The need for a digital rights management framework for the next generation of e-government services

Habtamu Abie* and Bent Foyn

Norwegian Computing Center, Gaustadalleen 23,
PO Box 114 Blindern, N-0314 Oslo, Norway
E-mail: Habtamu.Abie@nr.no E-mail: Bent.Foyn@nr.no
*Corresponding author

Jon Bing

Norwegian Research Centre for Computers of Law, Faculty of Law,
University of Oslo, PO Box 6706, St. Olavs plass, NO-0130 Oslo,
Norway
E-mail: Jon.Bing@jus.uio.no

Bernd Blobel and Peter Pharow

Institute for Biometry and Medical Informatics,
University of Magdeburg, Leipziger Strasse 44, D-39120 Magdeburg,
Germany
E-mail: Bernd.Blobel@mrz.uni-magdeburg.de
E-mail: Peter.Pharow@Medizin.Uni-Magdeburg.DE

Jaime Delgado

Universitat Pompeu Fabra, Pg. Circumval.lació 8,
E-08003 Barcelona, Spain
E-mail: jaime.delgado@upf.edu

Stamatis Karnouskos*

Fraunhofer Institute FOKUS, Kaiserin Augusta Allee 31,
D-10589 Berlin, Germany
E-mail: Stamatis.Karnouskos@fokus.fraunhofer.de
*Corresponding author

Olli Pitkänen

Helsinki Institute for Information Technology (HIIT),
PO Box 9800, 02015 HUT, Finland
E-mail: olli.pitkanen@hiit.fi

Dimitrios Tzovaras

Informatics and Telematics Institute, Centre Reseach and Technology,
Hellas, 1st Km Thermi-Panorama Road 57001, PO Box 361,
Thermi-Thessaloniki, Greece
E-mail: Dimitrios.Tzovaras@iti.gr

Abstract: The amount of government information is huge and relies mostly on traditional systems, inaccessible to citizens and often to government departments. In today's digital era, most of this content can be more intelligently processed and integrated within e-government. In the world of the future, where ambient intelligence and e-governments are a reality, citizens will interact with the available services in all areas of their lives; a situation that presents new challenges in the area of Digital Rights Management (DRM). Taking into account the nature of the information and the needs of different governmental departments and citizens, any e-government research must give full attention to DRM. In the process towards successful e-government, properly handling privacy, security and trust is an indispensable precondition for reliable legal safeguards, reliable technology and secure business, and for achieving acceptance by citizens. Therefore, we propose to establish a Network of Excellence (NoE) for a framework for policy, privacy, security, trust and risk management for DRM. The NoE will consist of experts from various disciplines and will conduct and guide on-going and future high quality research on e-government related domains.

Keywords: e-government; privacy; security; trust; digital rights management; network of excellence.

Reference to this paper should be made as follows: Abie, H., Foyn, B., Bing, J., Blobel, B., Pharow, P., Delgado, J., Karnouskos, S., Pitkanen, O. and Tzovaras, D. (2004) 'The need for a digital rights management framework for the next generation of e-government services', *Electronic Government*, Vol. 1, No. 1, pp.8–28.

Biographical notes: Habtamu Abie is a research scientist at the Norwegian Computing Centre. He has previously worked as Senior Engineer and Research Scientist at Telenor R&D Norway and as Scientific Associate and Scientific Fellow at CERN Switzerland. He has also held a research position at ABB Corporate Research and worked as a Software Development Engineer at Nera AS and Alcatel Telecom Norway AS. His past and present research interests include: security for communication and distributed systems, distributed object computing, digital rights management, privacy, policy, trust and risk management, architecture and methodology, formal methods and tools, and mobile and personal computing.

Bent Foyn has 12 years of research experience, the last seven years at the Norwegian Computing Centre. His research has mostly been focused on streaming media technology and learning. He has been project leader for a number of research projects, the latest three years for the LAVA Learning project involving 15 partners in a 3M€ project for streaming media usage in project based learning in Norwegian Schools. This project involved design and development of DRM technology to control content use in schools. At present, Bent Foyn holds the position of Assisting Research Director at NR.

Professor, dr juris Jon Bing, cand jur (Oslo) 1969, dr juris (Oslo) 1982, dr juris hon causae (Stockholm 1997 and Copenhagen 1998), Computer Law Pioneer Award (San Diego 1993), Visiting Professor, King's College (London) 1997-99.His former offices include Council of Europe Committee on Legal Data Processing (chair), Norwegian Film Council (chair), Norwegian Council for Cultural Affairs (chair). His current offices include Board of Governors, European Cultural Foundation (member), Legal Advisory Board Information Society Directorate General (member), Data Protection Tribunal (chair), Organising Committee IFLA 2005 Oslo (chair).

Dr. Bernd Blobel is Associate Professor, Director (prov.) of the Institute for Biometry and Medical Informatics as well as Head of Medical Informatics at

the Otto-von-Guericke University Magdeburg, Head of the Regional Clinical Cancer Registry Magdeburg/Saxony-Anhalt, Co-Chair of international Working Groups and Technical Committees in EFMI, ISO, CEN, HL7, OMG/CORBA on system architecture, modelling, security, electronic health record, health networks, health telematics, and communication standards. He is involved in a number of European and global projects and is Advisor to the German Federal Government on health telematics and health information systems architecture including EHR.

Peter Pharow works as a scientist at the Institute for Biometry and Medical Informatics. This deals with distributed health information systems, advanced system architecture, component systems, electronic health record systems, and medical documentation within the scope of national, European and international project activities. His working areas are aspects of security, safety and quality in Health Informatics, legal aspects, data security and protection, security services, mechanisms, and infrastructures, security policy and policy templates, Health Professional Cards, Trusted Third Party Infrastructures and related services as well as health networks and user behaviour.

