Comparison of Enterprise Digital Rights Management systems

M.H. van Beek

Master Thesis
Computer Science MT
Advice report Aia Software
Thesis number 565
June 22, 2007

Radboud University Nijmegen
Computer Science
Supervisor: Dr. Martijn Oostdijk
Management Science
Supervisor: Drs. Pepijn Vos
Aia Software
Supervisor: Drs. Paul Dirven

Preface

Illegal distribution of audio and video has been limited since large companies introduced Digital Rights Management systems. By using the same techniques inside companies, it is possible to protect classified information to be distributed to unauthorized people and assigning sophisticated rights to digital documents. Several companies developed these so called EDRM systems. These innovations triggered Aia Software and me to do research on the subject and to write this Master Thesis.

After six months of intensive research, I would like to thank my friends, family and especially Pepijn Vos from Management Science, Martijn Oostdijk from Computer Science and Paul Dirven from Aia Software for their support during the research project. I have learned a lot during this period at Aia Software, the university and even at home when writing this thesis. In this way, I would like to thank employees from Aia Software for their contribution as well. I consider EDRM to be a very interesting topic and I am really curious about new innovations and the potential practical implementations at organizations in the future. Although I think restrictions on digital content can be used to remain competitiveness within organizations, I do hope these organizations will not restrict employees too much by using EDRM systems.

Executive summary

Since the last few years, security of digital documents within organizations has become very important. Because loss of digital content at organizations has been increased, there is need to provide a solution to limit illegal distribution. Distribution of classified information leads to significant loss at organizations [AH05b]. Next to this, standard encryption methods do not provide an overall solution against distribution, because authorized persons still have all rights to distribute digital content. Enterprise Digital Rights Management systems were analyzed to be a potential solution for Aia Software during this research project. By using Enterprise Digital Rights Management within organizations, digital content can be secured no matter where it is distributed by offering sophisticated rights to privileged users. EDRM technology is rather new and EDRM innovations have been increased since these last few years. Aia Software would like to use an EDRM system to secure digital content produced by customers and the produced content by their own developed application (ITP). By using literature, technical knowledge about EDRM is gathered and a *selection criteria model* was built, to create business case specific criteria. After development of a selection criteria model, all current EDRM systems and their properties were gathered from literature and practice to be used next to business case specific inputs from Aia Software. Because real customers are not available, several inputs from Aia Software were used. These inputs all resulted into an evaluation and advice for using a specific EDRM system for Aia Software. To support the inputs, technical literature, testing these systems, and contact persons from EDRM developing companies where used to reveal the needed information. RMS, DOFS, Authentica and Adobe are evaluated with their EDRM solution. As a result of the research project, RMS was considered to be the best current existing solution for Aia Software. Several differences between these EDRM systems were found; wherefore it is necessary to gather business case specific requirements from customer organizations to choose the most appropriate solution. Because not all important requirements from Aia Software were supported by RMS, it is necessary to keep up with new EDRM innovations and new developed EDRM systems to provide the best possible EDRM solution to customers.

Contents

Chapter 1

Introduction

This introduction is divided into describing background, research objectives, relevance, purpose of document and a document guideline.

1.1 Background

Recently, Apple took three online publication companies (Powerpage, Apple Insider and Think Secret) to court for publishing detailed information on new unannounced Apple products [Fri04]. Apple's goal was to force the publishers to reveal their sources on who leaked the information and violated Apple's non-disclosure agreements. The fact that Apple is one of the major innovative organizations in the computer industry and has not been able to protect their trade secrets from being distributed to unauthorized people, implies there is need to prevent distribution of digital content to unauthorized people. Apple is not the only organization with the problem, that a lot of confidential information leaves the control of their owners. In this way, there have been many high estimates on the cost of intellectual property losses [AH05b]. Since a few years, several EDRM providing solutions are offered to be used by organizations to support distribution of digital content by using sophisticated privileges. This research project is done as a master thesis to support Aia Software for choosing an appropriate EDRM solution to protect their customer's documents (digital content).

1.2 Aia Software

Aia Software provides products and services to customer organizations, which are based on automated digital content generation. The *Intellectual Text Processing (ITP)* client-server based solution offers organizations the possibility to develop document models, which can be used to develop large amounts of automated digital content according to the requirements of their customers with related data extracted from databases. These customer organizations are threatened by distribution of digital content to unauthorized persons, for which Aia Software would like to offer a complete system to prevent loss of information to unauthorized recipients and competing organizations. During this research project, knowledge about Enterprise Digital Rights Management solutions is gathered to provide an advice for Aia Software's requirements.

1.3 Enterprise Digital Rights Management

Traditionally, data has been encrypted to secure digital content. After decryption of the content, users still have all rights to distribute content to unauthorized persons. File system protection has been used to support restrictions on users, files and directories next to these encryption techniques. However, these ways of protection really do not offer a complete solution against the underlying problem. Because encryption only prevents theft against unauthorized users, it is still possible to lose content directly or indirectly by distribution of authorized users. In this way, important digital content is not secure against illegal distribution by attackers and/or inaccurate users. An appropriate solution should at least offer protection mechanisms with more sophisticated privileges on digital content and users. Recently, security of digital content has become very important for many organizations to remain innovative and maintain competiveness.

DRM technology has mainly been used by record companies to protect music against mass distribution on the internet [App03]. Other applications with DRM technology such as securing e-books have been less successful [Oue06]. EDRM is another DRM technology based system, which aims to protect digital content for organizations against distribution to competitors by authorized or unauthorized users. An EDRM system provides the ability for users to assign access control rules on digital content to restrict users, which will work as prescribed or will not allow access at all. While access control rules are useful, it would be better if those rules were more sophisticated than only read and modify. Other control rules like restrictions on printing and excerption should be covered as well. Enterprise Digital Rights Management systems aim to provide sophisticated security mechanisms.

Nowadays, there are a few organizations which provide such technology. During this investigation, EDRM systems where analyzed resulting in an advice for Aia Software.

1.4 Objectives

During this research project, EDRM systems and potential usage for Aia Software are discussed and translated into an advice for further research and development. To provide an advice, the following question is used:

Which EDRM solution can be used to support Aia Software's technical requirements?

Because development of an entire new EDRM system would take an innovative organization at least 3 years, it is recommended to use existing EDRM systems or EDRM components for integration with an existing infrastructure [Oue06]. In this way, the research project is concerned with comparison of existing EDRM systems and *not developing* a whole new EDRM system. The research question results into achieving the following objective:

Providing an advice about current EDRM systems according to technical requirements for Aia Software.

To complete this objective, it was necessary to divide it into the following sub objectives:

1. Providing a model with technical selection criteria to be used on a specific business case next to current EDRM systems and their properties, which results into an advice for Aia Software.

2. Providing a set of EDRM systems and related properties, which can be used to compare systems with corresponding criteria.

3. Providing business case specific input to be used with the model and current EDRM systems and their properties to perform comparison of EDRM systems.

4. Providing an advice based on the previous described sub objectives.

1.5 Relevance

The research relevance is described for science and organizations. The research project is done for Aia Software, but can be used for other organizations as well to choose an appropriate EDRM solution.

1.5.1 Science

The first part of the research project is concerned with defining Enterprise Digital Rights Management and fencing of the project. Reliable scientific literature is analyzed to realize this goal and to define EDRM in a complete possible way. Scientific literature is collected and used to develop a model, which can be used in future practice for specific business cases. Literature has been used as a resource to collect EDRM specific functional and non-functional requirements, which are used to develop a *Selection Criteria Model* to support organizations in a complete possible way. This selection criteria model is used for Aia Software as a business case input to develop business case specific criteria. These Chapters can be used for future research about the subject. The definition analysis provides a dynamical way to define a business case specific complete definition in comparison with existing literature. The developed criteria can be used to develop EDRM requirements or to compare existing and new EDRM systems. Because gathering requirements can be done in several ways and there is not just one right way to gather requirements, this research project can be used to research further engineering methodologies in general by using methods from this research project. EDRM requirements from literature are used to develop a theoretical Selection Criteria Model to be able to compare several EDRM systems. The model is developed without implementation of own business case specific inputs and is used with Aia Software to create business case specific results. Such a model has not been available till now, and offers scientists to expand the model by using new available innovations. EDRM systems and related properties are analyzed and used to compare with business case specific results from the model. By using literature, the model was used to develop important requirements for an organization. Because the model can be used directly at organizations, this offers science to create more interaction with these organizations, to develop better EDRM solutions. In this way, conclusions and recommendations result into choosing an appropriate EDRM system with underlying differences. By using this research project it is possible to analyze and improve the used techniques and create better EDRM solutions as was done in the past.

1.5.2 Aia Software

The relevance for Aia Software is to gather more knowledge about EDRM and the current systems, which can be used to support their current infrastructure and creating a complete solution to customers. Distilled recommendations during the research project will Aia Software help to compete against other software providing organizations and in this way fulfilling the customer demands in a more complete way. Because the potential EDRM system should be integrated with the current software and hardware infrastructure, choosing the right EDRM system is an essential step before implementing it. By using scientific methods created during this project, it is possible to collect more knowledge about the subject. Customers can be persuaded more easily to choose for solutions provided by Aia Software, because the developed models could offer completeness and customer satisfaction.

1.5.3 Other organizations

The project can be relevance for other organizations as well. These organizations might be interested in using an EDRM system for their own organization or to sell it to other organizations. In this way, it is possible to use the developed models in the same way as described for Aia Software. By using this research project, it is possible to compete against other organizations like Aia Software by using the same models and strategy.

1.6 Purpose of document

This document provides a complete overview of the followed phases during the EDRM research project described in a scientifically justifiable way. The main goals of the project are divided into several other goals, which are all completed with each an own particular strategy. The purpose of the document is to provide a detailed overview of the research project as a whole with related results and motivation. Next to this, the document can be used for further research about the subject in many ways. Conclusions and recommendations can be used as a fundamental start for new research projects to support implementation of EDRM systems.

1.7 Document guideline

This document is described in a chronological way as the project was done. The following Chapter 2 describes an overall *research method*, which was used to complete

the project. The project is divided into several phases and each Chapter contains an own *introduction*, *research method* section with used methods for completing the related sub objectives. After providing the *results* per Chapter, *conclusions* are described as well.

The first objective concerns providing a *selection criteria model*, to be used for organizations to create appropriate selection criteria. This selection criteria model is created by developing a *definition analysis* (Chapter 3) and *requirements analysis* (Chapter 4) first according to the software methodology called the *waterfall model* [Som04]. Chapter 5 describes the developed *selection criterion model* by using the previous developed requirements. This selection criteria model was necessary to complete the first objective. After developing the model, there was need to gather a *set of current EDRM systems* (Chapter 6). To be able to compare EDRM systems, it was necessary to create a set of *system properties per EDRM system*. These EDRM system properties are described in Chapter 7. By using the model from Chapter 5, it was possible to create *EDRM specific selection criteria for Aia Software* in Chapter 8. The properties per EDRM system from Chapter 7 and the results from the selection criteria model from Chapter 8 were used to perform an *evaluation* in Chapter 9. After evaluating these systems, *conclusions and recommendations* are described in Chapter 10, which provides an advice for Aia Software. Next to this, recommendations are given for several related organizations and science in general to support future innovations.

Chapter 2

Research method

The main objective during this research project is considered as *providing an advice for using EDRM according to technical requirements from Aia Software.* This objective is divided into the following sub objectives:

1. Providing a model with technical selection criteria which can be used on a specific business case next to a set of current EDRM systems and their properties *(Selection criteria model).*

2. Providing a set of EDRM systems with related properties per EDRM system *(EDRM systems and EDRM system properties).*

3. Providing business case specific input as a result from the selection criteria model to be used for comparison *(Selection criteria Aia Software).*

4. Providing an evaluation based on the results from the selection criteria model and the EDRM system properties *(EDRM system evaluation).*

5. Providing an advice based on the previous results *(Conclusions and recommendations).*

In this Chapter the research methods are described per sub objective divided into phases. The first sub objective is to *develop a selection criteria model* and is divided into three phases (definition analysis, requirements analysis and selection criteria model). The second objective is to *create EDRM system properties for all current EDRM systems.* This is done by performing phases 4 and 5. The third sub objective is to *create business case specific input by applying the Selection Criteria Model on Aia Software.* This is done in phase 6. The next objective is to *evaluate EDRM systems by using the results from the selection criteria model and the EDRM*

system properties (phase 7). As a result from this research project, there was need to *create an advice* by using the previous phases. Each phase is shown in the following research model (figure 2.1) and the input and output relations between these phases are visualized by arrows. Several phases have multiple relations with other phases. After completion of all phases *conclusions and recommendations* are provided. The following sub sections describe the relations between the phases in further detail.

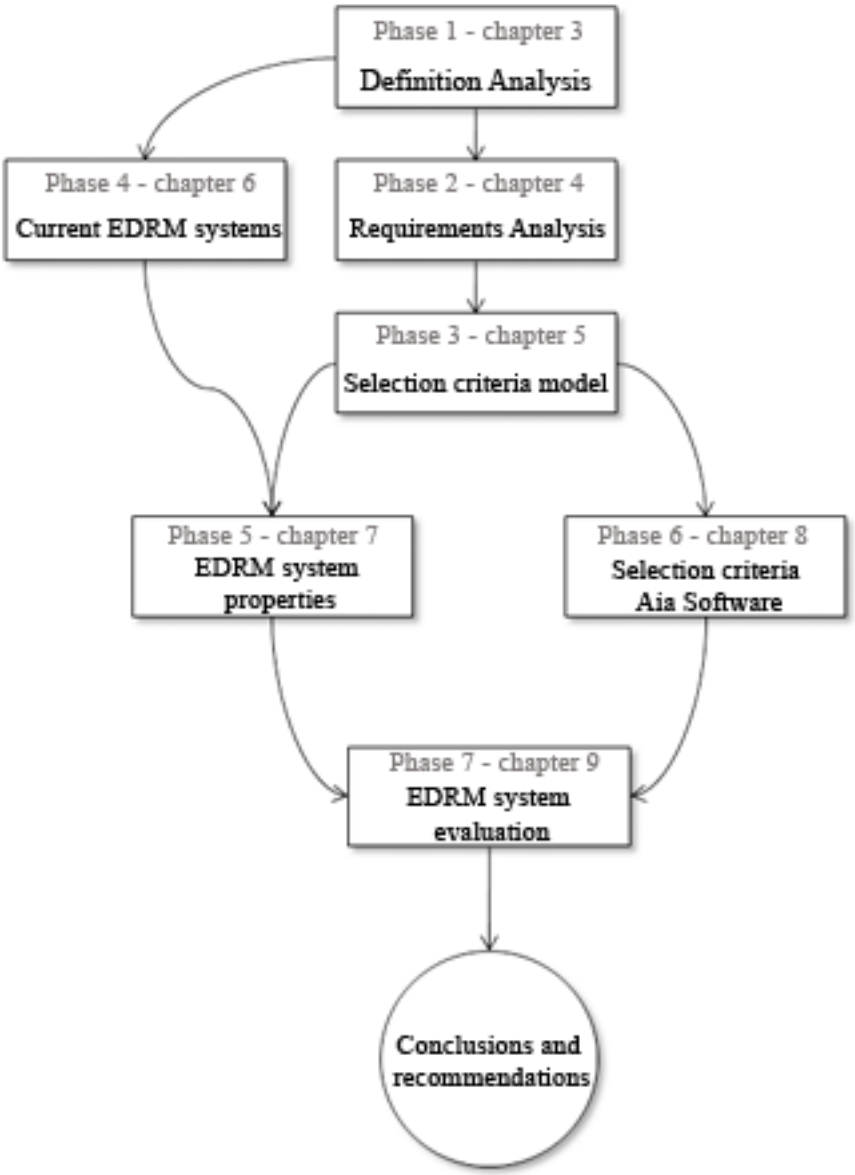

Figure 2.1: Research model

2.1 Definition analysis

To be able to create the required selection criteria model (phase 3), it is necessary to create technical EDRM requirements. Because a software engineering methodology offers the possibility to create technical requirements, it is necessary to fulfill the first few steps of this engineering practice till the requirements are gathered. The definition analysis (phase 1) is the first step of an engineering process and is used to create a complete definition for EDRM. This definition is considered as a result from this phase and is used as an input for the requirements analysis (phase 2). The definition is also used during a following phase as shown in the research model when gathering a current set of EDRM systems (phase 4). This definition analysis has the goal to formulate a complete possible definition for EDRM. Because EDRM and DRM are often confused and definitions from literature are not always specific, differences between these subjects are gathered to support future phases. A more detailed research method is described in the section definition analysis (Chapter 3).

2.2 Requirements analysis

The second part of the software engineering practice is described as the requirements analysis (phase 2). The goal of this phase is to use a requirements process to gather technical EDRM requirements from stakeholders. Although other methods are often used to gather requirements, this phase is based on gathering literature and results into a complete set of EDRM specific technical requirements to be used in the following phase (selection criteria model). The technical EDRM requirements are used develop the selection criteria model. The gathered requirements are based on literature and are not used on Aia Software at this point. In this way, these requirements are defined as universal requirements. These requirements could be used as guidelines to create business case specific requirements in a following phase. The requirements analysis is considered as phase 2 and is described in detail in Chapter 4.

