Teleservices, September 2-4, pp. 185-194, 2002

[13] J. Bing, The contribution of technology to the identification of rights, especially in sound and audio-visual works: An overview, Norwegian Research Centre for Computers and Law, University of Oslo, Norway

[14] J. Bing, Intellectual property exclusive rights and some policy implications, Norwegian Research Centre for Computers and Law, University of Oslo, Norway

[15] Risk Analysis Resource Page, Norwegian Computing Center, http://www.nr.no/~abie/RiskAnalysis.htm

[16] AS/NZS 4360:1999, Risk Management, Australian Standard, 12 April 1999-09-17

[17] Norwegian Standard, NS 5814, Requirements for Risk Analysis, August 1991

[18] T. Dimitrakos and J. Bicarregui, Towards Modelling e-Trust, 3rd Panhellenic Symposium on Logic Anogia academic village, Crete, Greece, July 2001

[19] O. Pitkänen, and M. Välimäki, Towards a Digital Rights Management Framework, IEC2000, Manchester , UK , 2000

[20] H. Chesbrough, and R. S. Rosenbloom: The Role of the Business Model in Capturing Value from Innovation: Evidence from Xerox Corporation's Technology Spin-off Companies, Harvard Business School, To be submitted to Industrial and Corporate Change.