Prof. Jaime Delgado holds a PhD in Telecommunication Engineering. He is a Professor of Computer Networks and Architecture at the Technology Department, Universitat Pompeu Fabra, Barcelona since 1999 as well as Dean of the Faculty of Informatics and Head of the Distributed Multimedia Applications Group (DMAG). He has been project manager for several European projects and is the Editor of several international standards. He has been an evaluator and reviewer for the European Commission since 1989, the author of around 100 published papers and a member or chairman of many conference programme committees.

Stamatis Karnouskos is a senior scientist and R&D project leader at Fraunhofer Institute FOKUS. He is involved in several projects related to software agents, active networks, security and mobility within national (German), industrial and European Union projects. His contributions include project management and coordination as well as technical research and development in the aforementioned domains. He is a guest editor of *IEEE T-SMC* journal, author of more than 20 technical papers in international refereed journals and conferences, and participates as a reviewer and member of the technical program committee of several international conferences and workshops.

Olli Pitkänen holds a licentiate (post-graduate) degree in software engineering and a master's degree in laws. He has worked as a researcher and a teacher at Helsinki University of Technology for about ten years. In 1999-2001, he was a visiting scholar at the University of California, Berkeley. His research interests include digital rights management, intellectual property rights, and software engineering. Prior to academia, he worked as a software engineer in several companies. He has also practised law at Opplex Attorneys at Law, which is a law firm specialising in legal issues related to information technology.

Dr. Dimitrios Tzovaras received a Diploma and PhD in Electrical and Computer Engineering from the Aristotle University of Thessaloniki (AUTH), in 1992 and 1997 respectively. He is currently Senior Researcher in the Informatics and Telematics Institute of Thessaloniki. His main research interests include information processing, representation and communication, multimedia data protection and virtual reality. His involvement with those research areas has led to the co-authoring of more than 30 papers in refereed journals and 50 papers at international conferences.

1 Introduction

Within the process of globalisation and the permeation of all areas of life by technology, e-government (e-gov) could arise as a powerful tool that will effectively integrate and manage the huge amount of existing information, as well as seamlessly integrate citizen interaction with its services. In order to do so, a DRM framework has to be in place, a framework that will guarantee for all e-gov actors the basic principles of trust, security, privacy, and policy and risk management.

Information and communications technologies (ICT) provide us not only with ever more powerful means to develop and distribute information products, but also with the means to copy-protect data and restrict its availability. On the one hand, valuable information products need protection from theft and prying eyes and, 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 privacy needs of all stakeholders must also be respected. The amount of sensitive information that must be securely stored, shared or distributed within and between governmental organisations and their partners, as well as citizens, is also rapidly increasing. Striking a balance between appropriate levels of security, the protection of citizens' privacy, and enabling citizens to control how personal identifying information is to be stored, distributed and used, is crucial. All of this is making DRM a critical success factor in the context of e-gov.

2 E-government and DRM

E-gov uses ICT to transform legacy procedures by making them more accessible, effective, accountable and citizen friendly. In this context the goal is to:

- better orchestrate the dissemination of information among different agencies and cooperating organisations and individuals
- provide greater access to government information and promote citizen interaction with governmental services (especially benefiting rural and traditionally under-served communities)
- make government more accountable by making its operations transparent, and allow policy-based secure handling of information, thereby reducing the phenomenon of mismanagement and corruption.

Governments produce a huge amount of information, much of which is potentially useful to individuals and businesses. The internet and mobile technologies are playing an ever increasing part in the lives of ordinary citizens and can help governments communicate directly with them. Furthermore, enabling citizens to participate in the processes of e-gov and interact with government and its representatives, without actually having to travel to local (if they exist) offices, can crack down on inefficient bureaucracy, reduce the workload of clerks and eliminate corrupt practices, like bribery. However, the information content disseminated by governments is varied and not all of it is aimed at the general public. A fair amount of it is sensitive information and for the exclusive

consumption of specified individuals or groups of individuals. A framework will have to ensure that, in a digital world, the intended individuals or groups use this content. Another common problem of legacy activities of government is duplicated information (which results in redundancy) and the slow processing of it (if any), usually manually using proprietary software developed for a specific department (or at best the whole agency) that doesn't cooperate with other inter-governmental systems and processes, and is difficult to evolve. Currently we see an effort on the part of some governments to use open source operating systems (such as Linux) and software to cut down costs and increase interoperability and openness, but even there we do not yet have efficient DRM enabled applications tailored to e-government's requirements. The approach proposed here also aims at tackling this domain. It is not the automation of the old processes that is critical to the success of e-government, but the creation of new ones, which take advantage of state of the art technologies and integrate better into the current and future context of an information-aware society.

To achieve these goals, there must be in place a DRM-enabled framework that will promote research and development of technologies that will empower next generation services and information management in e-government. 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 dependant 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 enhanced risk management processes and risk assessment methodologies. Consequently, security, trust and privacy policies must be developed and integrated into the DPM-enabled DRM system (DRMS). Furthermore, since we are paving our way towards the ambient intelligence environments, we are not solely interested in e-government but also in mGovernment. Therefore, the seamless interoperability of DRM solutions across fixed and wireless networks and infrastructures needs to be addressed.