2.3 Selection criteria model

During phase 3 there was need to build a universal selection criteria model, which could eventually be used on business cases (Aia Software during this project). The detailed description of how these selection criteria are gathered, used, provided with an importance and measurement are described in Chapter 5 *Selection criteria model*. This selection criteria model is used as an output for this phase and is used

as an input for *Selection criteria Aia Software* (phase 6). Because it is necessary to compare EDRM systems technically, it is necessary to create a measurement mechanism for these EDRM systems. The following tasks are needed to create a selection criteria model:

1. Developing a complete set of technical functional and non-functional EDRM criteria.
2. Business case applicability.
3. Providing a measurement for criteria with the EDRM system properties.
4. Assigning a mechanism to verify the importance per criterion.

According to the first task, it was necessary to gather a complete set of possible technical criteria about EDRM. The previous phases 1 and 2 are used for collecting these requirements. Aia Software does not have the experience and knowledge to reveal these criteria. Next to this, the system should be implemented for potential customers in the future. Real (customer) stakeholders are not available during the research project. Because of these reasons, there is need for knowledge and experience about the subject. In literature, experiences are gathered from real life and could be used as a fundamental resource to create these selection criteria. During the research project technical requirements are gathered and translated into selection criteria. To be able to translate the gathered requirements (phase 2) into selection criteria (phase 3), it was necessary to add an *importance* and *measurement* mechanism to each requirement. The selection criteria model offers organizations to create selection criteria and allows them to compare current EDRM systems by using the following phases. Before revealing the business case specific selection criteria from Aia Software, phases 4 and 5 were completed for analyzing the current EDRM systems on the market.

2.4 Current EDRM systems

Because there is no need for developing a new EDRM system, it was necessary to compare current existing EDRM systems as a potential solution for Aia Software. In this Chapter, it was necessary to gather information about which EDRM systems are available. These EDRM systems are used for evaluation in a following Chapter. The following tasks were performed in this phase:

1. Creating demands to verify systems to be EDRM.

2. Creating a set of existing EDRM systems.

The first task was to create demands, which could be used to verify which systems are EDRM. Because the definition analysis was used to create an EDRM definition, it was possible to use the definition as a measurement to verify a system to be EDRM. Internet search engines, scientific literature were used to find these EDRM systems. Also information from research company Gartner is used to create this set of EDRM systems. By giving an overview of the overall working of these systems, the earlier developed definition can be used to define these systems to be EDRM. When these EDRM systems were gathered from the used resources, it was possible to go on with the following EDRM system properties (phase 5).

2.5 EDRM system properties

To be able to create an advice, it was necessary to compare EDRM systems. During this phase properties per EDRM system are gathered by using the selection criteria model. The model uses requirements with added *measurements*. These measurements define how each property per EDRM systems could be measured. In phase 4 a set of EDRM systems is gathered. By using these previous phases, it was possible to provide properties per EDRM system. A more specific research method with results is described in Chapter 7.

2.6 Selection criteria Aia Software

In phase 3 (Chapter 5), a selection criteria model was built. This model is used on a business case provided by Aia Software and the results from the model are gathered in this phase 6 (Chapter 8) by using interviews with the director of Aia Software. The previous objectives resulted into creating a Selection criteria model (phase 3), a set of current EDRM systems (phase 4), a set of properties per EDRM system (phase 5). This phase resulted into a (6) set of important business case specific criteria with related importance. The importance was introduced in the selection criteria model and is now applied on the business case. By using the EDRM system properties from the Chapter 7 and combining them with the selection criteria from Aia Software, it was possible to evaluate the EDRM systems.

2.7 EDRM system evaluation

After performing the selection criteria model on Aia Software (phase 6), it was possible to use it next to the EDRM system properties (phase 5). During this phase the important criteria are evaluated by using the most important EDRM system properties of all current EDRM systems. To be able to compare EDRM systems, it was necessary to create a measurement technique. Therefore grades were assigned per property according to the prescribed measurement. This resulted in a list of properties with related degrees. A detailed description of how these properties were measured is described in phase 7 *EDRM system evaluation* (Chapter 9). This section results in a comparison of the system properties and the measurements from these EDRM systems according to the importance of Aia Software. In Chapter 9, the research method, results and conclusions are described in more detail. The results from this phase and all other previous phases are used in Chapter 10 to provide conclusions and recommendations as an advice for all related stakeholders as described in Chapter 1.

2.8 Summary

In this Chapter a research method is described divided in phases and related Chapters in this document. The following Chapters describe the gathered results from the research project. Each following Chapter is described with an introduction, detailed research method, results and conclusions. The first phase *Definition analysis* is described in the next Chapter.

Chapter 3

Definition analysis

The definition analysis was the first developed phase during the project and resulted into a business case suitable definition to be used during following phases. The main goal of the definition analysis is to develop a definition of EDRM for Aia Software as complete as possible by using available literature. Next to this, in literature sometimes terminology about DRM and EDRM are confused. An additional goal of this chapter is to disambiguate the notions of DRM and EDRM, which are sometimes confused in literature. The following section describes the detailed research method for developing this definition.

3.1 Research method

The objective during this *definition analysis* results into answering the following question:

What is EDRM according to Aia Software?

To be able to answer this research question, several steps needed to be performed and are described in the following sections including justification.

3.1.1 Information Technology system

First of all, there is need to provide a definition for Information Technology systems. By defining information technology systems first, it is possible to:

1. verify literature to be correct and usable during the project,

2. verify EDRM is really about software engineering practices,
3. support the software engineering waterfall methodology for the first two phases.

This section results into answering the following question:

What is an Information Technology system according to literature?

After developing this definition, it was possible to use correct literature to analyze EDRM during this research project and to use the developed research method.

3.1.2 EDRM literature analysis

The next step is to gather literature about EDRM and analyze this into a complete common definition. Similarities and differences are gathered as functions and definitions (Appendix A and B) and used to create a complete general definition. Because literature does not provide us one formal and complete definition, this research will contribute to science by providing a method, which results into a definition and can be used as a standard for future business cases. In this section the following research question is answered and results into a complete textual definition:

What is EDRM according to literature?

3.1.3 EDRM according to Aia Software

By gathering functions and definitions from literature (Appendix A and B), a complete possible definition is developed and needs to be verified with Aia Software. This is done by using the *EDRM literature analysis*. The complete created definition from literature is translated into questions, which were answered by Aia Software. These questions can be used by other organizations as well to develop an own specific EDRM definition. The set of questions are defined as *EDRM definition model* and is described in Appendix C. The developed definition by Aia Software is used as an input for the *Requirements analysis*.

During this definition analysis, there was need for fencing off the project by creating a definition, which was suitable for Aia Software. There was need to answer the following research question:

Which definition of EDRM can be used by Aia Software?

The following sections describe the results according to the research method. After describing these results, conclusions are mentioned to complete this phase.

3.2 Information technology systems

The first step within this phase was necessary to verify our first theorem about EDRM systems. The theorem is described as follows:

Theorem 3.2.1 *EDRM systems can be seen as a special case within the set information technology systems.*

If our theorem is sound, EDRM systems can be developed using (parts of) general system and software engineering methodologies. In this way, it is possible to use software engineering practices to create EDRM specific requirements (phase 2). In this phase a definition is developed, which can be used to verify a system to be an information technology system. After defining information technology systems, it was necessary to analyze and define EDRM. After defining EDRM systems it was possible to verify our theorem. Recommended literature is used as a definition to proof our theorem [Som04]. The following definition is used to define *systems*:

Definition 3.2.2 *A system is a purposeful collection of interrelated components that work together to achieve a common objective.*

According to this definition, a *system* contains one or more (sub) components, which can work independently, but contain a common goal. In this way, a definition for *information technology systems* is developed by using reliable literature [Som04, Wik07].

Definition 3.2.3 *An information technology system is a purposeful collection of interrelated hardware and software components that work together to achieve a common objective and offer an interface implemented in software to human users.*

This definition can be used to develop criteria, which enables us to decide whether a system can be categorized as an information technology system. This part ends with criteria, which are distilled from the definitions and are used in the following sections.

1. The system is dividable into one or more sub systems or sub components.
2. The system's sub systems and/or sub components consist of hardware and/or software parts.

3. The system's different components have a common goal.
4. The system offers an interface implemented in software to support human users.

3.3 EDRM literature analysis

In this part of the *Definition analysis* it was necessary *to define Enterprise Digital Rights Management according to literature* in a complete possible way, such that all elementary parts were present. Available literature has been used to gather definitions and partial functions (Appendix A and B). According to literature, terminology of DRM and EDRM is sometimes confused. To define EDRM, it is necessary to perform an analysis about the subject and gather differences between them. First EDRM is analyzed and defined. The next step was to find differences with DRM systems, which can be used to support the developed *definition model*.

3.3.1 Enterprise Digital Rights Management

In this section all elementary parts are discussed from literature, which are translated into a suitable definition. Several articles recognize three crucial elements of DRM systems in general: Technical, Legal and Social [BBGR03, oAP07]. The relation of these perspectives with EDRM is defined as follows:

1. The technical perspective involves technical infrastructure divided into functional and non functional aspects.
2. The social perspective involves aspects like expectations, mores and education.
3. The legal perspective involves aspects like legislation, compliance and investigation in jurisdictional rights.

When observing resources from literature, DRM is often used as terminology for defining a complete set of systems using DRM technology (including EDRM systems). This implies that the first part of our EDRM definition should be extended with these aspects as well. Another observation from the same literature (Appendix A and B) shows EDRM systems to be *a client-server-based information technology system*. This observation is needed for the definition as well.

Systems are built to achieve a specific goal [Som04]. When using literature, DRM systems offer *users* the possibility to restrict access to digital content to precisely what the user needs or pays for. In this way, users are divided into at least

two roles. EDRM technology provides security mechanisms for managing and/or enforcing digital content and assigns rights. This allows people to have certain rights on documents. During this project *Rights* is used as technical terminology to distinguish authorization on digital documents. *Privilege* is defined as jurisdictional authorization. Furthermore, EDRM systems use *tracking and control* mechanisms to determine illegal usage of content by *users* and *attackers*. Attackers are considered to be potential attackers from inside the organization (employee) or outside the organization. In this way, inside attackers and outside attackers are distinguished. Outside attackers are defined as persons from competitive organizations or do not work anymore at the organization, and try to capture content illegally [RD03, YcC04b, ASF04].

In the past, several other cryptographic techniques were developed to protect digital content against unauthorized people [vT03]. The most important differences between EDRM systems and the usage of regular encryption methods are *persistent protection* and the *sophistication of rights* on digital content assigned to users [BBGR03]. So, these must be described as a part of our definition as well. First, there is need to define *persistent protection*.

Definition 3.3.1 Persistent protection *is defined as protection of digital content against unauthorized persons, which is not only maintained within the secure components of a system, but is maintained during its whole life cycle [SN04].*

According to literature, there are several *stakeholders* concerned with EDRM systems. All users have the ability to create digital content as an *author* and receive digital content as a *recipient*. Next to this, *administrators* are used to manage users and EDRM administrators are used to manage EDRM server related configurations. Because of all security risks and the described goal, the system must be *secure*. EDRM provides a solution with managed confidentiality, authentication, authorization and access to digital content [Oue06].

Security of digital content is considered to be an important goal within EDRM systems. Organizations use different kinds of digital content with a certain importance, but globally they can be divided into *intellectual property* and *trade secrets*. It is necessary to define *intellectual property* and *trade secrets*:

Definition 3.3.2 Intellectual property *is a creation of the intellect that has commercial value, including copyrighted property such as literary or artistic works, and ideational property, such as patents, appellations of origin, business methods, and industrial processes [Law06].*

Definition 3.3.3 *A* **trade secret** *is confidential practice, method, process, design, or other information used by a company to compete with other businesses. It is also referred to in some jurisdictions as confidential information [Wik07].*

Intellectual property can be seen as digital content registered as a patent, and used to protect the resources from an organization. Trade secrets are not registered as a patent, but kept secret as a protection mechanism. The most famous example is Coca Cola [OJR07].

By using the previous described aspects, it was possible to create a complete definition by using literature. *EDRM according to literature* is defined as follows:

Definition 3.3.4 *Technological, legal and social aspects*
translated into a client-server-based information technology system providing:

1. *distribution of digital content*
2. *tracking and control of digital content*
3. *and persistent protection of digital content*
4. *between stakeholders*
5. *by enforcing sophisticated rights*
6. *on digital content such as intellectual property or trade secrets*
7. *per user*
8. *controlled by rights holders*
9. *against attackers*
10. *in a secure way*
11. *for organizations.*

3.3.2 Digital Rights Management

The goal of this section is to define the differences between DRM and EDRM. The EDRM definition according to literature and the gathered definitions and functions (Appendix A and B) are used for describing these differences. The goal is to use the

differences when developing the *definition model*.

Because of confusion between terminology of DRM and EDRM, it is necessary to analyze differences. Sometimes EDRM systems are called DRM, but most of the time it can be seen as a set of applicable technology, based on the same techniques, but with another purpose within a certain context. EDRM systems can be seen as a sub set within DRM systems. In this way, DRM is considered to be a large set with EDRM systems, DRM audio systems, DRM movie systems or DRM e-book systems.

To support the definition model in a more complete way, different kinds of goals of DRM systems are gathered. Gartner [Rus01] distinguishes DRM as *combat security against piracy for:*

1. Textbook Publishers and University Bookstores
2. Providers of music, games, and other electronic entertainment

Gartner [Rus01] defines EDRM as *controlling access to information and ensure that the secure content reaches those parties who are accountable for its application or implementation for:* Law Firms, Health Providers, Financial Organizations, Corporate Operations Departments. Although these particular types of organizations could have many benefits by using EDRM systems, each (innovative) organization with crucial information could create (competitive) advantages.

Other resources mention DRM systems have a particular goal, such as providing secured audio or video to consumers against *payment* [App03]. All DRM systems have equal goals like providing security on digital content against unauthorized people on a sophisticated way.

Differences are distinguished between DRM and EDRM [YcC04b, EBR03, YcC04a, AH05b]. However, EDRM systems:

1. are used for controlling and managing rights on digital *intellectual property* within enterprises.
2. are not implemented with *financial management services* to administrate payments for consumers.
3. operate in a more *closed environment* compared to DRM systems, which offers enterprises not need to cater for the flexibility required by consumers.
4. are *less publicized and have lower media coverage* compared to DRM systems.

5. are implemented in another *context*, where business processes of enterprises must not be disrupted by implementation of EDRM systems.
6. need to be integrated in a *secure and transparent way* with existing enterprise IT environment and applications.
7. offer decrease of (potential) financial loss and information *theft in enterprises by inside attackers.*
8. aim at employees and perhaps external people of cooperating companies, while DRM aim to distribute documents to all kinds of customers against a certain fee and aims to spread digital content (on a legal way).
9. aim to secure sensitive enterprise content and not world-wide audio and/or video distribution.
10. provide users more possible rights compared to consumers as users within DRM systems, which implies that the *business models statically* emerge.

3.4 EDRM according to Aia Software

The goal of this section is to create a definition for Aia Software. The previous section developed an EDRM definition by using literature and created a set of differences with DRM. By using these two inputs, a model is built as described in appendix C. The different aspects from these results are translated into questions, which define the *definition model*. These questions were used on the director of Aia Software to create an Aia Software business case specific definition.

Definition Aia Software for **Enterprise Digital Rights Management**:

Definition 3.4.1 *Technological, legal and social aspects*
translated into a server-client-based information technology system providing:

1. *distribution of digital content,*
2. *tracking and control of digital content*
3. *and persistent protection*
4. *between stakeholders*
5. *by enforcing sophisticated rights (read, alter, print, copy-paste)*

6. *on all produced digital content*
7. *for the customer organization*
8. *per user*
9. *controlled by rights holders*
10. *against outside attackers*

By using the questions from Appendix C, a business case specific definition completes the definition analysis. The definition is used as an input for the requirements analysis, where defining EDRM systems will take place into more detail. In future this definition analysis can be used to define EDRM for other business cases as well. As described, literature is used as an important resource to be able to create a model and related definition. This method provided a definition as a result by using experiences of others with more knowledge about the subject. Because the topic is new and innovations are taken place each day, it is hard to keep up with changes on the subject made by others. After gathering available literature, this definition can be seen as complete and concrete compared to other definitions. The definition model can be used to reveal answers from stakeholders and creating an own business case specific definition.

3.5 Conclusions

During this definition analysis many definitions and functions from literature are analyzed and compared. By creating a definition for information technology systems first and developing a definition for EDRM by using literature, it was possible to conclude EDRM systems to be a special type within the set of information technology. In this way, it was possible to build an EDRM definition according to literature. The goal was to develop a definition for EDRM according to Aia Software. An additional goal was to analyze differences with DRM. DRM can be seen as a main set and the systems within this set can be divided into several types with an own specific purpose:

1. protecting audio against piracy
2. protecting video against piracy
3. protecting e-books against piracy
4. protecting classified information within organizations against illegal distribution to maintain competiveness

The EDRM definition according to literature and the differences with DRM are translated into several questions, which can be seen as a *definition model* (Appendix C). This model was discussed with the director of Aia Software to create a business case specific definition. Because only one person is used to create a definition, it is possible that the definition is incomplete. The analyzed literature showed many limited definitions. In this way, the developed definition for EDRM in this phase is considered to be most complete. Because the model was built by using literature, it is possible that a more complete definition can be developed by using other resources. Next to this, the topic is rather new and not many books and articles are written on the subject. The developed definition is considered as a result from the definition analysis. It is possible to use software engineering practices on EDRM, because EDRM is considered to be an information technology system. Next to this, it is possible to use this phase for selecting appropriate literature about the subject. After performing the definition analysis, it is possible to develop EDRM requirements in the next Chapter, which are used to develop a selection criteria model.

