Chapter 8

Conclusion and Future Work

As defined in Section 1.3, the goal of this doctoral thesis has been to develop methods and tools for exchanging and processing XML-based rights expressions, in particular electronic contracts. This section sums up the findings the thesis at hand delivers to the research community in this field. For details, please refer to the respective sections in the earlier chapters.

Methods for the exchange of rights expressions

The methods developed in the work at hand shall support the overall goal of creating rights expressions that are easily exchangeable with respect to their content. In other words, it is necessary to ensure that the receiver of a rights expression can understand its content and semantics as it has been intended of the sender. Within this thesis, the following methods have been developed to support the processability of electronic contracts in software services:

- *Tailoring electronic contracts*. The work provides an analysis of basic information objects that occur in rights expressions and their relations. Analysing electronic contracts and their structure is important for their reliable processing. Electronic contracts in particular can be processed in various usage scenarios, such as access control, accounting, customer relationship management, etc. For each usage scenario
a specific agreement category has to be developed that describes objects that are relevant in this usage scenario. Accordingly, a process is introduced, that supports the tailored composition of agreement categories and thus electronic contracts depending on their later usage(s).

- **The generic Contract Schema (CoSa).** For a standardised processing of rights expressions and in particular of contracts, the concept of the generic Contract Schema (CoSa) has been developed. The CoSa serves as abstraction level for various rights expression languages or other representations of rights expression respectively contracts. With the concept of CoSa comes a generic API that allows to query all contract information represented in the CoSa format. The CoSa API stays consistent, also if the CoSa is application-specific.

- **The contract life cycle.** To build the bridge to the economic environment of exchanging and processing electronic contracts, the "contract life cycle" has been defined corresponding to the legal phases of contracts. With the help of the contract life cycle the developed methods and tools, as well as the defined terms have been classified to the respective life cycle phase. For example, the rights expression generator supports the negotiation phase of electronic contract, whereas the rights expression wrapper supports the offer placement as well as the offer confirmation, respectively the conclusion of the contract. Along the phases of the contract life cycle additionally the management issues are listed that are of importance, such as 'When is an electronic contract valid?' or 'What technical means have to be applied, as soon as the electronic contract is executed (to avoid double-spending)?'.

- **The enforceability matrix** that has been developed within this work helps to classify which information in rights expressions can be enforced as intended by the issuer. Three general criteria have been identified which facilitate the classification.

- **The rights expression communication model.** From Shannon’s basic communication model a rights expression communication model has been derived that allows for particular needs of rights expression exchange. The developed model takes into account that rights expressions are exchanged in a platform-independent format and require se-
curity means to be transmitted safely. The four resulting stages that rights expression have to pass between sender and receiver are: rights expression generator, - wrapper, - unwrapper, and - interpreter.

Besides the above mentioned methods a system has been developed for the description and classification of DRM systems respectively their functionality. Additionally the perspectives of DRM systems have been identified that help understanding the various impacts (e.g. legal, social, technical, etc.) of DRM systems.

Tools for the exchange of rights expressions

The tools developed in this thesis implement the rights expression exchange model mentioned above. The tools have been developed as software components that can be used autonomously or in combination as rights expression exchange framework, comprising the four sub components (tools):

- The rights expression generator transforms original rights information of a DRM component or actor (e.g. a contract party) into code, resulting in a rights expression message. This message is formulated in a rights expression language. In return, the rights expression generator adopts the syntax and semantics of the open digital rights language (ODRL) version 1.1.

- The rights expression wrapper and - unwrapper. Depending on the usage scenario, various security services have to be applied to the rights expression before transmitting it, e.g. digitally signing and packing the rights expression in a secure container. These services are provided by the rights expression wrapper. The rights expression unwrapper is the complementary component to the rights expression wrapper. It unwraps and also unpacks the rights expression after transmission and provides for the extrinsic checking of the digital contract, such as checking the contract integrity, authenticating the rights expression sender, and verifying the digital signature of rights expression.

- The rights expression interpreter is an open and extensible tool for the interpretation of rights expressions for subsequent processing. The interpreter implements the concept of the generic CoSa. It is currently able to interpret ODRL instances and to transform them into an application-specific CoSa. The application-specific CoSa can then be queried for the rights information via the CoSa API. Thus, ODRL
rights expressions are machine readable, and processable in various applications respectively usage scenarios.