Concluding, we need to establish a NoE for a research framework for policy, privacy, security, trust and risk management for DRM that will focus on the needs of e/mGovernment. It will consist of individual experts from various industrial as well as research institutes and organisations having expertise in the fields of technology, law, business, social science, ethics, policy-making and security. The ubiquity of digital content means that DRM concerns almost everyone, from authors and publishers, to consumers, libraries, educational institutions, infrastructure providers, hardware and software manufacturers, standardisation bodies and, most importantly, governments. Therefore, any DRM related research must take into account both the complexity of disciplines and the concerns of the various stakeholders.

3 The objectives

The overall aim is to develop a framework for policy, privacy, security, trust and risk management for DRM with the ultimate goal of establishing a virtual competence centre that will successfully provide a flexible context of technologies and concepts that can be

integrated to ease the management of e-government. This should be done by an open, cross-disciplinary and inter-domain approach at international level. The purpose being to:

- integrate the traditionally separated DRM research communities (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
- stimulate joint scientific research projects to gain insights into the fundamental issues and challenges associated with future DRM systems, harmonisation of DRM technologies and solutions, and learning programs at the European level
- create a self-sustainable set of knowledge-spreading activities through liaison with end-user communities, industries, standard bodies and government organisations, and a solid bi-directional technology transfer between industries, standard bodies, and governments.

The final goal is to establish a virtual self-sustained DRM research centre with the aim of developing 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 the usage of, and distribute trustable tangible and intangible digital assets without risking users' privacy. This will stimulate the development and use of digital content on the global networks, promoting the linguistic diversity of the Information Society. In particular, the new challenges presented by new broadband access networks and mobile telephony must be addressed in order to enable governmental agencies to publish information on any channel, e.g. internet-based systems, mobile devices and broadband television. Through all these, we aim to promote citizens' trust and confidence in e-government services so that the Intellectual Property Rights (IPR) business will flourish on a global scale.

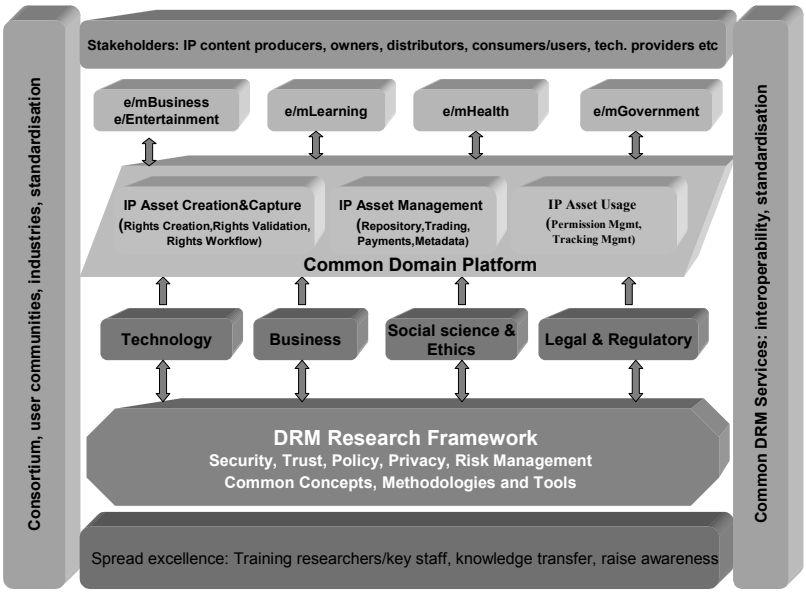
4 An integrated DRM research framework

The primary feature, which assures a coherent integration, is the well-defined collective goal, which can be simply stated as DRM. DRM is an extremely motivating goal for researchers, and the research effort to be invested is, by its nature, highly complicated and diverse. The necessity of a well-coordinated large and diverse research group to achieve this goal greatly discouraged researchers for a long time. There is, therefore, a need to network experts in the different disciplines necessary for a holistic view and understanding of DRM and its implication in e-government scenarios. For each discipline, a task force should be responsible for on-going and future high quality research into those aspects of the discipline concerned that are relevant to DRM. The task forces will cooperate with each other on joint research using common concepts, methodologies and tools that will be developed and synthesised 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 [1], control and tracking will be handled effectively as common domain platform services. Standards will be further developed to allow interoperability so as not to force DRM users to encode their works in proprietary formats or systems. This is of paramount interest in the e-government domain, where changes in procedures and information representation are slow.

The focus is mainly on technology, as this is the common denominator in tackling e-government issues at a global level. In this context, 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 regardless of the business processes or the country specific requirements involved. This will require a reliable and secure infrastructure that will depend on users' (citizens', businesses', communities') trust and confidence in the technology, which allows them to control privacy, security, accessibility and usability issues. Figure 1 depicts the proposed DRM research framework with some of its major components.

Figure 1 The research framework



4.1 Technology

The overall objective of the technology task force is to contribute to common DRM research methodology, integration and spread-of-excellence activities from the technology perspective for the e-government domain. This will involve:

- identifying and analysing the relevant technological challenges and solutions to DRM application scenarios for the e-government domain
- bringing forward existing and lacking knowledge as well as hands-on experiences in technology
- providing a clear understanding of 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.

4.1.1 Privacy-enhancing technologies

The need for privacy is predominant in any core business, especially in e-government, due to the enormous amount of personal information that it holds. 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 will manage rights holder's relationships [1]. 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, a protection that the DRMS itself must ensure. Although it is often claimed that privacy is protected and guaranteed by law, it should be understood that unscrupulous manufacturers and individuals might be technically capable of violating privacy undetected and, therefore, unpunished.