Chapter 4

Requirements analysis

To be able to choose an appropriate EDRM system, it is necessary to compare all current EDRM systems. As described in the global research method in Chapter 2, a *selection criteria model* (phase 3) is built to support comparison of EDRM systems in Chapter 5. The previous chapter provides an EDRM definition according to Aia Software (phase 1) and is used as an input to reveal technical EDRM specific requirements (phase 2) [Som04]. These requirements are described in this chapter and are used to create the *selection criteria model* described in the next chapter. According to literature, a requirements analysis can be performed by using techniques on stakeholders, but because these (customer) stakeholders are not available, another method is used to reveal requirements. This method can be used in the future when stakeholders are available. In the following section, a detailed research method is described and used to perform a requirements analysis. These requirements are based on literature and are not influenced by the business case in this Chapter.

4.1 Research method

To be able to create these requirements, the following tasks are completed:

1. Creating a method to reveal requirements (requirements process);
2. Creating a categorization to divide requirements (categorization process);
3. Creating a complete set of technical EDRM specific requirements by using the described method and categorization, needed for the future selection criteria model (by using EDRM requirements);

The following sub sections describe the used requirements process and categorization, which were used to complete this phase.

4.1.1 Requirements process

According to [Som04], a requirements analysis is defined as a *requirements process* and this process should be used in an iterative way on stakeholders of the potential system. This project is more concerned with current available requirements from literature, because there was not enough time to use a complete iterative process and actual stakeholders were not available as well. In this way, it was necessary to choose an alternative requirements process.

The following project characteristics are observed:

1. In this project only technical EDRM specific requirements are necessary;
2. Only a few people within the organization were available to distill requirements and ideas about EDRM, and these people are not the real stakeholders (users of the system);
3. Aia Software is not the end customer, and wants to use the advice for further innovation and usage for other potential customers;
4. Literature is one of the most important resources, because the topic is new for Aia Software.

The goal of the requirements analysis is to develop a complete set of technical EDRM specific requirements. According to [Som04] there is no perfect and universal applicable approach for the requirements analysis. There are several approaches, which can be chosen. All approaches are based on analyzing the stakeholders in practice. The first step should consist of *requirements elicitation and analysis* where several approaches can be chosen [Som04]. This iterative process could be covered by using the following techniques: *viewpoint-oriented elicitation, scenarios and ethnography.*

Viewpoint-oriented elicitation refers to the analysis of requirements from the different viewpoints of different kinds of people involved. This technique can be very useful when there are users to interview. In this way, it is possible to gather different kinds and overlapping requirements, which could all be translated into a complete set of requirements.

Another technique is called *scenarios.* Several stakeholders of the system are analyzed and scenarios are abstracted from real-life examples [Som04].

The third technique is known as ethnography. *Ethnography* is an observational technique that can be used to understand social and organizational requirements. In this way we should immerse ourselves into the working environment where the system is used.

As mentioned before, the phase of developing requirements is an iterative process, which consists of gathering requirements by interviewing all involved stakeholders and expanding the requirements in this way. The described *Interviewing* techniques will probably *not directly result* into a complete set of requirements, because there are only a few persons to interview and the real stakeholders who will use the system are not available. Because Aia Software will use the system to sell to new customers, there is need for more technical knowledge about EDRM specific requirements. This research project was done to reveal more information about EDRM for Aia Software and potential future organizations, so there is need for information from other organizations with experiences and knowledge about the subject. Because it is not possible to contact these organizations within a few months and use their requirements, another approach is used to develop the needed requirements.

In EDRM literature there is enough reliable information about potential EDRM specific requirements. Sommerville defines requirements as *a complete set of categorized technical user demands* [Som04]. In future, these requirements can be used as a guideline to gather more requirements from other stakeholders or to create the requirements into further detail.

The chosen research method is based on exploiting knowledge from others by using available and reliable EDRM literature. By using the definition and analyzing literature, it is possible to describe a complete set of technical EDRM specific requirements based on current available literature. Because the developed requirements came directly from literature and business case specific inputs are not added in this phase, the requirements are formulated in a universal way. These requirements are used in a following phase to develop a model. Eventually the developed model is combined with a business case to create business case specific requirements for EDRM systems.

4.1.2 Requirement categorization

The EDRM requirements are important during this research project. It is necessary to gather all possible technical requirements from literature and eventually use inputs from Aia Software. By using literature as a first step, experiences and knowledge from other organizations can be used. By using the literature, an appropriate categorization is developed, which can be used to divide the gathered requirements from literature. This categorization is used in the following phases as well.

Sommerville divides requirements into *functional* and *non-functional* requirements [Som04]. These are defined as follows:

Definition 4.1.1 *Functional requirements are statements of services the system should provide, how the system should react to particular inputs and how the system should behave in particular situations.*

In some situations the functional requirements may also explicitly state what the system should not do.

Definition 4.1.2 *Non-functional requirements are constraints on the services or functions offered by the system.*

These non-functional requirements include timing constraints, constraints on the developments process, standards, etc. In the same way these non-functional requirements include properties or characteristics of the system that its stakeholders demand from it (e.g. constraints and qualities).

The differences between functional and non-functional are sometimes in practice rather difficult to observe. Next to this, the requirements are divided according to another categorization. When observing the own developed EDRM definition (Definition Analysis), several categories can be distilled:

1. Rights management
2. Content management
3. Tracking and control management
4. Stakeholder management
5. Security management

Rights management, content management, tracking and control management and stakeholder management contain functional requirements. The functional EDRM requirements are divided into these categories. Security management concerns non-functional requirements and will therefore be categorized in this way. Another category called *other non-functional requirements* is used to categorize the remaining non-functional requirements, which were not easy dividable. The requirements were gathered from literature and are therefore described on a universal way. In this way, these requirements are not yet concrete, but can be used with stakeholders to reveal concrete requirements. The requirements can be used as a guideline to develop more concrete requirements by using them on actual stakeholders. The following sections describe the gathered functional and non-functional requirements from literature.

4.2 Functional requirements

The functional requirements are described in the following sub sections and are categorized into *Rights management, Content management, Tracking and control management and Stakeholder management.*

4.2.1 Content management

Content management is concerned with digital content related requirements.

Content creation

Each user must have the ability to create different kinds of digital content and secure the created content with rights for other users [AH04, AH05b].

Content metadata

When a digital document is secured, it is useful to add metadata with content (e.g. author, title, description). In this way, information about the secured document can always be read [AH04, AH05b].

Uniquely identifiable content

Secured digital content should be uniquely identifiable. Each document must be prepared with a unique identifier, which enables it to be linked with users [AH04, AH05b].

Distribution model

The EDRM system should be able to support different distribution models (e.g push, pull, super-distribution).

Searchability

Secured digital documents should be searchable by other users. This allows users to search through a content management system with gathered documents [RD03].

Partial asset protection

The system has the ability to apply different usage rights to parts of a digital document [oAP07].

User access to information about rights

There is need to give the EDRM system the ability for the user to obtain extra information (e.g. copyright information, available permissions, available rights) [YcC04b].

Personal backup

The EDRM system should allow the creation of personal backup copies of digital documents per user [BBGR03].

4.2.2 Tracking and control management

These requirements concern the functional requirements for tracking and controlling management. Tracking and control management requirements are defined as requirements concerning detection of misusage.

Logging content usage

Usage of secured digital content and rights can be monitored. Digital content, which is stored on a content deposit, can be distributed in a controlled way. In this way server logs can be gathered with several kinds of information about the usage of documents. The advantage of tracking usage is that when a document is excessively used, the system could register who is responsible for illegal distribution.

Watermarking

Watermarking of digital content can be used to mark digital content with for example its distributors id [Lew98]. This technology is embedded with the document and can be used to prove ownership of certain digital content. When an attacker occupies a certain document and the organization detects the misuse, the identity of the excessive internal person might be discovered with the use of tracking methods like watermarking.

4.2.3 User management

In this section, technical EDRM requirements concerning *user management* are gathered. User management requirements are concerned with requirements about users.

User registration

The system is implemented to protect digital content against unauthorized users. The system provides users to work with different kinds of digital content, wherefore the rights are available. At any time, certain users can be assigned to certain projects or leave particular projects. It is necessary to create a new user or delete existing users from projects/organization with assigned digital content [Sta04].

Scalability

The ability and flexibility of a system to meet growth of an organization is important. The system should be scalable in a way, such that problems are prevented. An organization might grow with different users, which could affect the performance of authentication protocols and the effectiveness. Next to this, the content management system could grow as well and in this way scalability can be very important. There is need to verify if an EDRM system could meet the grow capacity of an organization. Each user produces digital content and EDRM systems should be scalable with the produced documents and related users [AH05b, HW03, JM03].

Uniquely identifiable users

Unique identification of users is important within EDRM systems. Users must be authenticated in a unique way. Attackers and eavesdroppers must not be able to reveal and simulate the authentication protocol illegally [AH04, AH05b, Sta04, RD03, HW03, JM03].

4.2.4 Rights management

This section is concerned with rights management requirements. These requirements are defined as all requirements concerning rights.

Rights per document per user

Users have the ability to provide rights per digital content per user. Sophistication of rights can be different between EDRM systems. Which kinds of rights are necessary for stakeholders should be determined. The following rights can be used as an example: full control, modify, read, print, copy-paste, email [AH04, AH05b, RD03, HW03, JM03].

Limited document usage

The EDRM system should be able to restrict the usage of the content by various conditions (e.g., number of times accessing content, expiration date, embargo date, etc.) [ASF04, Guo01, JM03].

Rights transfer

There is need to give certain users within the EDRM system the role to transfer rights between users, without risking illegal usage [AH04, AH05b, RD03, HW03, Sta04, JM03].

Dynamical rights

Assigned rights should be changeable. Authors, users with full control or administrators have the ability to change rights afterwards. After an author has assigned certain rights, it should be possible to change the rights of digital documents [AH04, AH05b, RD03, HW03, Sta04, JM03].

Rights templates

Templates with usable rights prescribed by an organization can be used to limit authors by choosing certain rights and increasing security in this way. Authors have the possibility to choose from a selection of prescribed rights per template [BBGR03, JM03].

Content versioning

The EDRM system should be able to provide users with the ability to create different versions of a given content [BBGR03, JM03].

Rights and protected content recovery

The user has the ability to delete an instance of protected content, while keeping the rights associated with that content, such that a user could later restore the protected content on the device, without having to obtain new rights [BBGR03, JM03, AH05b, RD03].

4.3 Non-functional requirements

The first important category for Non-functional requirements is defined as *Security management*. The remaining non-functional requirements are gather into the section *other non-functional requirements*.

4.3.1 Security management requirements

In this section the non-functional requirements related to security management are described.

Key individualization

When accessing digital content, there is need to provide the necessary mechanisms to associate, a unique individual key to each of the content items [ASF04, Guo01, JM03].

Decryption keys non-disclosure

The EDRM system should be able to distribute decryption keys only to authenticated and authorized users and devices [ASF04, Guo01, JM03].

Renewability

The EDRM system should be able to renew the essential security elements of the EDRM system in case of invulnerabilities [ASF04, Guo01, JM03].

Standard key management

The EDRM system should be able to use standard key management systems (for example PKI), to the extent that this is required for interoperability [ASF04, Guo01, JM03].

Tamper-resistance

Tamper-resistant mechanisms can be used to protect content and enforce content usage rules. In most EDRM systems the client software can be seen as the part with the most risk for security failures. Most EDRM systems are based on encrypting content, which enforces the client software to encrypt data by using keys. When using this approach, digital content could be accessed by performing reverse engineering [ASF04, Guo01, JM03].

No single point of failure

This is where one part of a system will make the whole system fail in case this part fails [ASF04, Guo01, JM03].

4.3.2 Other non-functional requirements

In literature several other requirements were mentioned related to EDRM and are described as well.

Simple installation

Installation of the new system should not imply complete reorganization. It should be relative easy to advance the current IT infrastructure [ASF04, Guo01, JM03].

Maintainable

The system should be maintainable by for example administrators, such that it is possible to prevent or to interfere in case of failures [ASF04, Guo01, JM03].

Portability - Platform shifting

This option gives the user the flexibility to change the platform where he or she is working on. The consideration involves whether EDRM systems should be able to communicate with different types of platforms [ASF04, Guo01, JM03].

Portability - Format shifting

By using this technique it is possible to change the format of an existing secured digital document. Available file extensions for protection should be determined and the ability, whether it should be possible to shift the format as well [ASF04, Guo01, JM03, AH05b].

Portability - Space shifting

This term refers to the fact that people can use different types of devices to access digital content according to the prescribed rights [AH05b, ASF04, Guo01, JM03].

Portability - Time shifting

This feature facilitates that users can access the digital content whenever the user wants to. An important issue is the decision whether the user needs to be online or has the ability to be offline while accessing digital content. Not all locations are equipped with an internet connection. Offline access reduces monitoring and tracking opportunities and next to this, it limits the control of data by enterprises, which are both disadvantages [ASF04, Guo01, JM03].

Integration with existing applications

Most software organizations developed own software or use other existing software. Methods for integration with existing applications should be supported [ASF04, Guo01, JM03].

4.4 Conclusions

During this phase an alternative way of gathering technical EDRM specific requirements is used. Because it was not possible to use interviewing techniques with real

customers, literature is used as a fundamental approach to gather important universal technical categorized requirements. The requirements are divided into functional and non-functional requirements as described. By using the developed definition from the definition analysis, it was possible to create more detailed categories (user management, stakeholder management, rights management, content management and security management). Because the topic is rather new, there is not much literature on the subject. This could lead to limitations on the gathered requirements. It is recommended to update requirements with new additional literature and other experiences with EDRM producing companies. Next to this, EDRM systems are not used very often in practice and experiences could be quite scarce for that reason. This could all result into less complete requirements and could eventually influence the developed advice. Organizations (like Aia Software) are able to use them on own business cases and create more concrete requirements by applying the selection criteria model (Chapter 5). The gathered requirements are used in the following Chapter, where they are translated into a selection criteria model.

Chapter 5

Selection criteria model

The first objective was to create a *selection criteria model*, which can be used for organizations to create business case specific selection criteria. The previous phases resulted into an EDRM definition and a set of categorized technical functional and non-functional EDRM requirements. These requirements were based on resources from literature. During this phase these requirements are used to create the *selection criteria model*. The goal is to develop a model, which can be used on business cases to develop business case specific requirements. A *selection criteria model* is defined as a set of universal functional and non-functional categorized requirements with a *measurement* and *degree of importance* option. The measurement part is necessary to reveal how a requirement can be measured when analyzing *EDRM systems properties* and is used in Chapter 7. The degree of importance is used next to the business case specific questions to reveal how important the requirements are for stakeholders. This phase is concerned with developing that model (phase 3) and not revealing the criteria from the business case by applying it (phase 6). By developing the model and applying it in phase 6 on the organization, it is possible to compare EDRM system properties to verify if EDRM systems fulfill the requirements of an organization. The following section provides a research method, which motivates how the gathered technical requirements from Chapter 4 can be translated into the *selection criteria model*.

5.1 Research method

To be able to develop the requested model, the following tasks need to be completed:

1. Completeness of all technical EDRM specific functional and non-functional requirements.

2. Business case applicability.

3. Measurement with EDRM system properties.

4. Degree of importance per criterion.

These tasks allow the selection criteria to be complete to apply on business cases and to compare with EDRM system properties (Chapter 7). The measurement ensures the model to be comparable with EDRM systems and their properties. The degree of importance provides business cases to distinguish important criteria from optional criteria. The gathered requirements are expanded in a way, such that it would be usable by adding the needed properties. After adding these tasks to the requirements and performing on a business case, they are defined as *selection criteria*. The developed model is dynamically applicable on business cases and can be used in future by other organizations in the same way as was done for Aia Software (in Chapter 8). In this way, this Chapter is used to develop the model and Chapter 8 is used to use it on Aia Software as a business case. The following sub sections describe the additional parameters of the model in further detail.

5.1.1 Completeness of criteria

The usage of our developed model should result into completeness of technical functional and non-functional selection criteria. During this research project, literature is used to develop a complete set of technical functional and non-functional universal requirements (phase 2). These requirements are now used as a first ingredient for developing selection criteria model. The literature research from the previous chapter provided completeness by gathering functional and non-functional requirements. Because these requirements are not concrete yet, they represent guidelines and real requirements can be created by using inputs from stakeholders.

5.1.2 Business case applicability

To be able to reveal concrete criteria, it is necessary to reveal certain information related to the constructed requirements described in the previous sub section. Business case questions were developed by using these descriptions. By answering these questions by stakeholders, detailed criteria can be revealed. These questions are defined as a first add-on to the developed requirements.

5.1.3 Measurement with EDRM systems

Per requirements it is necessary to develop a measurement mechanism, which can be used to create EDRM system properties in Chapter 7. These measurements are created by analyzing the described requirements. This measurement defines how requirements can be measured per EDRM system. This is the second add-on for the selection criteria model per requirement.

5.1.4 Degree of importance

According to [Som04], it is useful to assign all criteria with a certain importance. Because some criteria are more important compared to other criteria in other business cases, a *degree of importance* is used to determine the importance per criterion. The degree of importance needs to be filled in by stakeholders as well.

value	**semantics**
-1	Explicitly not mandatory
0	Not important
1	Nice to have
2	Mandatory

Table 5.1: Degree of importance

When combining all criteria, it is possible to assign them to a certain degree. In this way, it is possible to assign all criteria to a value from -1 to 2. Stakeholders can be used to decide, which criteria are important when comparing EDRM systems. When comparing EDRM systems, it is necessary to choose an EDRM system which fulfills the selection criteria with a high degree of importance according to stakeholders. Because real customer stakeholders were not available during this project, the project supervisor from Aia Software is used to answer the questions as described in Chapter 8. The following sections provide results with translated requirements into the actual selection criteria model without influences from business cases. The following sub sections describe the categorized functional and non-functional selection criteria defined as the *selection criteria model* with the defined add-ons.