Apart from this thesis, we are not aware of any other comprehensive study that supports methods and tools for the entire exchange task of rights expressions and for their subsequent processing. The developed methods are of generic nature and independent of any particular technology (e.g. a programming language or a rights expression language). The tools are prototype implementations that are open and extensible. They have well defined interfaces that assure its (re)use in various environments and ease its integration into existing systems. The implementations are coded in an appropriate programming language, reuse existing technology, and consider all relevant standards. The tools prove the correctness and usability of the introduced methods tailored contract composition, rights expression communication model, CoSa, and enforceability.

Taking everything into account, I come to the conclusion that the introduced methods and tools have the potential to bring forward current technology for the exchange of rights expressions (in particular the exchange of electronic contracts) in order to improve the interoperability of digital rights management systems and thus to quicken future electronic commerce.

**Future Work**

The work addresses a large number of subjects in the area of rights expression exchange and processing. Therefore, the future work to be done is equally broad. In the following paragraphes the fields of future work are mentioned that have my particular interest.

- The implementation of the rights expression interpreter has provided a detailed insight to rights expression languages. Due to the specialisation in certain applications respectively domains and to the few current usages of both XrML respectively MPEG 21 REL and ODRL they lack a well-defined data model for rights expressions and comprehensive, unambiguous, formal semantics. The lack of formal semantics considerably restricts the clarity of all existing RELs. Furthermore, today's RELs are not sufficiently designed for the later processing in software services. Consequently, the development of comprehensive formal semantics is a fundamental issue of future work in the field of
RELs. Also the introduced rights expression languages are not designed to support service level agreements. A subject to future work is an analysis, whether the predominant RELs are respectively should be able to express service level agreements.

- My investigations in the field of RELs have resulted in a close cooperation with Renato Iannella (founder of the ODRL initiative) and the people from ContentGuard who are developing ODRL respectively XrML. We intend to continue this fruitful cooperation in order to develop more sophisticated RELs. My participation in the ODRL initiative has resulted in the organisation of an international ODRL workshop in April 2004 in Vienna, where the leading researchers in the field of rights expression languages are going to meet to share their research findings. The achievements of the workshop will certainly have an impact on the next version of ODRL.

- Future work in this field will also be concerned with finding an adequate transport medium for electronic contracts, e.g. x509 certificates [IT93a]. Sandhu and Park have introduced smart certificates for attribute services on the web [PR99]. They use the extension field of X.509v3 certificates to bind attributes to a subject (party). In an other contribution Sandhu and Park [PS99] present an implementation where the extension field of a X.509v3 certificate is used to assign role information to a subject. Based on the subject’s role information, web servers use roles instead of a user’s identity for access control purposes. In my future work smart certificates, respectively the extension field of x509 certificates shall be investigated as a transport medium for electronic contracts with the help of a prototype implementation.

- This thesis addresses the perspectives of DRM systems and mentions their interrelation. For example, intentional perspective of a DRM system heavily influences its functions, respectively the technical implementation. Therefore, I consider it necessary to now investigate the concrete number of relations and their effect respectively the gravity of dependencies between the six perspectives. For example, a catalogue could be helpful that guides strategic and technic DRM system developers through system reengineering and change management.
• The thesis at hand addresses various security mechanisms that are required in DRM systems respectively in a rights expression exchange framework. Each of the security mechanism could be addressed and implemented in more conceptual detail. For a rights expression exchange framework, for example, the tamper resistance of the distinct components needs to be addressed for a concrete application. In this context it is also important to address the processing of electronic signatures in more detail. For example, for electronic contracts it has to be assured that the right people have signed the contract in the correct sequence.

• The most important challenge that future work should respond to is the creation of a standardised respectively globally unique vocabulary for rights and conditions, as they are available for individuals (e.g. x509) or resources (e.g. DOI), to improve the explicit semantics of rights expression languages. The MPEG 21 initiative is currently working on a uniform framework for the expression of rights in the course of developing part 6 of the MPEG 21 standard, a uniform data dictionary for rights expressions.

• To make sure that the application of electronic contracts is an absolute convenience for all future participant of e-commerce, is has to be taken care of the privacy matter in this context. It is important to design a process that ensures privacy for all contract parties, i.e. that addresses the management of privacy issues throughout the entire contract life cycle and covers the following issues: Who decides on the contract content? Is the contract publicly available in whole or part? etc.

• For the mapping from one rights expression language to the other, simple tables have been used in this thesis. For mapping the semantics from more than two rights expression languages a "rights ontology" needs to be developed.