Thus, the aim is to investigate approaches to protecting the privacy of individuals, groups and even companies that directly interact within the context of e-government. Furthermore, it should provide citizens with the option of controlling how personally identifying information is obtained and used [2–4]. Challenges include:

- *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, on the basis of community norms, when users' desires conflict, and government regulation, if community norms differ [5].
- Provision of controls fine-tuned for the balance of, on the one hand, privacy and security and, on the other, accessibility and usability that users need.

4.1.2 Digital policy management (DPM)

The concern of DPM 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. Brose *et al.* [6] have also proposed a systematic approach to integrating security policy design into the system development process. The aim of this activity is to investigate different trust and privacy policies that must be developed and integrated into the DPM-enabled DRMS for e-government. This digital policy can, for example, be embedded in a mobile software component, which may provide services supporting authorised use of the digital content. For the DRM policy, an architecture [7] is proposed in which the IPR owners (e.g. content providers) are associated with a broker in charge of exploiting (selling) their content rights and, once those are sold, ensuring that the rights are respected, for example, that no illegal copies are circulating on the internet.

4.1.3 Security architecture and infrastructure services

The problem of protecting digital information from unauthorised distribution is the primary concern of many rights holders, content providers and distributors. The objective of this activity will be the investigation of DRM-enabling security architecture and infrastructure services as a basis for DRM-enabled e-government applications. The aim of the security infrastructure is to enable valid users to create, distribute, store, manipulate and communicate information objects across organisational boundaries with the required level of security [8].

In order to achieve DRM solutions that are interoperable and standard-based as well as applicable in different domains, a common infrastructure platform with integrated security services is required at both the application and infrastructure levels. Openness and interoperability are mandatory in order to lead to a seamless inter-connection and cooperation of security services. According to the Layered General Security Model developed within the European ISHTAR project, the concepts of communication security and application security can be distinguished [9]. Communication security services comprise the 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, authorisation and access control in connection with data and functions, integrity, availability, confidentiality of information recorded, processed and stored, as well as some notary services and audit. The foreseen challenges include:

- research on the application of cryptographic technologies and their practical application e.g. Public Key Infrastructure (PKI) for IPR protection
- DRM-enabled security infrastructure as a basis for e-government applications
- design, analysis and implementation of an advanced architecture and related security protocols that will provide security at several layers on which applications can rely, and seamless integration of DRM with existing approaches, e.g. single sign on (SSO)
- integration of biometrics, smart cards and other authentication devices for integration with DRM applications.

4.1.4 Trust management

Trust is an essential factor in any business-transaction system and much more so in the e-government domain. Systems of e-government need to establish trust and confidence within and between agencies, across governments and, of course, with citizens and businesses. This has to be reflected by the electronic services and citizens need the ability to control their privacy and information. Lack of trust in the ability of the DRM infrastructure to protect IPR is a significant barrier to growth in IPR business transactions. Usage tracking is essential to provide 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 quality of the service is the one agreed upon. Understanding user concerns related to trust and confidence plays a key role in the success of any DRM-enabled services of e-government. Therefore, it is essential to facilitate the cross-disciplinary investigation of fundamental issues underpinning trust models by bringing together expertise from technology-oriented sciences, law and social sciences. Activities include:

- developing formal social cognitive theories of trust and reputation and exploring the role of reputation in the evolution of altruism and cooperation in human societies
- applying the trust models to the agent society [10]
- testing theory-driven hypotheses about the effects of different types of reputation systems by means of simulation-based and natural experiments, also with a view to optimising existing online reputation reporting systems
- facilitating the emergence of widely acceptable trust management processes for open DRM systems and applications
- exploring the role of attitudes towards a DRM-based transaction, which are 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 there is sufficient authenticity and provenance evidence of the transaction to make a digital content sufficiently trustworthy
- modelling and stimulating human factors regarding trust and security to understand the real background of the trust phenomenon.

4.1.5 Risk management

Risk management is firmly coupled with security: a security policy is necessary to support the security infrastructure required for the secure transfer of sensitive information across and within e-government boundaries [11]. 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 and the application of appropriate controls to manage risks. The risk management process provides a framework for identifying risks and deciding how to manage them. Risk management is not a task to be completed and shelved, but an ongoing process (with well-defined steps [12,13]) that, once understood, should be integrated into all aspects of e-government's management. Risk in the digital environment is typically influenced by the organisational structure (e.g. the different governmental agencies) and circumstances that affect human interaction (situational trust), beliefs and inclinations (human centric trust), and confidence in the technology infrastructure in place (computer centric trust). Risk management allows us to combine risk with trust in order to form a security policy [14]. Furthermore, DRM and content distribution industry related companies 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. Successful risk management will strengthen the sense of confidence and safety of e-government services available to citizens. The challenges foreseen include:

- establishing the appropriate balance between trust, privacy, policy, and risk management for DRM with a balanced legal framework that takes account of changes in the academic, political, economic and socio-cultural environment while, at the same time, safeguarding fundamental rights, freedoms, fair-use and private-use in the digital world
- managing in advance and in a number of different ways future possible risks related to information in a digital form [15]

- research regarding risks and threats specifically related to DRM, 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 risk controls
- research on DRM scenarios to support qualitatively and quantitatively appropriate decision making processes for the minimisation of risks, based on 'system dynamics based modelling and simulation'.

4.1.6 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 of it, and the management of distribution/communication channels. Plenty of techniques capable of identifying the original content exist today, e.g. hash codes in digital files, watermarks in images, and hidden sound codes in music files. Further investigation is envisaged on:

- watermarking (2D/3D multimedia data), combining watermarking with indexing
- IPR protection of data transmitted, for example, over the internet or mobile telecommunication systems using encryption and watermarking
- accountability mechanisms: this is a challenging problem for distributed or peer-to-peer systems and networks, where it is hard to securely prove users' identity and obtain information about their past behaviour 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.