5.2 Functional selection criteria

This section describes the functional selection criteria. The functional selection criteria are divided into the same distilled subjects from the definition (content

management, rights management, stakeholder management, tracking and control management).

5.2.1 Content management

These selection criteria are related to content management aspects about EDRM systems.

Content creation

Each user must have the ability to create different kinds of digital content. In this section it is necessary to verify from stakeholders how digital content can be created and which demands are requested [AH04, AH05b].

Related question(s):
How can content be created?
Which other demands are concerned with securing new digital content?

Measurement: Content can be created by using certain applications. EDRM systems can be observed how content can be created. Secure or insecure content creation should be distinguished. Illegal extraction of content could be tested per EDRM system as well.

Content metadata

Metadata next to the secured digital content can be provided. In this way, information about the secured content can be given [AH04, AH05b].

Related question(s):
Which metadata is necessary when securing digital content?

Measurement: In most EDRM systems metadata contains a title, description, date and name of author. EDRM systems can be analyzed in what way metadata is used or not.

Uniquely identifiable content

Unique identification of digital content is very important. Each document must be prepared with a unique identifier, which enables it to be linked with users and rights.

[AH04, AH05b].

Related question(s):
Is there need for uniquely identifiable content?

Measurement: Uniquely identifiable content is examined by researching the methods, which are used for content identification with EDRM systems.

Distribution model

EDRM systems are able to support different distribution models for distributing digital content among others (e.g; push, pull, super-distribution).

Related question(s):
How can digital content be distributed by authors?

Measurement: push, pull or super-distribution should be compared with the methods which are provided by EDRM systems.

Searchability

There is need for searchability of content. This allows users to search through a deposit with digital content and possible linked metadata [RD03].

Related question(s):
How can users search for/through secured digital documents?

Measurement: EDRM systems and its content management part must be analyzed. By using literature and testing the systems, it is possible to verify searchability features and how users can search for/through digital documents with EDRM systems.

Partial asset protection

EDRM systems should be able to apply different usage rules/rights to parts of a larger content item [oAP07].

Related question(s):
Is there need for partial asset protection?

Measurement: Partial asset protection can be verified by using literature and tested

with the available EDRM systems. In this way, it should be clear whether it is possible to secure parts within a document or just the whole document.

User access to information about rights

EDRM systems should be able to obtain information, e.g. copyright information, available permissions, regarding rights of the user or rendering device [YcC04b].

Related question(s):
Is it possible to reveal certain information about rights from secured digital documents?

Measurement: EDRM systems should be verified to provide certain information from secured digital documents.

Personal backup

EDRM systems should provide personal backup features of digital documents [BBGR03].

Related question(s):
Is there need to facilitate personal backup for secured digital documents?

Measurement: EDRM systems can be verified to have personal backup features.

5.2.2 Tracking and control management

Tracking and control management is concerned with misusage by users and in what way this can be done.

Logging content usage

Usage of secured digital documents and rights can be monitored. Digital documents, which are stored on a content deposit, can be distributed in a controlled way. In this way server logs can be gathered with several kinds of information about the usage of documents. The advantage of tracking usage is that when a document is excessively used, the system could register who is responsible for certain actions.

Related question(s):
Which logging facilities are needed to record usage of digital content?

Measurement: Logging of content, users and rights need to be clarified with EDRM systems.

Watermarking

A method, which allows tracking, is watermarking of digital content [Lew98]. This technology is embedded with the document and can be used to prove/maintain ownership of certain digital content. When an outside attacker occupies a certain document and the organization detects the misuse, the identity of the excessive internal person might be discovered with the use of tracking methods like watermarking. Tracking methods might be very useful, but in what way we want to use certain techniques must be decided. It is also necessary to validate in what way user privacy is concerned, but these are more *legal aspects* and are not discussed during this research project.

Related question(s):
Is there need to provide watermarking techniques? Is there need to protect print screens?

Measurement: Watermarking techniques can be verified per EDRM system. Systems can be verified to secure against print screens. Usage of watermarking can be verified by comparing EDRM systems.

5.2.3 User management

User management is the part of EDRM systems, which is concerned with users, roles and privileges with other related EDRM parts.

User registration

The system is implemented to protect digital content against attackers. The system facilitates users to work with different kinds of digital documents, where rights are available. Every day certain users can be assigned to certain projects or leave particular projects. It is necessary to create a new user or delete existing users from projects and/or assigned digital documents [Sta04].

Related question(s):
How can users be managed?

Which other demands are necessary for managing users?

Measurement: Management of users should be possible by users with administrator roles. These tasks should be done by certain people and not by all users of the system. Business models should be developed in a way such that misusage is limited. Possible scenarios can be verified with the current EDRM systems. It is necessary to maintain security when providing certain roles to certain users.

Uniquely identifiable users

Users need to be uniquely identified. It should not be possible for users to use each other's identities [AH04, AH05b, RD03, Sta04, HW03, JM03].

Related question(s):
Is unique identification necessary?

Measurement: Authentication mechanisms can be verified to measure how EDRM systems provide uniquely identifiable users.

Scalability

The ability and flexibility of an application to meet growth of users at an organization is an important requirement for EDRM systems. An organization might grow with different users, which could affect the performance and effectiveness of the EDRM system. Next to this, the content management system could grow as well and in this way scalability can be very important [AH05b, HW03, JM03].

Related question(s):
Could scalability be a problem in future?

Measurement: EDRM systems can be verified to be scalable. Scalability is influenced by processes of the server. Because the server could lose performance when the number of users increases, it is necessary to measure whether this could be a risk. Server clustering could be used for example to improve performance. In this way, EDRM systems could be verified to use these kinds of techniques.

5.2.4 Rights management

Rights per document and user

Users have the ability to provide rights per digital content per user [AH04, AH05b, RD03, HW03, JM03].

Related question(s):
Which rights should be assignable to digital documents?

Measurement: The EDRM systems can be evaluated which rights could be used in the EDRM system.

Limited document usage

There is a need to give the EDRM system the ability to restrict the usage of the content by various parameters (e.g., number of times accessing content, expiration date, etc.) [ASF04, Guo01, JM03].

Related question(s):
Is limited document usage necessary?

Measurement: Conditions related to rights such as expiration date, embargo date and number of accessing content can be verified in EDRM systems.

Rights transfer

Certain users or administrators within the EDRM system have the ability to transfer rights between users. Because users could have the ability to transfer all rights to their selves, the digital content could not be secure anymore. In this way, organizations should consider in what way they want to apply rights transfers [AH04, AH05b, RD03, HW03, Sta04, JM03].

Related question(s):
Which demands are requested for transfers of rights?

Measurement: EDRM systems can be verified, which users and related roles can be used to transfer rights.

Dynamical rights

Assigned rights should be changeable. After an author has prescribed rights, it should be possible to change the rights of digital documents afterwards[AH04, AH05b, RD03, HW03, Sta04, JM03].

Related question(s):
Is it necessary to change rights easily after distribution of digital documents?

Measurement: Rights can be verified to be changeable dynamically. Central storage of rights provides the ability to change rights dynamically. This can be verified by comparing it with the working of current EDRM systems.

Rights templates

It might be necessary to create templates with usable rights prescribed by an organization. In this way, authors have the possibility to choose from a limited selection of prescribed rights provided by this organization. [BBGR03, JM03].

Related question(s):
Is it necessary to use rights templates?

Measurement: EDRM systems can easily be verified whether rights templates can be used.

Content versioning

There is a need to give the EDRM system the ability to propose various business models and usage rules for different versions of given content [BBGR03, JM03].

Related question(s):
Is there need for version control?

Measurement: Within the content management part it could be possible to use version control features. These features should be verified per EDRM system.

Rights and protected content recovery

An EDRM system should be able to allow users to delete an instance of protected content, while keeping the rights associated with that content. In this way, the user

could later restore the protected content on the device, without having to obtain new rights.

Related question(s):
Is there need for protected content recovery?

Measurement: Protected content recovery can be verified to be available by using literature and testing the system.

5.3 Non-functional selection criteria

Non-functional selection criteria are divided into two categories called Security management and other non-functional selection criteria.

5.3.1 Security management

The following selection criteria are used for security management.

Key individualization

There is need to give the system the ability to provide the necessary mechanisms to associate, whenever needed, a unique individual key to each of the digital documents to prevent intruders [ASF04, Guo01, JM03].

Related question(s):
Is individualization of keys necessary?

Measurement: Key individualization can be verified by comparing the mechanisms of EDRM systems.

Decryption keys non-disclosure

The EDRM system should be able to distribute decryption key(s) only to applications with authenticated users and devices [ASF04, Guo01, JM03].

Related question(s):
Is illegal closure of decryption keys necessary?

Measurement: The EDRM system should be verified for using non-disclosure of decryption keys.

Renewability

There is a need to give the EDRM system the ability for the essential security elements of the EDRM system to be renewable in case of invulnerabilities [ASF04, Guo01, JM03].

Related question(s):
Is renewability a requested feature?

Measurement: Renewability can be verified by informing producing EDRM companies.

Standard key management

There is a need to give the EDRM system the ability to use standard key management systems (for example PKI), which might be necessary for interoperability [ASF04, Guo01, JM03].

Related question(s):
Is standard key encryption necessary?

Measurement: Standard key management such as PKI can be verified per EDRM system.

Tamper-resistance

Tamper-resistant mechanisms can be used to protect content and enforce content usage rules. In most EDRM systems, the client software can be seen as the part with the most risk for security failures. Most EDRM systems are based on encrypting content, which enforces the client software to encrypt data by using keys. When using this approach, digital content can be accessed on an unauthorized way by performing reverse engineering skills. [ASF04, Guo01, JM03].

Related question(s):
Is tamper-resistance needed?

Measurement: Tamper-resistance can be measured by comparing techniques about these EDRM systems.

No single point of failure

Another security issue, which should be avoided, is the single point of failure. EDRM systems can be very vulnerable to Denial of Service attacks (DoS) when having single points of failure [ASF04, Guo01, JM03].

Related question(s):
Should single points of failure be prevented?

Measurement: The infrastructure of EDRM systems should be analyzed for single points of failure.

5.3.2 Other non-functional selection criteria

In literature several other non-functional requirements related to EDRM were gathered and are described as well.

Simple installation

Another requirement for the system is that the installation of the new system should be relative easy [ASF04, Guo01, JM03].

Related question(s):
Is simple installation needed?

Measurement: By comparing the current infrastructure and EDRM systems, it is possible to verify an EDRM system to be simply implementable in current infrastructure.

Portability - Platform shifting

This feature gives the user the flexibility to change from platform that he or she is working on. The consideration involves whether EDRM systems should be able to communicate with different types of platforms [ASF04, Guo01, JM03].

Related question(s):

Is platform shifting needed?

Measurement: First there is need to verify which platforms should be supported by stakeholders. The EDRM systems can be compared for their platform support.

Portability - Format shifting

This feature enables the user to change the formats of digital content [AH05b]. Next to this multiple file extensions should be possible as well when shifting from format [ASF04, Guo01, JM03].

Related question(s):
Is format shifting needed?

Measurement: Format shifting can be verified by knowing first which formats are available and tested if it is possible from shift format when a document is secured.

Portability - Space shifting

Space shifting refers to the fact that people can use different types of devices to access digital content according to the prescribed rights [ASF04, Guo01, JM03, AH05b].

Related question(s):
Is space shifting needed and which devices are needed?

Measurement: Other devices can be verified to work with EDRM systems. After gathering these devices it is possible to compare requirements between EDRM systems.

Portability - Time shifting

This feature facilitates users to access the digital content whenever the user wants to. An important issue is the decision whether the user needs to be online or has the possibility to access offline. Not all locations are equipped with an internet connection. Offline usage has many disadvantages. Offline access reduces monitoring and tracking opportunities and next to this, it limits the control of data for enterprises [ASF04, Guo01, JM03].

Related question(s):
Which ways of time shifting are needed?

Measurement: Time shifting possibilities can be seen as online or offline and inside the company or outside the company. These features can easily be verified.

Integration with existing applications

Most organizations have own developed software or use other existing software, which need to interact with EDRM systems [ASF04, Guo01, JM03].

Related question(s):
Is there need for integration with currently existing software? Which requirements are necessary to communicate with this software?

Measurement: EDRM systems can be verified to be communicative with other possible applications or environments.

5.4 Conclusions

This Chapter resulted into developing a *selection criteria model* by using previously developed EDRM technical requirements. The previous sub sections describe an overview of this model with related questions and measurements. The related questions should be answered by stakeholders to develop concrete EDRM system requirements. The measurements are used in Chapter 8 when developing EDRM system properties. In this way, the EDRM system properties which resulted from the measurement can be compared with the results from the Selection criteria model of Aia Software (Chapter 8). Next to this, it was necessary to create a *degree of importance* to measure the importance of the selection criteria by business cases. Stakeholders should in this way assign a certain degree of importance as well after answering the provided questions. This option allows stakeholders to distinguish important criteria from optional criteria. An overview of tables is given in appendix D with all previously mentioned selection criteria as a template to fill in the *degree of importance* by organizations. Because the model is developed by using the requirements from the previous chapter, there is a risk these criteria could not be up-to-date. Because of the new topic, it is possible for EDRM producing organizations to develop new features. Next to this, each criterion is added by business case questions. It could be possible; organizations have additional wishes per requirement subject. Next to this, it is possible stakeholders have other wishes resulting from the questions which were not measured in Chapter 7. In this way, it would be necessary to do more research on the subject and update the missing properties.

This model could be updated adding new resources from literature or experiences from organizations. Organizations are expected to use EDRM system more often in future, which could provide inputs for further research on subject. An organization could be able to develop its own complete selection criteria model by using this standard.

In a following phase it is necessary to reveal the results from Aia Software by using this selection criteria model, but first current existing EDRM systems are analyzed in the following phase. After analyzing the current EDRM systems, EDRM system properties are developed per EDRM system based on the measurement rules from this phase.

Chapter 6

EDRM system analysis

In chapter 5 an EDRM selection criteria model is developed. The next step is to perform an analysis about which EDRM systems are currently available on the market (Chapter 6). Next to this, it is necessary to gather for each EDRM system properties (Chapter 7) according to the earlier developed measurements from the selection criteria model (Chapter 5), which can be used to compare the systems. This chapter results into a set of currently available EDRM systems. The following section describes the research method to support the results in this phase.

6.1 Research method

The objective is to create a complete set of current EDRM systems. To be able to gather this set of EDRM systems, it was necessary to develop criteria to distinguish EDRM from other systems.

Which systems are potential EDRM systems?

To be able to answer this question, it was necessary to use reliable and as many important resources as possible. During the first phases (definition and requirements analysis) resources were used to complete these phases. The same resources are used during this phase to gather EDRM systems. Next to this, search engines are used to gather these EDRM systems as well. Gartner is an organization specialized in research about information technology [Oue06]. Resources from Gartner are used to create this list as well. Next to this, DRM Watch [DRM07] can be seen as a web community with a lot of information about current EDRM systems. To ensure completeness of EDRM systems, this resource has been used as well for gathering information about the subject. All resources were used to create this list with EDRM

systems. To be able to define a system to be EDRM, the developed definition from the *definition analysis* is used. Next to this, EDRM systems which are able to secure Microsoft Office related documents are needed during this project. This additional criterion is used as well. Because the developed definition is complete, systems can be judged to be EDRM.

From the *definition analysis*, the following properties can be distilled as criteria for selecting EDRM systems:

1. Information technology system
2. Client-server based
3. Provides distribution of digital content
4. Provides tracking and control of digital content
5. Provides persistent protection of digital content
6. Provides users to set privileges on digital content for other users
7. The goal of the system characterizes itself to protect digital intellectual properties and trade secrets for organizations against outside attackers.

In the following sections, the EDRM systems are described in such a way that they could be compared with the described definition criteria.

6.2 Microsoft RMS

RMS is a component based EDRM system provided by Microsoft. Although this is not a complete product, Microsoft provides several products or services to be used as one whole EDRM system. The system uses its own operating system Windows 2003 server, which can be expanded with an RMS component on the server and several client add-ons on windows client machines.

Figure 6.1 gives an overview of the RMS client-server based infrastructure. The system provides users to create content (author) and secures it by authorizing at the server. After setting permissions for users, by defining rights and users, the author sends an issuance license to the Server. The server signs the issuance license and sends the signed license back. Now the author sends the signed license with the encrypted document to the receivers. The next step for the receiver is to authenticate with the RMS server. After authentication, the receiver sends the signed license and

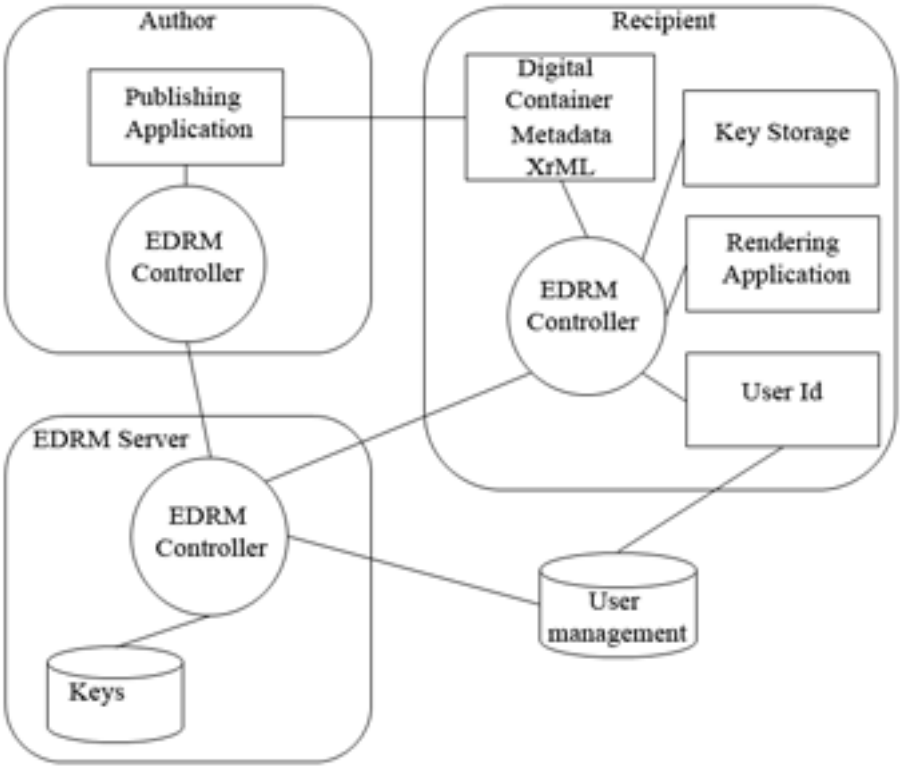

Figure 6.1: EDRM system: Microsoft RMS

receives the decryption key next to an end user license. This decryption key and end user license enables the EDRM controller to encrypt the content with assigned rights. The SSL protocol ensures attackers are not able to capture keys and RSA is used for encrypting sent messages. The documents are furthermore encrypted by AES symmetric encryption.

The first property demands the system to be *client-server based*. According to the picture, this certainly is true. The RMS server is based on Windows Server 2003 with an RMS add-on and functions as a server to provide users the appropriate functionality for securing digital content. In this way, *distribution of digital content* is done by the users themselves by sending the secured digital content with digital communication protocols. Another expansion with Microsoft SharePoint provides users the ability to save digital content on a central deposit. In this way, users have the ability to search for secured digital content. This provides the organization the advantage to share digital content, without risking loss. *Tracking and control management* of digital content is done by the logging database. According to Microsoft, the system helps safeguarding digital information from unauthorized usage both on-

line and offline, inside and outside a firewall while enforcing rights. In this way, *persistent protection* is achieved per digital document [Mic06d, Mic06c, Mic06a].

6.3 DOFS

DOFS stands for Display-Only-File-System and is an EDRM system as a complete solution provided by Rether Networks Inc. [Inc05]. This EDRM system uses other techniques to secure digital content against inside and outside attackers. Figure 6.2 provides an overview of the DOFS infrastructure. As shown in the figure, the users are authenticated by the DOFS server and are logged on by a terminal session. This terminal prevents transferring digital content from the DOFS server to the remote client. In this way, the real bits of digital content never reach the client side. Content is encrypted and stored locally on the server. The first criterion needs the system to be a *client-server based information technology system*. This certainly is the case because *terminal sessions* are based on client-server models and this system at least uses a server and one or more client systems. Because all the actions on digital content remain on the DOFS server, critical operations such as checking in, modification, deletion, printing, including as email attachment and checking out are fully monitored, logged and controlled by a *tracking and control management* part of the system. The *distribution model* of digital content consists of several possibilities. Search mechanisms can be used or an organization can only choose to use a push strategy for acquiring digital content by other users. When emailing content, a content identifier is encrypted and sent to a recipient. In this way, the actual content still does not leave the server. Rights are stored on a central database which supports the terminal controller for enforcing rights. This mechanism ensures *persistent protection* by controlling digital content on the server [ASF04, YcC04a, YcC04b].

6.4 Authentica Active Rights Management

Authentica's system is an EDRM system as a complete solution. The system uses encryption techniques and stores them next to rights policies on a central server. When an Authentica client application intends to open a rights-protected file, it must connect to the central server to get the keys and rights policies. The used technique to store rights differs from Windows RMS, because with Authentica the rights are not distributed together with the protected files. This system uses the Server to store decryption keys, rights policies, audit logs and authentication configurations. In this way, the digital container (secured document) only consists of

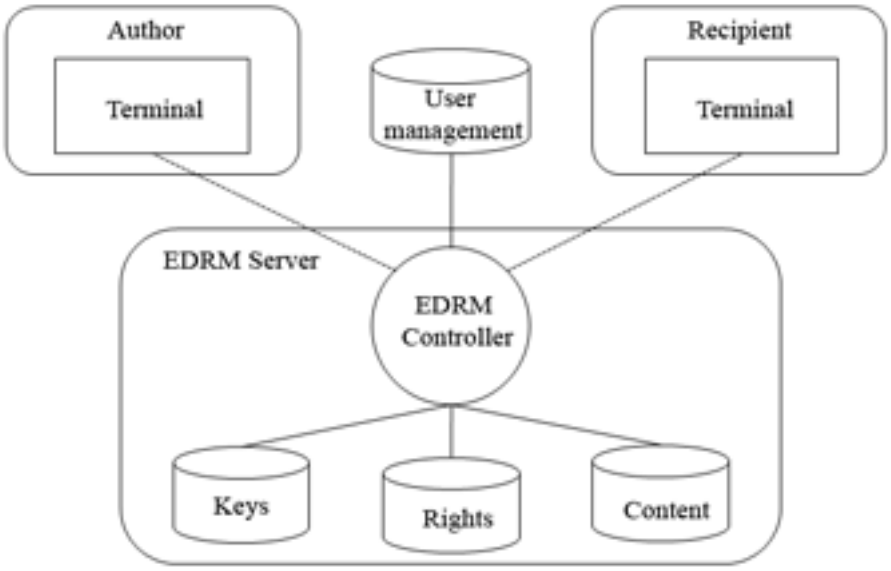

Figure 6.2: EDRM system: Display-Only-File-Server

encryption of content. The client plug-in receives the symmetric decryption key by using RSA communications keys after authentication to decrypt digital content and to receive the rights policies. Between the system components, a SSL channel is used to transfer data on a secure way. All activities are logged on the Policy Server. The client authoring component encrypts the protected file content by a symmetric key from the Policy Server. It also computes a message digest and passes it to the server for verification of the protected content's integrity in future. Once the rights policies are registered on the policy server, a recipient must connect to the server and be authorized to receive the decryption keys. The separation of rights policies with its protected information also ensures that the rights policies can be changed dynamically very easily for all content. Client authentication to the policy servers can be supported by existing LDAP Directories, Active Directory, or digital certificate.

Authentica also supports a work-offline mode, if the rights policy allows the protected files to be accessed offline. In this case, once the user authenticates to the Policy Server, a lease is generated and the rights policies will be distributed to the

client computer temporarily. Therefore, users do not have to connect to the Policy Server to access the file until the lease permission expires, and the full audit log of the offline access is sent to the server when the user connects back to the Policy Server. In this way, Authentica fulfils all demands to be EDRM according to the criteria. Figure 6.3 gives an overview of Authentica Rights Management system.

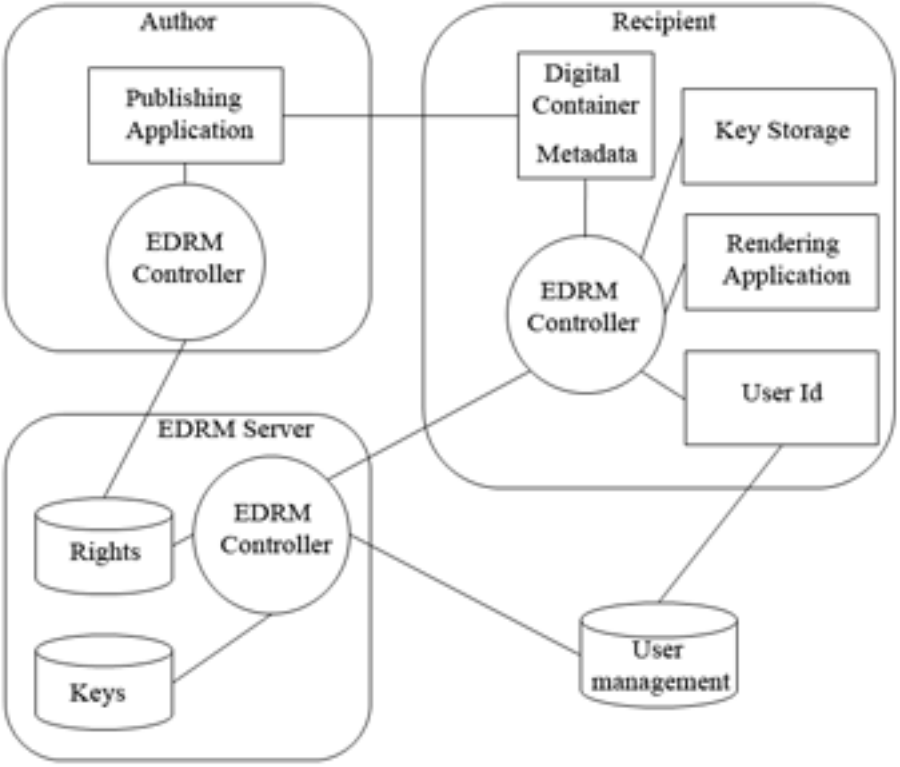

Figure 6.3: EDRM system: Authentica or Adobe LiveCycle

6.5 Adobe LiveCycle

Adobe's EDRM system was one of the earliest implementations on the market. Adobe is the supplier of one of the major eBook formats, and used to secure digital content in by converting documents first into a PDF format. Unlike Authentica and Microsoft RMS, the original aim of Adobe's DRM system is to protect digital content that are published in the PDF format.

Nowadays, the product LiveCycle suite is a collection of programs that allow creation and management of protected Office files and pdf. The Adobe LiveCycle

Document Security system is a web service that secures digital content into a digital cryptographic container designed for a specific recipient like RMS and Authentica. The Adobe LiveCycle Policy Server is used for management of the protected content by adding functionality like document expiry dates and changing user rights after distribution. LiveCycle Document Security enables organizations to bring paper-based business processes online by providing digital signature and encryption capabilities in a server environment. LiveCycle Document Security can be used to secure several digital content formats by using plug-ins per application. The LiveCycle server enables users to create own policies, which can be applied to digital content. Users can access the web service and distribute in this way digital content. The server uses tracking and logging mechanisms on each activity which is taken place by users. Because of the similarities with Authentica, figure 6.3 gives an overview of the Adobe EDRM system as well. In this way, Adobe LiveCycle does fulfill all criteria to be EDRM as well.

6.6 Conclusions

The goal of this phase is to create a complete set of current EDRM systems. This was done by using available literature and using search engines to collect these systems. The gathered systems where proven to be EDRM by using the properties developed from the definition analysis (Chapter 3). The following systems where found and described during this phase by using the developed definition:

1. Microsoft RMS
2. DOFS
3. Authentica Active Rights Management
4. Adobe LiveCycle

By using available literature, no other known EDRM systems were found. Literature was selected by using the definitions analysis. All referred resources from this document are used to gather these EDRM systems. During the project, the systems were tested in real life to verify documentation. Because I cannot be certain whether all available literature is used, I cannot be certain whether all EDRM systems were used during this research project. In this way, it is certain that the well known systems are used during this research project. It seems that Adobe and Authentica use the same techniques as an EDRM solution. Because the topic is new and innovations are still taking place by EDRM producing companies, it is possible new EDRM systems are developed after publishing this document. Chapter 7 is

needed to create properties of the described EDRM systems by using the developed requirements and measurements from the Selection Criteria model from Chapter 5. After completing these properties for the described EDRM systems, it is possible to compare the systems by using developed results from the selection criteria model according to Aia Software (Chapter 8). These results are developed by applying that model as a business case by using the supervisor of Aia Software as a stakeholder. First EDRM system properties are gathered in Chapter 7.

Chapter 7

EDRM system properties

This Chapter describes EDRM system properties for all gathered EDRM systems from chapter 6. Because it was necessary to compare EDRM systems (Chapter 9) according to the requirements from Aia Software, there is need to determine in what way the EDRM systems fulfill certain requirements. These requirements are gathered by applying the Selection Criteria Model. The developed *Selection criteria model* (Chapter 5) is used next to the current set of EDRM systems (Chapter 5) to develop the requested system properties in this Chapter. The following section describes the used research method. This phase results in a complete set of EDRM system properties per EDRM system related to the Selection Criteria Model.

7.1 Research Method

To be able to research the properties of these EDRM systems, it is necessary to gather the properties per requirement per EDRM system. In Chapter 6, a list was gathered with current EDRM systems. Now, it is necessary to reveal more details from these systems, which allows comparison of these EDRM systems in Chapter 9. To be able to gather these EDRM specific properties, the following resources are used:

1. Available literature from internet and scientific resources.
2. Testing these systems to reveal the mechanisms.
3. Using contact with EDRM producing companies.

Literature, testing and contacts with producing companies were used as a resource to gather the requested EDRM system properties. To be able to test the

EDRM systems, these systems were installed locally to discover certain properties or verify literature. The requirements were used as guidelines for investigating these properties per EDRM system. The following sections give an overview of all gathered properties categorized per EDRM system. The same consistent categorization is used to describe the system properties.

7.2 Microsoft RMS

Microsoft RMS is a component based EDRM system and can be used with a combination of other Microsoft components. The following subsections describe the working of the system by using the selection criteria model and the described measurement per criterion.

7.2.1 Content management

These properties concern the functional properties of content management.

Content creation

Office applications can be used to create digital content. All office applications allow the user to secure digital content straight to the hard disk. The application encrypts the digital content before saving it (from memory), and it is also possible to first save digital content as test results showed. Next to this, Client-side API's can be used to create RMS compliant applications. In both ways, it is possible to assign several rights to certain users. It was not possible to capture secured content by using e.g. Macro-functions from Office. Other capturing tools were not tested [Mic06d, Mic06c, Mic06a].

Content metadata

RMS uses metadata like author, title and a short description, which can be accessed without decrypting the digital document. That data can be used to search for these properties or finding out who is the author of a certain document [Aut05a].

Unique identifiable content

All content is encrypted with a symmetric key (AES). All content is unique and secured next to the assigned users, rights and conditions. Hash techniques are used

to verify the contents id and the necessary keys are secured on the server. The content is encrypted by using one symmetric key, but each user uses RSA to receive that particular symmetric key. These keys are received by the client application when authorized. Next to this, each encrypted document is bounded to an signed issuance license by the server distributed by the author. The server provides an end-user license when the user is authorized [Mic06d, Mic06c, Mic06a].

Distribution model

For distribution, users have the ability to encrypt digital content and distribute it manually or use the content management system which offers other users to search for (full text search). In this way, classified information remains safe and does not exist for unauthorized users.

Searchability

Digital content can be distributed by using Microsoft SharePoint as a content management system. In this case, one content version is used at SharePoint and users have the ability to search through the digital content. When unauthorized users want to access it, they need to ask for permission from the author. The SharePoint uses a super user-key which enables users to search through digital content (like search engines), and therefore it is necessary to only allow authorized users to SharePoint. Because documents are indexed by SharePoint, unauthorized people would be able to search through content on an illegal way [Aut05a].

Partial asset protection

With RMS it is not possible to provide several rights assigned to secure parts within digital content. Authors have the ability to assign users with rights, conditions and the whole digital document [Mic06c].

User access to information about rights

A user who is not allowed to access digital content can retrieve information (metadata) about the author, who could be contacted for rights approval [Mic06d].

Personal backup

Microsoft does not support personal backup. The users are responsible for creating their own backups per digital content. Because rights are encrypted with the digital content, multiple copies might be distributed with each its own rights [Mic06d, Mic06c, Mic06a].

7.2.2 Tracking and control

For tracking and control management it is necessary to identify misusage by users.

Logging content usage

When creating digital content, users and rights are assigned to the digital document (digital container). The RMS server receives a list of potential users which can be chosen from to assign rights and potential conditions. Each time a user wants to access digital content, the user needs to authenticate at the RMS server (by using an authentication protocol). When a user accesses digital content, logs are made when requesting the appropriate key for encryption. Because the rights are stored locally with the content, the client application uses the restrictions which are locally stored. Because several copies of digital content can be used with several different rights, not all rights associations are stored on the logging database. When a recipient user accesses digital content, logs are made about accessing digital content [Mic06b].

Watermarking

It is only possible to use watermarking when printing documents with Office applications. Watermarking can be used for other file-extensions like XPS or PDF. Print screen attacks were possible by using virtual machine software. In this way, it is not possible to protect documents against these techniques and watermarking might be inevitable [Mic06b].

7.2.3 User management

These properties concern the functional properties concerning user management.

User registration

For user registration the active directory can be used at organizations or .net passport features for authentication. Active directory can be used by system engineers to create and delete accounts. In this way, it is possible for an engineer to change the account of a user to be able to use the rights from certain digital content by simulating the user with the needed rights. In this way, it is almost impossible to create a completely safe protocol unless you can trust certain employees/administrators. Next to this, it is possible to create a super-user, who has the possibility to access all digital content by using settings on the RMS server. It is necessary to keep classified digital content only among the necessary users, because administrators have rights to read classified information as well. This is possible, because it is not necessary to share secured digital content on a central deposit (SharePoint) and all rights and privileges are secured in the digital content itself. When classified digital content is only distributed to authorized users, it is possible to keep the digital content secure [Mic06d, Mic06c, Mic06a].