4.1.7 Information representation semantics

In order to improve the management of rights in the digital e-gov environment, there is a need for a common language for DRM representation. This will help to build a reliable context where IPR and content subject to DRM can be managed in an open, global and adaptable way. This has to be in compliance with the semantic web vision and spawn future e/m infrastructures. Using metadata for referencing multimedia material is becoming more and more usual. This provides better ways of discovering and locating the material and services. Currently, there are several initiatives afoot to investigate metadata models, but each focuses on its own requirements when defining metadata attributes, thus limiting their globality. Therefore, information processing is differently understood in different environments due to different non-fully-interoperable metadata sets. A global cross-discipline DRM ontology can overcome this problem and boost machine-based processing, e.g. via agent technology. The idea is to facilitate the automation and interoperability of DRM frameworks, integrating both parts, called Rights Expression Language and Rights Data Dictionary, using ontologies. 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.

Ontologies are tools developed for the purpose of structuring knowledge and offer an appropriate framework for information representation in e-gov. The semantics of knowledge specification and description models capable of describing the capabilities and the interface for e-government at all levels are essential. Significant user involvement from different e-government areas will be needed in order to develop an appropriate vocabulary capable of depicting most e-government transactions and services. Challenges include:

- establishing a flexible ontology infrastructure, which will cover different e-government application areas, define and represent e-government capabilities and interfaces so as to be able to represent a general model for e-products and services, and provide scalability and hierarchical features, e.g. a full description might be available to a closely collaborating company, while a less-detailed description at a lower level in the description hierarchy might be publicly available
- developing descriptors and techniques for semantic interoperability using reference ontologies from specific application domains, enriched to include DRM issues and e-government processes. An important addition will be the enrichment of ontologies, apart from the DRM issues, and with more specific low-level features capable of describing e-products and services, thus offering added value functionalities, such as automatic catalogue creation from the included descriptions and enhanced search and retrieval functionalities
- developing user-friendly graphical tools to support authoring and retrieval based on this ontology infrastructure, and for generating the ontology-based descriptions or 'profiles' of e-products and services. These tools will interface with this infrastructure and will help users to create, edit and maintain their own descriptions
- supporting efficient machine-readable representation formats for the representation of e-government ontology representation using the state-of-the-art knowledge representation languages such as OWL (W3C Web Ontology Language) and RDF/S (Resource Description Framework/Schema), already successfully used in semantic web applications.

4.2 Business processes and models

The basic and common principle in the field of business processes and models is the detailed analysis of all involved actors. On the one hand there are the rights holders, who are a heterogeneous group with acting parts, such as authors, agencies and publishing houses, which pursue different aims and are connected 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 [16] is a description of how a company intends to create value in the marketplace. It includes the unique combination of products, services, image and distribution that a company presents, and the underlying organisation of people and the operational infrastructure that

they use to do their work. Any DRM scheme that will be integrated into e-government has to take into consideration these models and be flexible enough to dynamically adapt them to future needs.

The objective of the business models task force is to analyse existing proposed business models for e-government scenarios and identify relevant results that can be integrated. The main research challenges to be addressed in this activity are negotiation, contracting, and production processes, publication and data models.

4.2.1 Negotiating

The negotiation protocol is part of the 'Service Request' phase in an e/m-commerce model, and has three sub-phases: initial offer, co-operative contract production and payment. The contract production sub-phase is the most complex but also the most important one and, today, several alternative procedures exist. Firstly, the selling entity initiates the protocol with an initial proposal of digital rights conditions, normally taken from a pre-defined subset. The buying entity has three alternatives: accept the offer, make a counter-offer or reject the offer. After the initial proposal, the negotiating entities elaborate on the contract details, using the negotiation protocol, from the sequence of offers and counter-offers until a final agreement is reached, which will then form the final electronic contract.

4.2.2 Contracting

By DRM negotiation we mean the process by which, at the time of purchase, the content buyer and the rights owner (or representative) negotiate the conditions (concerning rights) under which that material is sold. This process is equivalent to the creation of an electronic contract and can be seen as a joint editing of a structured document (the contract), following pre-specified alternative rules. The electronic contract, which should be electronically signed, has two parts, the mandatory part, which contains the minimum information necessary to formalise an electronic contract, and the optional part, which contains optional information related to any kind of contract.

4.2.3 Production processes, publication and data models

Publishing houses, media companies and government agencies are developing opportunities to strengthen their own competitive position with the aid of innovative products and services as well as acquiring entirely new areas of the market. At the same time, they are confronted by a lack of systematic processes and methods that take heed of issues of DRM. Such processes are essential in order 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 that is manageable by typical midsize companies. This demand results from changing methods of data storage and large 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 cooperation within publishing houses as well as cooperation between companies; they should allow multiple uses of content through standardised asset management, and support the use of integrated information systems along with the production processes.

4.3 Legal, regulatory, private and public policies

The objective is to analyse and study legal and societal aspects of the DRM scenarios in question. Relevant research and results for the selected e-government scenarios have to be considered. The most important research challenges lie in the area of legal, regulatory, policy and societal aspects. The following four aspects are critical:

4.3.1 Data protection

A basic task will be to identify IPR in terms of elementary actions that require the consent of a rights holder, i.e., to 'copy', to 'public performance', to 'systematically access and extract elements from a data base', etc., [10,17]. There are also fundamental unsolved issues related to IPR in new kinds of information products, e.g. understanding which intellectual property rights are applicable to different information products and which parts of the products are protected. To protect data, it will be necessary to decide how relevant consent is to be obtained from a data subject, or work out alternative ways of obtaining the right to process the personal data involved. This will be a challenge, especially in the e-government domain and the health care sector, where the data will be of a sensitive nature but should be globally accessible to authorised personnel. Though co-ordinated by the data protection directive, different national states have implemented the provisions rather differently, especially with respect to sensitive data, of which the processing in many jurisdictions is subject to license from a national data protection authority. Thus, the inter-legal issues (jurisdiction and choice of law) have to be included.