Scalability

Scalability is another feature, which should be supported. RMS can be expanded by creating clusters of servers, which ensures an adjustable scalability. Processes like encryption are the most consuming mechanisms of the system, but are taken place at the client. According to Microsoft, scalability is not an issue and it is possible to expand the infrastructure to support many users, such that it does not matter how large the company is [Mic06a].

Uniquely identifiable users

Active directory or the .NET passport mechanism can be used to provide authentication. Each EDRM client must be set up with a RMS lockbox before usage and ensures the usage of an authenticated client (client enrollment). The lockbox is defined as client software, which receives the keys and enforces the rights. By installation of a lockbox, the server is able to trust the client system. Furthermore, it is possible to communicate between the client and the server in a secure way. All authenticated users have the ability to use all trusted client systems which are prepared with a lockbox. The RMS server caches all users from the user management to be used for assigning with rights and content [Mic06a].

7.2.4 Rights management

The following properties are concerned with rights of digital content and the related users.

Rights per digital content and user

EDRM systems offer techniques to assign rights to users and digital documents. The following rights: view, edit, print, email, copy-and-paste, screen capture are available within RMS by using XrML certificates. XrML is a rights expression language (REL) and is used to develop critical rights management providing interoperability between potential other EDRM systems. XrML provides a simple-to-use, universal method for expressing rights that are linked to the use and security of digital content. Because of XrML, developers can easily integrate other existing rights management systems. The XrML certificate is bounded to the secured digital content and not stored on the database. Encryption keys (AES) and other transportation keys (RSA) are stored on the server.

Limited document usage

It is possible for authors to set an expiration time with digital content. Next to this, it is not possible to specify a start date (embargo) [Mic06d].

Rights transfer

When a user creates a digital document, this user is defined as the author with full rights. This user has the ability to assign rights to other registered users. Because the rights are stored in the digital container itself, each copy could consist of several rights with several users. When a user wants to have more rights, he could contact the author and the author could prescribe more rights by sending the same document, with extra rights.

Next to this, there are revocation lists, which can be used by system administrators. The system administrator has the ability to revoke content files, rms-enabled applications, client systems, user id's and publish/use licenses. The system administrator has the possibility to write program code in XrML and thereby enforcing certain flexible constrains on these entities. Although XrML is developed as a standard, not each administrator would be able to write the needed code. This leads to inconvenience, because when a system administrator wants to change rights to a digital document he needs to:

1. Revoke use license for the documents
2. Create new publishing license to the content with new users
3. Revoke old publishing licenses
4. Send new files to users who are authorized

The disadvantage of this system is that a system administrator must be contacted and the administrator must be able to know the XrML language to enforce rights by using a computer language on the RMS server environment [Mic06d].

Dynamical rights

Because all rights are secured in the digital container, rights are not controlled in a dynamical way. When an author needs to limit rights for a certain user, there is need to contact the system administrator to enforce rights on certain digital content by using XrML as described in *rights transfer*. Next to this, it is necessary to redistribute digital content to all authorized users again, with the new licenses [Mic06d].

Rights templates

RMS supports the use of rights templates. Policy rights templates reside in the RMS database and are always used when a use-license is created such that the most recent policy set by the RMS administrator is enforced. Each template created must be exported to each RMS client computer that needs to use the template. These local versions of the templates do not need to be updated every time the RMS administrator updates the template, because the RMS server uses its own copy when evaluating the rights specified in the template.

Content versioning

Several versions can be developed with different kinds of rights. These versions can be shared in SharePoint to support other users [Mic06d].

Rights and protected content recovery

It is not possible to store rights and protected content recovery. Assigned rights and users from deleted content are deleted with the digital content [Mic06d].

7.2.5 Security management

These properties concern the non-functional security properties of RMS.

Key individualization

All digital content is secured by each an own symmetric key. This symmetric key is furthermore securely transferred by using (PKI encryption) a RSA 1024 bits key mechanism. Because each secured document is unique, each document needs an own key to be encrypted or decrypted. The RSA communication keys are different per user [YcC04a].

Decryption keys non-disclosure

The symmetric encryption keys remain secure per digital document and are used to encrypt and decrypt the digital content. The RSA key is sent by a secured http protocol after authentication (with the user and its device) and cannot be captured during transfers, because SSL is used to transfer data through. The only way to capture the encryption key is to perform reverse engineering techniques at the client environment. Because the symmetric key must be stored at the client side while accessing content, it should theoretically be possible to reverse engineer the client software and capture the main key. In this way, the client software is relative safe but 100% safety cannot be guaranteed. Because RMS is integrated on the underlying operating system, the mechanism is the safest way by using keys and the encrypted content at a relative insecure environment [Mic06d].

Renewability

Microsoft offers Microsoft update facilities to improve software in case of invulnerabilities [Mic06d].

Standard key management

Symmetric key usage with AES for document encryption and decryption is used. Asymmetric key usage with RSA provides security when sending encryption and decryption keys [Mic06d].

Tamper-resistance

As mentioned before, the client receives several keys to decrypt the digital content according to specified rights. During the research project the system was tested when securing content and using licenses. It was not possible to capture the data with tracking tools, because the client encrypts the data directly as a secured document. Next to this, macros where used to created backups of the secured digital content, but it was impossible during the project to create an insecure file on an illegal way. Print screen attacks were possible by using virtual machine software. In this way, it is not possible to protect documents against these techniques and watermarking might be inevitable. According to literature it should be possible in theory by using reverse engineering practices to capture the original content, but this practice was not done during the research project [YcC04a].

No single point of failure

The RMS server seems to be a single point of failure, because it should be operable when creating or consuming digital documents. The Active Directory is in this way a single point of failure, since it is used for identification of users. The RMS server needs to secure the keys in a configuration database, which is always required for encryption or decryption of digital content. Microsoft acknowledges these single points of failures and recommends to use clusters of servers to balance the traffic load. Next to this, it is necessary to use backup mechanisms to create backups of all data like Active Directory, licensing service, certificate service and the related databases. This assures an organization to recover from backups when the system is down, clusters can be used directly to substitute down services. In this way, single points of failure can be limited. Microsoft developed a document for scaling disasters and recovery plans. It seems that problems can be reduced to the minimum and there does not have to be a single point of failure as long preparations are made [YcC04a].

7.2.6 Other non-functional properties

These properties concern other non-functional properties of the RMS system.

Simple installation

The RMS system can be installed easily by using RMS service packs on windows clients and windows servers. Databases can be generated automatically by using

MS SQL server. Content Management System called SharePoint can be installed easily as well and used for defining groups and sharing digital contents [Mic06a].

Maintainable

RMS can be seen as maintainable. Administrators have privileges to adjust certain rights in case of problems. Next to this, updates are offered by Microsoft to improve services and fix bugs [Mic06a].

Portability Platform shifting

Servers need to be prepared as Microsoft Windows 2000 or 2003 server. All clients need to be installed on a windows platform [Aut05a].

Portability - Format shifting

It is not possible to convert a secured digital content to another file type, but when a user has enough rights, it is possible to copy-paste content into another application, by using the clipboard [Mic06d].

Portability - Time and space shifting

It should be possible to create and read digital content from outside an organization. RMS uses Active Directory or the .NET passport to verify users and their privileges. Active Directory at other organizations (e.g. partners) can be used and connected to provide support at these locations. Next to this, it is possible to use offline usage on a trusted (enrolled) client. A user has for example the possibility to use the trusted laptop at the home location. In this way, the user could access documents offline and the system would download the requested keys. Next to this, the expiration date is set and the user has the ability to use offline usage for a certain period. The keys are downloaded and used locally. The system handles a micro safe with a time tampering system. When the user tries to chance the system time, the client will not allow access any more, till the user goes online to verify authorization.

Integration with existing applications

There is a Windows Rights Management SDK available at Microsoft, which enables software developers to add RMS functionality to other applications with complete documentation and examples. Many organizations that create digital content use

applications that were not developed by Microsoft. The availability of the RMS SDK enables a more comprehensive solution. For the recipients of rights-protected information who do not have access to RMS-enabled programs, a trusted RMS-enabled browser, the Rights Management Add-on (RMA) for Microsoft Internet Explorer is available. Software engineers are able to use API's to make an application RMS compliant. Next to this, SOAP can be used for interaction with RMS servers to retrieve keys and other necessary data. All kinds of applications can be made RMS compliant to support EDRM [Mic06d, Mic06c, Mic06a].

7.3 Display-Only-File-Server

As described in the previous chapter, the DOFS system uses a terminal session which enables users to login at the server. All content stays at the server as long as the users work online. All client software in this case runs on the server and users only operate the controls on the server and not the client. In this way, a client never receives the actual bits of the digital content. The terminal software is prohibited to use print screen functionality and transfer data to the client. The following sections describe the properties for DOFS.

7.3.1 Content management

These properties concern the functional properties concerning digital content of DOFS.

Content creation

When using DOFS, all content is created directly on the server in a secure way. The digital document is assigned with rights and users. In this way, other users have the ability to use their rights on the same way via a terminal session. When created content is classified, it should only be available for the authorized persons. There aren't API's available to create secure digital content, such that it is only possible to create digital content with existing supported applications like MS Office, acrobat PDF software and postscript viewers [YcC04b, YcC04a, Inc05].

Content metadata

Content metadata such as author, title and description are available [Inc05].

Uniquely identifiable content

The created digital content is uniquely stored on the server, by using hashing techniques. In this way, it is possible to create documents with the same contents but different identifiers. This information is secured with the digital content and remains on the server. After authentication, the users receive rights on the server via terminal sessions. All content remains at the server [YcC04b, YcC04a, Inc05].

Distribution model

Users have the ability to email other users an encrypted package, which contains a location on the server. After another user receives the digital content, it is decrypted (when authorized) and this user can also access the digital content via a terminal session [YcC04b, YcC04a, Inc05].

Searchability

Users have the ability to browse for digital content, but cannot use full text search mechanisms to find digital content. The producing organization does not provide features for searchability [YcC04b, YcC04a, Inc05].

Partial asset protection

It is not possible to secure parts within digital content, only the whole content file [YcC04b, YcC04a, Inc05].

User access to information about rights

When a user tries to access digital content without access, information can be received about the author. In this way, the author can be requested for permissions [YcC04b, YcC04a, Inc05].

Personal backup

All actions are taken place on the server. All documents could easily be back upped, but the system does not provide a personal backup feature [YcC04b, YcC04a, Inc05].

7.3.2 Tracking and control

In this section tracking and control management properties are discussed for DOFS.

Logging content usage

All actions take place on the server. DOFS uses this advantage by logging each action per user and digital content [YcC04b, YcC04a, Inc05].

Watermarking

All created digital documents are marked by watermarking techniques and a signed id by its author [YcC04b, YcC04a, Inc05].

7.3.3 User management

This section describes all properties of DOFS concerned with user management.

User registration

For user registration, the active directory mechanism can be used. In this way, domain administrators have possibilities to authenticate as other users. Administrators have the possibility to capture and copy rights and to create a new insecure file on the server. It should not be very hard to capture digital content by administrators and therefore they should be trusted.

Scalability

Scalability is another issue, which in comparison with the other EDRM systems is hard to achieve. Because all transactions are processed by the server, the server must be load balanced by multiple servers. All users and documents should be calculated first before implementing the system. In this way, the scalability risk can be limited, but the server transactions might be to complex and slow for larger organizations [YcC04a, YcC04b].

Uniquely identifiable users

Users are identified in a unique way by using active directory [YcC04a, YcC04b].

7.3.4 Rights management

This section describes all properties of DOFS concerning rights management.

Rights per digital content and user

Rights like read, copy-paste, write, email, copy and expiration are available for authors to assign to users[YcC04a, YcC04b].

Limited document usage

Authors have the ability to use expirations on digital content [YcC04a, YcC04b].

Rights transfer

There are possibilities for the users to transfer rights to other users. In this way, domain administrators have the ability as well to transfer rights [YcC04a, YcC04b].

Dynamical rights

Because all rights are located on the server, rights can be altered dynamically [YcC04a, YcC04b].

Rights templates

Rights templates are not mentioned in literature and in resources from the developing organization. In this way, it is not possible to create a rights template [YcC04a, YcC04b].

Content versioning

Content versioning is not possible unless the users develop their own versions on an alternative way [YcC04a, YcC04b].

Rights and protected content recovery

It is not possible to create certain rights templates. Users have only the ability to choose from the provided rights from the system [YcC04a, YcC04b].

7.3.5 Security management

This section describes all non-functional properties of DOFS concerning security.

Key individualization

On the server, encryption is used to secure digital content and the keys remain on the server. The pointer files which are decrypted and used for email purposes don't have to remain on the server, because the real content is not inside this encrypted document [YcC04a, YcC04b].

Decryption keys non-disclosure

Non-disclosure of decryption keys is maintained, because keys never leave the server environment [YcC04a, YcC04b].

Renewability

The organization does not provide updates in case of security breaches [YcC04a, YcC04b].

Standard key management

Symmetric key encryption is used to encrypt the content on the server [YcC04a, YcC04b].

Tamper-resistance

There could be multiple possible attacks on the client, but none of them should result into receiving the actual bits of the digital content. Inside attackers could try to bypass the client control for example, but this could only result into losing the connection with the server. Attackers could also try to infiltrate Trojan horses, but usage of firewalls and virus scanners should limit these risks. Because no bits actually leave the server, it is not possible to capture information by using the terminal sessions and remains secure in comparisons with other client software [YcC04a, YcC04b].

No single point of failure

The DOFS server is certainly a single point of failure and therefore a cluster of load balancing servers and backup servers should be used. In this way risks are limited against for example a DoS attack. Because all transaction are processed by the server, it should be disastrous when the servers are unavailable [YcC04a, YcC04b].

7.3.6 Other non-functional properties

This section describes all other remaining non-functional properties of DOFS.

Simple installation

The implementation for DOFS could become quite complex when more users use the system. Most organizations use normal client-server installations and not terminal sessions. In this way all servers and clients need to be restructured and therefore this implementation becomes more complex in comparison with other EDRM systems [YcC04a, YcC04b].

Maintainable

The infrastructure is maintainable when the number of users is limited. In case of usage by very large companies, the system could become instable and complex, because all actions must be done by the server [YcC04a, YcC04b].

Portability - Platform shifting

For client software only the following platforms are required: Windows NT, Windows 2000, Windows XP and Windows 2003. For the server there is need for: Windows 2000 server or Windows 2000 advanced server with Terminal Service support [YcC04a, YcC04b].

Portability - Format shifting

It is not possible to change the format of digital content, but with enough rights it is possible to use (copy-paste) contents with several content extensions [YcC04a, YcC04b].

Portability - Space shifting

The DOFS mechanism was implemented with a tamper-resistant offline mechanism. In this way it is possible to encrypt the digital content and use the bits outside the organization. All content is secured into an executable program with integrated rights. The designers of the system only developed this mechanism to compete with other EDRM systems. This way of encryption is at least as safe as the offline usage mechanism provided by Microsoft RMS, Authentica and Adobe. Although it is possible to use offline usage, it is not recommended to be used, because complete security cannot be achieved. In this way, the content can be accessed everywhere on each location [YcC04a, YcC04b]

Portability - Time shifting

Time shifting is completed as well as mentioned in the previous criterion about space shifting [YcC04a, YcC04b].

Integration with existing applications

It is possible to connect with the DOFS server and use existing applications on other servers to secure digital content in theory, but in practice there are none working examples available and documentation is not provided. SDK's are not available to make existing applications DOFS compliant [YcC04a, YcC04b].

7.4 Authentica Active Rights Management

Authentica has developed a security mechanism to secure PDF content in 1999. The product's original name was PageRecall and was based on converting digital content into PDF and then securing it with rights and encryption. One year later they focussed on securing mail content, which forces users to email only users with certain content which was allowed. Recently, Authentica came with Secure Office, which provides EDRM functionality for Microsoft Office documents and not only converted PDF extensions. The Active Rights Management infrastructure uses a rendering application as well. In this case, the Microsoft Office applications are used with an EDRM controller as a plug-in to enforce restrictions on the content. The system uses encryption techniques and stores them next to the rights policies on a central server, which is different in comparison with RMS. When an Authentica client application intends to open secured digital content, it must connect to the central server to retrieve the keys and rights policies after authentication. This

system uses the Policy Server as a central server to store decryption keys, rights policies, audit logs and authentication configurations. The following sections gather the system properties according to the developed requirements.

7.4.1 Content management

These properties concern the functional properties of digital content for Authentica.

Content creation

Content creation can be done by users by using Microsoft Office software. Authentica delivers a plug-in, which can easily be installed on the client. This plug-in software is used as the EDRM controller and renders the content according to prescribed rights. Authors are required to create and save digital content locally and secure it using the EDRM controller. In this way, it is always necessary for users to save their document first before encrypting. After the document is saved, the plug-in encrypts the saved document. In this way, it is possible for authors to keep copies of the initial content. This could (unintentionally) lead to leakage of critical information in the first phase. If there cannot be created a temporary insecure content file, the plug-in cannot secure it. I have tried to develop an Office macro function, but I was not possible to capture content illegally [Aut05b, Aut05a].

Content metadata

Metadata with secured content is used: Author, title, description [Aut05b, Aut05a].

Uniquely identifiable content

All created digital content is uniquely identifiable and all policies are stored on the server. The system uses a hash function (SHA) to create a unique id (fingerprint) of digital content. Because the policies of all users to assigned content is stored separately from the file itself, it is necessary to identify each file to be able to assign the correct rights with the correct user and to provide the encryption key [RD03, Aut05b].