4.3.2 Content policies

Content policies are developed on the basis of directives coordinating national copyright and related rights. 'Content' is a facile term covering a variety of material in different legal categories, copyrighted material and material subject to neighbouring 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 define precisely the concept of content, as it can differ depending on the kind of information product. In general, it can be described as the actual payload of the information product. Not only commercial publishers produce information products or content but, using modern information technology, authors themselves will more and more distribute their own work and end-users will increasingly contribute to the content. Often, the object of trade is not content but the usage rights associated with it, on the basis of which the purchaser will be able to use the content in accordance with the terms of licensing agreement, which will also include terms of payment.

4.3.3 Ethical aspects

Legal rules may not be sufficient for business models to operate, in which case they will have to be bolstered by more restrictive ethical rights. If data is to be protected, explicit trade practices must be laid down. 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, but this is a small problem compared to the legal and

ethical issues related to privacy, anonymity and identity. In general, everybody should be able to remain anonymous and to retain his/her privacy if they wish and if this is acceptable to the specific service in question. On the other hand, a human being may have a large number of roles that should be distinguished. For example, usage rights like private use or fair use are often different depending on the role of the user, and a license may only cover certain role-based usages. Therefore, it is hardly possible to build solutions that, in general, rely on the direct identification of human beings. Instead, most systems need to depend on indirect user identification, e.g. based on device identification.

4.3.4 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 (e.g. only authorised 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 being, it can be very difficult to understand what those complex sentences mean. However, when somebody buys an information product, it is essential to license or assign rights. 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.

4.4 Societal questions

The rights of the provider or rights holder must be weighed carefully against those of the end-user, within the context of the society in question, where electronic trade may be conducted in accordance with a new separate trade policy or with already existing trade policies. 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 one of its key objectives. This raises important societal aspects on DRM, as this may unnecessarily prevent people from accessing information or increase the digital divide between population groups. 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 typical 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 organisations create programs together and distribute them freely. This model is expected to expand and cover many walks of life.

4.5 Application domains and stakeholders

Today, we witness a lack of communication between application domains. Practitioners in one domain are frequently totally ignorant of the similar activities of their peers in other domains, 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 across disciplines. The same concepts and ideas often apply in many different areas, and those few who manage to abstract these concepts from one domain and apply them to the problems of another have often boosted research in that domain. Therefore, special attention has to be given to inter-domain communication and cooperation.

DRM is a key part of the future platform for application and service provision, and an architecture that balances the interests of the various stakeholders will be a key enabler of new applications; an ill-balanced architecture is a showstopper. Therefore, DRM enabled e-government solutions will have to address the needs of all stakeholders.

In the special domain of health, information for citizens or patients as a specific category of citizens must be reliable. Navigating through the information offered over the internet, this special group needs guidance in assessing and using that information. One way is under establishment, clearly naming the author and his qualification to do this job by his ID certificate (digital signature) and corresponding attribute certificates. Additionally, patient information should be certified by a certification body, e.g., a group of experts acting as evaluators counter-signing the document. This quality assurance procedure is inevitable in health-related e-government.

4.6 Harmonising and reusing other project's approaches and results

A completely model driven architecture covering all aforementioned domains involved in e-government, based on the Generic Component Model developed in the mid-nineties and deployed, e.g. for the European HARP project, seems to be the most promising approach [18,19]. By separating logical and technological views on systems and their components at meta level, components expressing concepts, behaviour, processes and rules, but also technical details, can be modelled and instantiated. The Generic Component Model considers the different views on components defined in the ISO Reference Model – Open Distributed Processing [20] such as the enterprise, information, computational, engineering and technology view. Enhancing the model by adding the dimension of granularity to the abstraction level can enable any construction of components, processes, policies, etc. Flexibly aggregating different components realises negotiation procedures. This approach is under deployment globally, e.g., in the revision of standards such as CEN ENV 13606, Electronic Health Record Communication or CEN ENV Health Information Systems Architecture (HISA) and includes security-related aspects. Regarding DPM and DRM, the ISO work item "Privilege management and access control" follows the stream described [21].

5 Methodology and DRM research centre

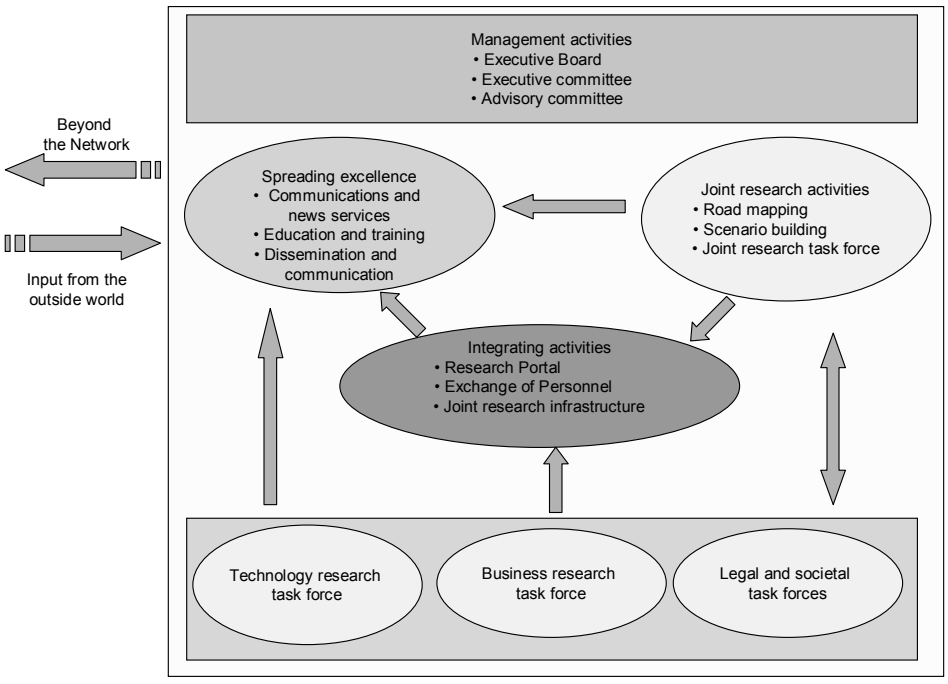
5.1 Scenario methodology – making the goals operative

The proposed approach aims to explore cross-discipline future systems that will successfully integrate DRM technology and its satellite concepts into a flexible e-government infrastructure. This is a complicated task since, at first sight, it seems that legal challenges related to the systems should be analysed 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 analysing them. Thus, it is almost impossible to say anything about the future using conventional methods. Instead, future research provides us with more suitable methods, especially scenarios that are useful when we want to describe what the world will be like, e.g. what e-government services will look like in ten years from now. In addition to providing us with adequate research methods, scenarios are excellent means of integrating and communicating ideas, views and concepts. Scenarios used in other fields of science are typically quite broad. On the other hand, it is sometimes useful to create very small scenarios or use-cases. We expect that e-government scenarios with regard to citizen-government interaction will be relatively narrow: they will merely describe simple possible services, interaction with which will not require advanced technological knowledge and understanding. However, there may emerge a need to develop bigger scenarios also (but this will be mostly on inter-agency cooperation within the scope of e-government). Our scenarios are to form a vision, depict possibilities and concerns that may exist in the future.

5.2 Integrating process

Figure 2 Integration process



The proposed approach 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. Therefore, DRM matters need

to be addressed from all perspectives and possible future obstacles, which will have to be overcome, must be identified. This goal can be achieved via a number of carefully planned activities, which collectively bring a high degree of long lasting integration. Figure 2 depicts the integration process/cycle with the main activities and task forces.

5.3 Establishing a virtual DRM research centre

The objective is to ensure that the necessary steps are taken towards forming a virtual organisation that will be self-sustained. Important questions that have to be addressed are:

- how to ensure that the network becomes the preferred unit of cooperation and reference point within DRM research globally
- how to create services that will lead to the self-sustainability of the network
- how to ensure sufficient anchoring to international organisations that run conferences, standardisation work and other scientific activities, and within the most important partners in DRM research.

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

6 Advantages for e-government

As noted in [22], the central issue in e-government is the application of ICT in governmental activities, both political and civil, in which both citizens and government institutions exchange information or ideas in order to improve existing and/or define new public administration services. The latest is achieved by introducing new digital products and services and their underlying business models [23]. These activities can be considered as an e-governmental value chain model linking 'trading' partners, like citizens, administrative agencies and constitutional institutions.

This e-governmental value chain model can be extended to situations in which governments exchange information or ideas with each other, and in which government and private companies communicate and negotiate. In the latter situation, private companies will provide government with value added services, such as web services [24], which will improve its ability to discharge its official duties. In this model, security [25] is a most important requirement for all actors, as is privacy. Since IPR ownership in such a shared ownership system is increasingly a problem area, any government that encourages the use of e-government must have plans and strategies [26] for the development and enforcement of IPR in such a way that the rights of all involved parties are protected. It must also enforce laws preventing the misuse by government of data provided by consumers to merchants or government, and the unjustified monitoring by government of transactions between businesses and consumers.

Consequently, DRM can be argued to be ideally suited to the needs of e-government, since it aims to protect IPR over digital assets, increases security, trust and privacy when information is exchanged over open networks throughout the entire value chain, i.e. from

producer to distributor to consumer, and potentially from consumer to consumer. Society in general, and the e-government community in particular, would, thus, greatly benefit from DRM, which will engender trust in e-communications [27], thereby building consumer and business trust in e-government services by preserving citizens' privacy.

In addition to the above, our proposed integrated framework will provide digital policy management and risk management from multidiscipline and inter-domain perspectives, and facilitate the automation of e-government activities. The major benefits include:

- it will enable government to make available electronically a large amount of information in a secure manner, which will open new business opportunities and improve services to citizens, e.g., eTaxation [25], eWelfare [24], etc.
- it will enhance the enforcement of IPR, which will improve credibility and will, thus, encourage the production of digital products and services
- it will boost eHealth, by protecting the integrity of medical records while at the same time making them easily and quickly accessible to health service personnel on a differential basis
- it will boost eEducation, by facilitating the easy and secure management of the creation, retrieval, trading and distribution of online learning objects and by supporting secure collaborative development [28,29].

7 Conclusions

In this paper we have described a DRM research framework, which aims to:

- integrate the traditionally separated DRM research communities across Europe (both at national and international level) in the fields of technology, business, law, ethics and social science, all of which are vital to understanding the issues related to DRM in the future and its use
- stimulate joint scientific research projects to gain insights into the fundamental issues and challenges associated with future DRM systems
- create a self-sustainable set of knowledge-spreading activities through liaison with end-user communities, industries, standards bodies and government organisations.