Distribution model

The distribution model is formally based on a push strategy from one user to another user. Documentum, IBM Content Manager, Hummingbird Enterprise can be used

as a content repository, but it is not possible to use full-text-search, because the digital content remains encrypted. Although these content management systems will work with the EDRM architecture, the CMS is not designed for all features with integration of this EDRM system. Experiences from literature and practice are rather scarce. The system provides an additional right called embargo date, which could be used to provide classified digital content to be readable after a certain period [RD03, Aut05b].

Searchability

Authentica can be advanced with content management (Documentum, IBM Content Manager, Hummingbird Enterprise) easily and users can access the digital content when rights are prescribed [Aut05b, RD03].

Partial asset protection

It is not possible to secure parts of digital content [Aut05b, RD03].

User access to information about rights

The system reveals the identity of the author to recipient users when access is denied. In this way, it is possible to request rights by contacting the author [RD03, Aut05b].

Personal backup

Authentica does not offer a personal backup feature within the system. Although, everything but the encrypted content is located on the server, it is possible to reuse rights on new content. Next to this, alternative backup techniques can be used to create backups [RD03, Aut05b].

7.4.2 Tracking and control management

This section is concerned with tracking and control management properties for Authentica [RD03, Aut05b].

Logging content usage

All keys and policies are gathered on a central server. In this way, the user must contact the server for authentication en authorization. All actions from users are recorded by the server and logged in a central database [RD03, Aut05b].

Watermarking

Watermarking can be used on PDF files or printed office documents. Print screen attacks were possible by using virtual machine software. In this way, it is not possible to protect documents against these techniques and watermarking might be inevitable [RD03, Aut05b].

7.4.3 User management

This section describes the properties for user management of Authentica.

User registration

The same problem occurs as described for RMS. Because Active Directory provides certain privileges to domain administrators, it is always possible to capture digital content by these user roles. The difference with RMS, provides system administrators another advantage to reveal information. All usage is logged and can be captured by these system administrators. Next to this, rights can be captured because these are located on the server, the only required to steal digital content is the secured content file. In this way, it should be necessary to divide administrator roles for Active Directory and the Policy server. This should lower the risk, but when an active directory administrator knows who has full control about certain content, it is possible to change credentials and capture the content by using the authors (full control) rights [RD03, Aut05b].

Scalability

Scalability is maintained in the same way other EDRM systems are scaled. Authentica recommends clustering of servers, which should balance the workload. The server stores all keys and privileges and has more workload compared to RMS because all rights are stored at the server as well, but this will not be a problem when adding more server clusters [RD03, Aut05b].

Uniquely identifiable users

Users can be uniquely identified by using active directory or .NET pasports. Other authentication mechanisms can be implemented as well [RD03, Aut05b]:

1. SSPI, native windows login
2. LDAP
3. X509 certificates
4. RSA SecurID cards or SmartCards

7.4.4 Rights management

This section describes the properties for rights management by Authentica [RD03, Aut05b].

Rights per digital content and user

Like other EDRM systems, it is possible to assign rights to digital content. As mentioned before these rights are directly stored on the policy server per digital content and assigned user. These rights include: View, Print, copy-paste, edit, embargo date and expiration date [RD03, Aut05b].

Limited document usage

The policies concerning digital content can be refined by conditions as well. These conditions e.g. expire date or embargo date can be used to expand standard rights. Next to this it is possible to use policy templates, which can be used on group level within organizations. This helps organizations to prescribed usage of rights for authors within defined groups [RD03, Aut05b].

Rights transfer

Because the rights per digital content are stored on the central policy server, it is possible to transfer rights on a central way. It does not matter how many copies are distributed among users, because all users must authenticate themselves at the policy server before accessing digital content [RD03, Aut05b].

Dynamical rights

As previously described with *rights transfer*, all rights are centrally stored on the server. This implies rights can dynamically be altered [RD03, Aut05b].

Rights templates

It is possible for administrators to define templates, that prescribe certain rights for authors [RD03, Aut05b].

Content versioning

It is not possible to use content versioning with the system, but content management systems can be used to support this feature [RD03, Aut05b].

Rights and protected content recovery

Rights can be saved like a rights profile, but there are no standard ways to backup digital content. Alternative backups need to be used to complete this feature [RD03, Aut05b].

7.4.5 Security management

This section describes the properties concerning security management of Authentica.

Key individualization

Each user which is authenticated by (e.g.) Active Directory uses a temporary session key to communicate with the policy server by a Secure Socket Layer (SSL). The content contains a unique identification and is received from the server next to the symmetric encryption/decryption key. The EDRM controller (client plug-in) uses these credentials to render the content. In this way, key individualization is handled per session for authentication and for encryption of digital content [RD03, Aut05b].

Decryption keys non-disclosure

The symmetric decryption/encryption key is transferred by a SSL communication protocol secured by an asymmetric session key. The decryption key remains secure as

long as the plug-in is safe. This plug-in is less integrated with its client environment and therefore offers more risks. Compared to RMS this plug-in only operates on the application layer. All underlying layers could be used to capture information. Because reverse engineering practices can result into disclosure of the decryption key, disclosure of decryption keys cannot be completely met [RD03, Aut05b].

Renewability

Authentica offers downloadable updates in case of security invulnerabilities. In this way, software can be updated [RD03].

Standard key management

Symmetric key usage with AES for document encryption and decryption is used. After authentication an SSL protocol combined with an RSA algorithm allows it to transfer the decryption key to the client [Aut05b].

Tamper resistance

The plug-in is installed at the application level of the system. This level is not explicitly safe against reverse engineering. After reverse engineering practices it is possible to develop another plug-in, which can be installed on clients to capture the symmetric encryption/decryption key. Print screen attacks were possible by using virtual machine software. In this way, it is not possible to protect documents against these techniques and watermarking might be inevitable. Therefore this system is not tamper-resistant [RD03, Aut05b].

No single point of failure

The server could become a major single point of failure. Documentation is provided by Authentica for clustering servers to achieve balanced loads, provide backups and keep services online [RD03, Aut05b].

7.4.6 Other non-functional properties

This section describes other non-functional properties of Authentica.

Simple installation

The installation of Authentica is even easier compared to RMS. The plug-in is compliant with all windows operating systems and for all office versions these plug-ins are available as well. Active Directory can be used for authentication and the policy server can be installed by using available installation manuals [RD03, Aut05b].

Maintainable

Server and client software consist of minimum extra software add-ons and is very easy to maintain. Updates can be downloaded when necessary in case of security breaches [Aut05b].

Portability - Platform shifting

Authentica's server software runs on Windows NT Server 4.0, Windows 2000 Server, Windows Advanced Server, Windows Server 2003, and Sun Solaris 2.8 and 2.9. In this way, it is possible to shift between platforms [Aut05a].

Portability - Format shifting

It is not possible to export a certain secured file extension to another file extension, although it is possible to reuse content from one file to another file (copy-paste) [Aut05a].

Portability - Space shifting

This feature enables users to access the digital content wherever the user wants to. As long as the plug-in is installed, session keys are communicated with the server. In this way, it is possible to use the content on each authenticated system by the domain server [RD03, Aut05b].

Portability - Time shifting

Offline usage is possible and the necessary keys are stored on the local client system (which is not 100% safe), where the client plug-in can use it. There is need to use a certain expire time when accessing content and the user must go online within a certain period to verify whether the policy is still valid. Online access can be done

by using the online security service or LDAP and Active Directory authentication [RD03, Aut05b].

Integration with existing applications

Many platforms are supported and a server-side SDK can be used to communicate with the server and secure digital content. Windows NT Server 4.0, Windows 2000 Server, Windows Advanced Server, Windows Server 2003, and Sun Solaris 2.8 and 2.9 are the supported operating systems as a server. Although this SDK is available, it is quit hard to find supportive documentation and examples, which can be seen as a disadvantage [RD03, Aut05b].

7.5 Adobe LiveCycle

Adobe LiveCycle is another application plug-in based EDRM system, which has remarkably many similarities with Authentica. The organization of the famous PDF document format developed next to securing PDF files an EDRM security mechanism for Office applications as well. This system is evaluated in the following sub sections.

7.5.1 Content management

This section describes the functional properties concerning content management of Adobe.

Content creation

Like Authentica, this plug-in needs to save the digital content first on a temporary location before encrypting it. Adobe introduced Document Center, a web-based service that allows business users to safeguard, share and trace the usage of Adobe PDF and Microsoft Office documents. In this way, users have the ability to search for content in the document center only by authenticated users. Content can be created by using own developed applications by using the server-based SDK [Ado07e].

Content metadata

Metadata with secured content is used: Author, title, description [Ado07e].

Unique identifiable content

The plug-in creates a unique id from the secured digital content, which is used by the plug-in to authenticate the digital content to the Policy server. SHA-1 Hash technology is used on digital documents to create a unique number. The unique identifier is stored on the server to authenticate the documents and verify the requested keys [Ado07a, Ado07d, Ado07c, Ado07f].

Distribution model

The distribution model for Adobe can be determined by the author. It is possible to send documents directly to the recipient or to add the document to the online content management (Adobe document center) [Ado07e].

Searchability

Searchability can be provided by the Adobe Document Center, where documents can be searched for by using metadata or full text search. Adobe Document Center is a new Web-based service that will allow business users to safeguard, share and trace the usage of Adobe PDF, Microsoft Word and Microsoft Excel documents [Ado07e].

Partial asset protection

It is not possible to secure only parts of a document or assign certain rights [Ado07e, RD03].

User access to information about rights

The system reveals the identity of the author to unauthorized users when access is denied. In this way it is possible to request rights by contacting the author [RD03, Ado07e].

Personal backup

Adobe LiveCycle does not offer a personal backup feature within the system. Although, everything but the encrypted content is located on the server, it is possible to reuse rights on new content. Next to this, alternative backup techniques can be used to create backups [RD03, Ado07c].

7.5.2 Tracking and control management

This section describes the tracking and control properties for Adobe LiveCycle.

Logging content usage

All actions with digital content are stored by the Adobe LiveCycle in cooperation with Document Center [RD03, Ado07e].

Watermarking

Watermarking can be used on PDF files or printed office documents. Print screen attacks were possible by using virtual machine software. In this way, it is not possible to protect documents against these techniques and watermarking might be inevitable [RD03, Ado07c].

7.5.3 User management

This section describes the user management properties for the Adobe system.

User registration

Adobe LiveCycle uses an administrator, which can be used to change policies on digital content and next to the domain administrator, these administrators have many privileges. Similar to Authentica, illegal usage by an administrator is possible.

Uniquely identifiable users

All users can be uniquely identified by using Active Directory or LDAP authentication protocols. Next to this, adobe offers an online user authentication mechanism, which offers users to use that server [Ado07c, Ado07d].

Scalability

Scalability should not be a problem, because servers can be clustered to balance load or prevent servers being down like Authentica and Adobe [Ado07c, Ado07d].

7.5.4 Rights management

This section describes the properties for rights management of Adobe LiveCycle.

Rights per digital content and user

There are several different kinds of rights possible to use on digital content like full rights, read, print, copy, transfer rights, expire dates [Ado07c, Ado07d].

Limited document usage

Conditions can be added to rights and digital documents. These conditions e.g. expiration date or embargo date can be used to expand standard rights. Next to this it is possible to use policy templates, which can be used on a group level within organizations. This supports administrators to prescribed usage of rights templates to authors [Ado07c, Ado07d].

Rights transfer

Because the rights per digital content are stored on the central LiveCycle server, it is possible to transfer rights on a central way by users or administrators. It doesn't matter how many copies are distributed among users, because all users must authenticate themselves at the policy server before accessing digital content [Ado07c, Ado07d].

Dynamical rights

As described with *rights transfer*, all rights are centrally stored on the server, whereby changing rights on a dynamical way is very easy [Ado07c, Ado07d].

Rights templates

It is possible for administrators to define templates (favorites), which can be used to prescribe certain rights by authors [Ado07c, Ado07d].

Content versioning

It is possible to use content versioning with the Document Center system, because rights are centrally controlled and stored [Ado07c, Ado07d].

Rights and protected content recovery

Rights can be saved like a rights profile, but there are no standard ways to backup digital content. Alternative backups need to be used to complete this feature. Content cannot be recovered when a document is deleted [Ado07c, Ado07d].

7.5.5 Security management

This section describes the properties concerning security management for Adobe LiveCycle.

Key individualization

Each user which is authenticated by for example Active Directory uses a temporary session key to communicate with the policy server with Secure Socket Layer (SSL). The content contains a unique id by using hashing techniques and is received from the server next to the symmetric encryption/decryption key (AES). The EDRM controller (client plug-in) uses these credentials to render the content. In this way, key individualization is handled per session for authentication and for encryption of digital content [Ado07c, Ado07d].

Decryption keys non-disclosure

Symmetric keys are transferred by SSL protocol and secured by an asymmetric algorithm (RSA 512 - 2048 bits key space). The decryption key remains secure as long as the plug-in is safe. This plug-in is less integrated with its applications and concerns more risks just like Authentica. Compared to RMS this plug-in only operates on the application layer. All underlying layers could be used to capture information. Because reverse engineering practices can result into achievement of the decryption key, non-disclosure of decryption keys cannot be completely met [Ado07c, Ado07d].

Renewability

Adobe offers downloadable updates in case of security invulnerabilities. In this way, software can be updated [Ado07c, Ado07d].

Standard key management

Symmetric key usage with AES for document encryption and decryption is used. After authentication an SSL protocol combined with an RSA algorithm allows it to transfer the decryption key to the client [Ado07d].

Tamper resistance

The plug-in is deployed on the application level of the system. This level is not explicitly safe against reverse engineering. After reverse engineering practices it is possible to develop another plug-in, which can be installed on clients to capture the symmetric encryption/decryption key. Print screen attacks were possible by using virtual machine software. In this way, it is not possible to protect documents against these techniques and watermarking might be inevitable. Therefore this system is not completely tamper-resistant [Ado07c, Ado07d].

No single point of failure

The policy could become a major single point of failure. Documentation is provided for clustering servers to achieve balance loads, provide backups and keep services online [Ado07c, Ado07d].

7.5.6 Other non-functional properties

This section describes other non-functional properties used with Adobe.

Simple installation

The installation of Adobe is the same as installation of Authentica. The plug-in is compliant with all windows operating systems, other platforms and suitable for all previous office releases. Active Directory, LDAP or online authentication mechanisms can be used for authentication and the policy server can be installed with the support of provided manuals [Ado07c, Ado07d].

Maintainable

Server and client software consist of minimum extra software add-ons and is very easy to maintain. Updates can be downloaded in case of security breaches [Ado07c].

Portability - Platform shifting

Adobe's LiveCycle server runs on Windows NT Server 4.0, Windows 2000 Server, Windows Advanced Server and Windows Server 2003 [Ado07c].

Portability - Format shifting

It is not possible to export a certain secured file extension to another file extension, although it is possible to reuse content from one file to another file (copy-paste) [Ado07c].

Portability - Space shifting

This feature facilitates users to access the digital content wherever the user wants to. As long as the plug-in is installed, session keys are communicated with the server. In this way, it is possible to use the content on every authenticated system [Ado07c, Ado07d].

Portability - Time shifting

Offline usage is possible and the necessary keys are stored on the local client system, where the client plug-in can use it. There is need to use a certain expire time for accessing and the user must go online within a certain period to verify whether the policies are still valid. Online access can be done by using the online security service or LDAP and Active Directory authentication [Ado07c, Ado07d].

Integration with existing applications

Multiple platforms are supported and a server-side SDK can be used to call API's by .NET or Java developers to support own developed applications [Ado07c, Ado07d, Ado07a, Ado07b].

7.6 Conclusions

In this chapter the gathered set of EDRM systems are discussed into more detail. The gathered set of selection criteria with related measurements from the selection criteria model are used and each EDRM system is analyzed by using literature, test scenarios and contact with EDRM producing companies. In this way, all properties

were gathered by using the selection criteria model and the defined measurements per requirement. Because the topic is rather new and innovations could be taken place anytime, there is a risk that the properties are not up-to-date. Some articles where rather vague about certain properties, but contact with EDRM producing companies and testing these systems resulted in more specific properties. It is recommended to keep up-to-date and informed when new innovations are taken place.

After analyzing the EDRM system properties, I divide EDRM systems into several categories:

1. Application plug-ins
2. Operating system plug-ins
3. Secure viewers
4. Server based terminal

When an application is designed, such that software can be installed as an add-on to take over functions on the application layer, EDRM rights are bounded to the *Application plug-in* and the related application. Adobe, Authentica and RMS are examples of such EDRM systems. This technique is considered as the weakest system of them all, because the plug-in receives all keys and is located on the insecure client environment. Reverse engineers should have enough power to reveal the decryption key and thus capture the content. In this way, another plug-in could be developed to capture keys by using a man in the middle attack. Next to this, data can be manipulated at the underlying levels such as the operating system. Adobe LiveCycle and Authentica suffer from these disadvantages.

Some approaches to EDRM involve patching the kernel of the operating system and are called *operating system plug-in*. In this way, all input/output calls are examined to see if they are on encrypted files, by using the kernel. The EDRM Controller checks the credentials of the user or device requesting the I/O before it grants approval. Microsoft RMS uses this mechanism and seems *more integrated with its client environment* compared to Adobe or Authentica. This implies that it should provide better security and could prevent reverse engineering. This technique does not ensure complete safety against attackers, but will make it a lot harder to hack the system. Till now, non hacking skills were able to access digital content by capturing the keys from users with no privileges.