We have proposed an integrated multidiscipline and inter-domain approach to address the vision of *trust and confidence* in e-government services and satellite electronic activities, to wit, communication, business, entertainment, learning, health and generic-services. We have also highlighted how DRM will benefit e-government. It is our considered opinion and firm conviction that such an integrated research framework will help governments understand the uptake of the knowledge-based digital economy in the context of e-government.

References

1 Iannella, R. (2001) 'Digital rights management (DRM) architectures', *D-Lib Magazine*, Vol. 7, No. 6, Available from: http://www.dlib.org/dlib/june01/iannella/06iannella.html

2 Feigenbaum, J., Freedman, M.J., Sander, T. and Shostack, A. (2001) *Privacy Engineering for Digital Rights Management Systems*, Available from: http://www.pdos.lcs.mit.edu/~mfreed/docs/privacy-engineering.pdf

3 Cohen, J.E. (2003) *DRM and Privacy*, Available from: http://www.law.berkeley.edu/institutes/bclt/drm/papers/cohen-drmandprivacy-btlj2003.html

4 Electronic Privacy Information Centre (2002) *Digital Rights Management and Privacy*, Available from: http://www.epic.org/privacy/drm/

5 Hoffman, L.J. and Carreiro, K.A.M. (1997) *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

6 Brose, G., Koch, M. and Lohr, K.P. (2001) 'Integrating security policy design into the software development process', *Technical Report B-01-06*, Institut fur Informatik Freie Universität Berlin, Germany

7 Delgado, J., Gallego, I. and Perramon, X. (2001) *Broker-Based Secure Negotiation of Intellectual Property Rights,* ISC'01, LNCS 2200, Springer-Verlag.

8 Abie, H. (2002) '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*, 2-4 September, pp.185–194.

9 Blobel, B. and Baum-Waidner, B. (2001) 'Current security issues faced by health care establishments and resulting requirements for a secure health information system architecture', in The ISHTAR Consortium (Ed.) *Implementing Secure Health Telematics Applications in Europe*, *Series Studies in Health Technology and Informatics*, Vol. 66. IOS Press, Amsterdam, pp.101–147.

10 Bing, J. (2002) *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.

11 Risk Analysis Resource Page (2001) Norwegian Computing Center, Available from: http://www.nr.no/~abie/RiskAnalysis.htm

12 AS/NZS 4360 (1999) 'Risk management', *Australian Standard*, 12 April 1999-09-17.

13 Norwegian Standard (1991) *NS 5814, Requirements for Risk Analysis*.

14 Dimitrakos, T. and Bicarregui, J. (2001) 'Towards modelling e-trust', *3rd Panhellenic Symposium on Logic Anogia Academic Village*, Crete, Greece.

15 Pitkänen, O. and Välimäki, M. (2000) *Towards A Digital Rights Management Framework*, IEC2000, Manchester, UK.

16 Chesbrough, H. and Rosenbloom, R.S. (2002) *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.

17 Bing, J. (2002) *Intellectual Property Exclusive Rights and Some Policy Implications*, Norwegian Research Centre for Computers and Law, University of Oslo, Norway

18 Blobel, B. (2000) 'Application of the component paradigm for analysis and design of advanced health system architectures', *International Journal of Medical Informatics*, Vol. 60, No. 3, pp.281–301.

19 HARP Consortium, Available from: http://www.ist-harp.org

20 ISO/IEC 10746-2 'Information technology – open distributed processing – reference model: part 2: foundations'.

21 Blobel, B. and Nordberg, R. (2003) 'Privilege management and access control in shared care IS and HER', in R. Baud, M. Fieschi, P. LeBeux and P. Ruch (Eds.) *The New Navigators: From Professionals to Patients, Series Studies in Health Technology and Informatics*, Vol. 95, IOS Press, Amsterdam, pp.251–256.

22 Wassenaar, A. (2000) 'E-governmental value chain models e-government from a business (modelling) perspective'*, Proceedings of 11th International Workshop on Database and Expert Systems Applications*, pp.289–293.

23 Timmers, P. (1998) 'Business models for electronic markets', in Y. Gadient, B.F. Schmid and D. Selz (1998) *EM – electronic commerce in Europe*. *EM – Electronic Markets*, Vol. 8, No. 2, July, pp.3–8.

24 Medjahed, B., Rezgui, A., Bouguettaya, A. and Ouzzani, M. (2003) 'Infrastructure for e-government web services', *Internet Computing*, *IEEE*, Vol. 7, No. 1, pp.58–65.

25 Leitold, H., Hollosi, A. and Posch, R. (2002) 'Security architecture of the Austrian citizen card concept', *Proceedings of 18th Annual Computer Security Applications Conference*, pp.391–400.

26 Porter, M.E. (1996) 'What is strategy?', *Harvard Business Review*.

27 Galindo, F. (2001) 'Public key certification providers and e-government assurance agencies: an appraisal of trust on the internet, database and expert systems applications', *Proceedings 12th International Workshop*, 3-7 Sept., pp.345–349.

28 Liu, Q., Safavi-Naini, R. and Sheppard, N.P. (2003) 'Digital rights management for content distribution', *Proc. Australasian Information Security Workshop*, Adelaide, Australia.

29 Johnson, C., Montague, P. and Steketee, C. (Eds.) *Conferences in Research and Practice in Information Technology*, Vol. 21, ACS, pp.49–58.