A third approach involves creating a *secure viewer application* that can be used to render certain file formats and acts as its own EDRM Controller. This solution

has the same problems as the application plug-in and can be seen as vulnerable. Sometimes the secure viewer is translated as being an executable program with only the embedded functions as prescribed rights, but this does not secure digital content against print screens or analogue attacks. This technique is used by DOFS, when using offline access outside an organization. This part about DOFS can be seen as vulnerable. The only consolation for DOFS seems to be that other EDRM techniques offer a vulnerable solution for offline usage outside the organization as well.

Server based terminal is a used technique within the DOFS architecture. The client terminal forwards all actions performed by users on the server. Terminal sessions are used to forward actions to the encrypted content on the server and the actual bits never really leave the server. This is a solution, which is considered to be relative safe. Although it is the most secure solution to choose, the system does not provide *integration with other existing systems*. Scalability could be a problem as well, because all processes are performed by the server using terminal sessions at the client. Next to this, DOFS does not provide *search mechanisms* to support users to search for digital content and the producing company does not provide *updates in case of security breaches*. When implementing the system at an organization, the current infrastructure should probably be reorganized. Because all processes are performed by the server, the system suffers on a *single point of failure*. Next to this, the producing company does not provide solutions to *load balance* the server by using server clusters.

Furthermore, Authentica and Adobe have many similarities. Next to this, RMS and DOFS are the only tamper resistant systems, because Adobe and Authentica only secure digital content on an application layer. Other differences like dynamical rights and storage of rights in the digital container or on the server provide advantages and disadvantages. Because RMS stores the rights in the digital container, it is hard to limit rights for users after distribution of the documents. RMS seems to be a solution when Microsoft products are used on the server and clients. Next to this, RMS is the only EDRM system, which has the ability to secure XPS formats. For Adobe and Authentica it is necessary to save digital documents first before securing them. In this way, it is possible for users to create insecure digital documents. Adobe and Authentica both use server APIs for integration with in-house developed applications. RMS provides an API to create RMS compliant client applications. In this way, it should be possible to develop own applications, which secure digital content. The content management system of RMS is integrated more properly, because users have the ability to search through indexed digital documents. None of the described EDRM systems have the possibility for

partial asset protection. All EDRM systems use RSA communication keys and symmetric keys for document encryption. None of the EDRM systems offer personal backups. Watermarking is only for printed documents and PDFs, except for DOFS. Administrators should be trusted, because in practice they seem to have too many privileges. Next to this, watermarking seems to be necessary, because during the research project it was possible to create print screens by using virtual machines. Only DOFS does not seem to be scalable for large organizations.

The found results were gathered by using many literature resources. After testing the systems, all requested information could be found. Although the results are found by using the selection criteria model, it is always possible customers would like to know more properties about certain EDRM systems. In this way, it is necessary to keep the research results up-to-date, such that customer satisfaction could be guaranteed. The next step is to gather EDRM selection criteria by using Aia Software as a business case (Chapter 8). After evaluation of the founded results by comparing the business case results and the EDRM system properties, a final advice is provided to support Aia Software, Science and other organizations.

Chapter 8

Selection criteria Aia Software

In the previous chapters EDRM systems properties were gathered by using the selection criteria model and the related measurements (Chapter 5). These system properties are gathered by using literature, testing these EDRM systems and using contact persons from these EDRM producing companies. In another chapter, a selection criteria model was developed. This dynamical model is used on Aia Software to be able to develop EDRM specific selection criteria. The results from the applied model on Aia Software are gathered in this chapter. The objective during this phase is to gather business case specific criteria as a result from the selection criteria model and Aia Software. To be able to distill these selection criteria from Aia Software, it was necessary to answer several other research questions:

Which stakeholders can be used to gather the information?

After determining the stakeholders it was necessary to answer the following research question:

Which criteria can be used from these stakeholders?

8.1 Research Method

Stakeholders have another influence on the completeness of requirements [Som04]. Because stakeholders were not directly available for our system, only a few other resources could be used. To be able to generate input from Aia Software, interviews were held. Because real stakeholders are not available and this project had to be done within a certain time, only a few persons are used for inputs. Next to this, the actual knowledge about EDRM was not available within the organization. Two

directors of Aia Software are used as a first resource. Next to this, an interview with representatives of Microsoft and other employees are used as a second input at the organization. In this way, completeness of requirements is achieved by performing a literature analysis and these people to answer questions. In this way results are based on the gathered results from literature and input from the organization as described in the section about *Selection criteria model*. Per criterion a certain degree of importance is used to verify the value according to the organization. Each criterion from the selection criteria model consists of one or more questions, which are used during the interviews.

value	**semantics**
-1	Explicitly not mandatory
0	Not important
1	Nice to have
2	Mandatory

Table 8.1: Degree of importance

In the following sections the results according to Aia Software are described with the same structure as the model was built (section: Selection criteria model). By using the related questions from the model and assigning a degree of importance to the selection criteria, it was possible to determine Aia Software's selection criteria.

8.2 Functional selection criteria

Like the selection criteria model, the criteria are categorized as well into functional and non-functional criteria.

8.2.1 Content management criteria

This sub section describes the criteria for content management by Aia Software.

Content creation

Users should only create secure digital content. It is necessary to prevent users to create insecure digital content, because there would be risks from users to create insecure digital content which could be distributed to unauthorized persons. When creating digital content, it will go through several *phases*. The first phase contains *creation* of the digital content. During this phase the creator must provide the

importance (classified or not classified) of the digital content. When digital content is seen as important, other users must not be able to find the particular digital content by searching through a content deposit. When the digital content is less important, other users have the ability to search for digital content by using search features. The following figure describes the possible actions between the users. The essential part of the scenarios is to keep classified digital content secret from unauthorized users. EDRM systems must be able to disable users to create digital content without securing the content. Next to this, the system must provide above described life cycle per digital content (importance: 2).

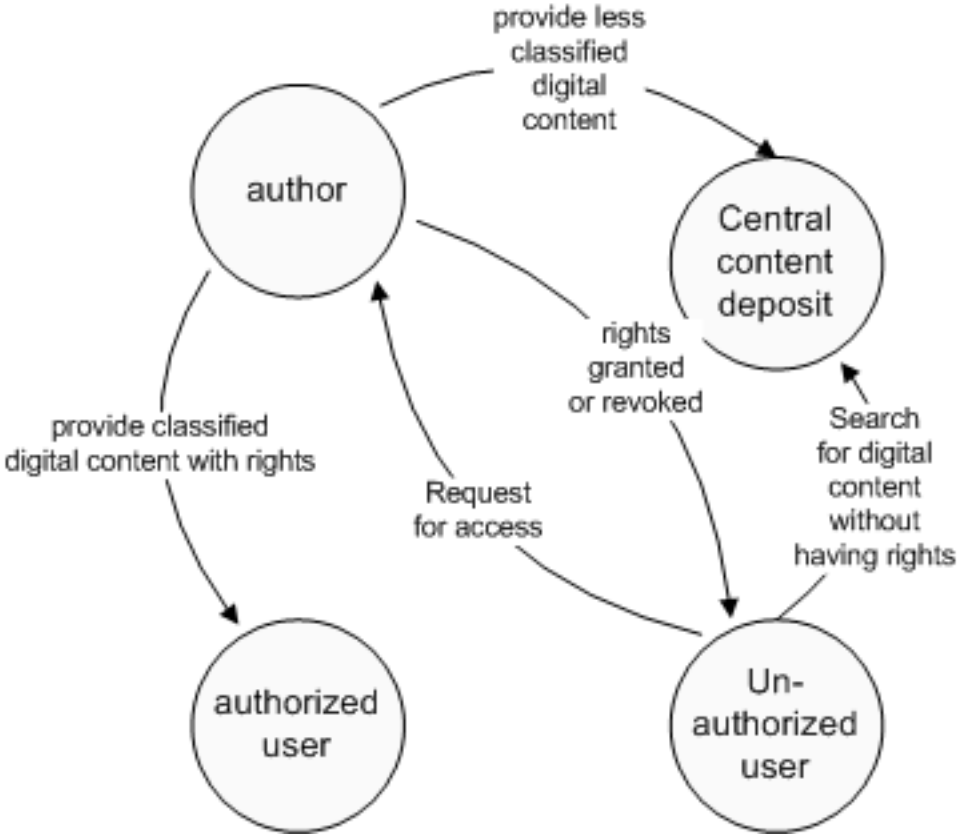

Figure 8.1: Content creation process

Content metadata

There is no necessary need to provide metadata with content. Metadata is used to provide search possibilities for users. When digital content is classified, it is not possible to search for this particular digital content by other authorized or unauthorized users. When digital content is not classified anymore, the author has

still the possibility to change content and provide it to be not classified anymore. Metadata in most EDRM systems contain title, description, date and author. In this business case it is not necessary to use metadata (importance: 0).

Uniquely identifiable content

Unique identification of digital content is very important. Each document must be prepared with a unique identifier, which enables it to assign to users. The risk that content can be accessed by unauthorized users must be prevented (importance: 2) [AH04, AH05b].

Distribution model

There is a need to give the EDRM system the ability to support different distribution models (e.g; push, pull, super-distribution). Aia Software wants to use a push strategy for classified information or a closed content deposit to be used by only certain authorized persons. In this way, a pull strategy like search mechanisms must not be used by unauthorized users to reveal the content. After digital content is not classified anymore, it is possible for users to reveal the content by using search features when these users are authorized. Super-distribution (distribution by users to other users) can be used, but unauthorized users must not be able to find and reveal the content. Only authors or users with full control have the ability to assign rights to other users. The push strategy can be used for *classified* digital content. Pull and or super-distribution can be used after the digital content is not classified anymore (importance: 2).

Searchability

There is need for users to search for digital content. Users can search through a deposit with secured digital content and possible linked metadata. As mentioned before, the initial user (author) has the ability to add the digital content to the central deposit or to remain it secret among other users. When the digital content should be public within the organization for search features (not access only search), the author can add it to the central deposit. As mentioned in figure 5. The availability for searchability and how users can search for digital content must be done according to the described protocol (importance: 2).

Partial asset protection

There is no essential need to give the system the ability to apply different usage rules/rights to parts of a larger content item. This feature is not essential and will not be taken into account when comparing EDRM systems (importance: 0).

User access to information about rights

Unauthorized users have the ability to search for digital content which is not classified. These unauthorized users have the ability to read information like title, author and description of the digital content. This supports users to be able to request for certain rights. Classified digital content can never be found by unauthorized users. It should not be possible for unauthorized users to reveal more information than title, author and description (importance: 2).

Personal backup

There is no need to provide personal backups per users. Backups will be done at the server without providing backup features for users. No measurement is necessary (importance: 0).

8.2.2 Tracking and control management criteria

This section provides the necessary properties, which are concerned with tracking and control management.

Logging content usage

Usage of digital content and rights should be monitored. Each action from the users must be recorded and stored on a content deposit in a controlled way. In this way, server logs can be gathered with all information about usage of digital content. Because EDRM provides restrictions to unauthorized users, it is necessary to log as much as possible. In this way, it is possible to log the actions on the digital content before it leaves an organization. When critical content has been leaked, the chance is larger to catch accessory employees. The EDRM system should be advanced with tracking and control mechanisms, such that each action is registered and digital content is marked with the user and its rights (importance: 2).

Watermarking

Watermarking should be applied to documents with related user identification. In this way, the content is related to a user and misusage can be detected. This also provides extra protection in case of print screens (importance: 2).

8.2.3 User management criteria

This section provides selection criteria for user management according to Aia Software.

User registration

Users of the EDRM system are divided into several roles. For administration of users within the organization, there is need to use administrators which have the ability to manage the users. Next to this, there are roles for a rights holder, recipient and rights transfer. A user becomes automatically rights holder when creating digital content. This user is able to assign all other users as a potential recipient with rights. These recipients have the ability to access digital content with prescribed rights. Another role is transferring rights. When users must not have access anymore, a user within the system must ensure to transfer the rights to another user. This role must be assigned to a user, without having risks for leaking information. Aia Software would like to split up these roles to several users, to avoid the risks of misusage. Roles as user management, rights holder, recipient and transferring rights must be divided among several users such that the risk of misusage is limited (importance: 2).

Scalability

Customers of Aia Software will probably not be very large. In future it is possible to acquire larger organizations (¿25.000 employees) as a customer. The scalability of the system could be measured by the average number of employees using the system per second. In this way, the system should not be offline, because employees would not be able to use the system. In case of larger organizations, the problem could be solved by using more parallel servers. The requirement for scalability requires it would be possible to use multiple server clusters. The server should be expandable with more parallel running servers to support scalability without losing inconsistence (importance: 2).

Unique identifiable users

Users need to be uniquely identified. It should not be possible for users to use each other's identities and reveal restricted content. Unique identifiable users are a requirements for each EDRM system to maintain its purpose (importance: 2).

8.2.4 Rights management criteria

This section describes the results from the selection criteria model for rights management according to Aia Software.

Rights per document and user

Users should be able to assign rights to other users of the system. The following rights should be available for users: view, edit, print, email, copy-and-paste. Next to this it is desired to secure digital content against screen captures (importance: 2).

Limited document usage

There is a need to give users the ability to restrict the usage of the content by various parameters by giving an expiration date. This is necessary to provide external partners the ability to use secured digital content from the organization. (importance: 2).

Rights transfer

There is need to give certain users within the EDRM system the role for transferring rights to other users. There is need to provide these functions to only trustworthy users, who will not abuse it. Next to this, it must not be possible to transfer rights to the person himself such that he or she can use it to distribute further. Next to this, the person who will leave the company cannot be trusted either. Another major issue contributes to unauthorized distribution as well: System administrators have the ability to change passwords and to log on to the system as another user. In this way, it is possible for them to give themselves these rights. This is a vulnerable part of the system, because these system administrators probably always have the possibility to decide which users could get the digital content. Because of this issue and the power of the system administrators, it would be most secure to give these users the rights for rights transferring. We can conclude it is very hard to develop a

secure EDRM system. EDRM systems will be judged on their way of working with transfer of rights and the user management as described in this section (importance: 2).

Dynamical rights

Dynamical rights involve resetting the rights for certain distributed digital content, no matter where it is located. When an employee leaves the organization, it should be possible to restrict the rights, before the user has the ability to distribute content to a competitor for example. It is necessary to use a role within the system, which allows it to transfer or change certain rights by performing tasks. Aia Software would like to apply this role to certain users within the system, such that illegal distribution is limited (importance: 2).

Rights templates

Rights templates are not necessary users should be able to determine which rights to assign (importance: 1).

Content versioning

Version control is not necessary (importance: 0).

Rights and protected content recovery

There is no explicit need for rights and protected content recovery (importance: 0).

8.3 Non-functional selection criteria

This section describes the non-functional security criteria provided by Aia Software. All other remaining non-functional requirements are gathered into the section *Other non-functional requirements*.

8.3.1 Security management criteria

The following security management criteria are gathered from Aia Software.

Key individualization

Key individualization is necessary for users, but the system must be able to search through content which is indexed on the content deposit. In this way, the EDRM system itself maintains a super-user key to index data. It should be necessary as well to keep this key save from other unauthorized users. It should not be possible for users to prevent to be someone else and in this way retrieve digital content on an unauthorized way (importance: 2).

Decryption keys non-disclosure

There is a need to give the EDRM system the ability to distribute decryption key(s) only to authenticated rights holders or devices. This is a necessary demand for key distribution. The EDRM system should be verified for using non-disclosure of decryption keys (importance: 2).

Renewability

It should be possible to provide updates by producing companies in case of security breaches (importance: 2).

Standard key management

There is nice to give the EDRM system the ability to use standard key management systems (for example PKI), but it is not necessary. As long as content is secure, it does not matter which kind of key management is used (importance: 1).

Tamper resistance

Most client software to secure digital content used by EDRM systems should be tamper-resistant. Only 100% security can be managed when the secured content will not reach the client side, because users can control their own client environment. To be able to give users access to digital content, it is almost inevitable not to transfer data to the client side. Aia Software wants users to take digital content with them, such that users can control data offline and outside the company. In this way, it is necessary to transfer data to the client, which is a relative insecure environment. EDRM systems should be able to support security while data remains on an insecure environment (importance: 2).

No single point of failure

Another security issue, which should be avoided, is *single point of failure*. EDRM systems can be very vulnerable when having single points of failure. Because employees need to produce documents and there is necessity to create only secure digital content, an offline EDRM system could be disastrous. EDRM systems should be equipped to limit single point of failures (importance: 2).

8.3.2 Other non-functional criteria

This section describes other non-functional criteria according to Aia Software.

Simple installation

An important requirement for the system to develop is concerned with simple installation. Because organizations already are equipped with certain infrastructure, complete reorganization should be avoided. Aia Software's clients use a Microsoft infrastructure and with active directory to maintain users. This current infrastructure should be supported. The EDRM system should work effectively with the Microsoft platform and active directory (importance: 2).

Maintainable

Users should be managed by using Active Directory and the server should be maintainable by administrators, such that risks are limited (importance: 2).

Portability - Platform shifting

This option gives the organization the flexibility to change platforms. It should be nice to work with other platforms as well such, but the only platform required is based on the windows platform. Other supporting environments are not necessary but nice to have (importance: 1).

Portability - Format shifting

Format shifting is not necessary, but nice to have (importance: 1).

Portability - Space shifting

Space shifting refers to the fact that people can use different types of devices to access digital content according to prescribed rights. Only the working environment is important, which implies different kinds of environments are not really important (importance: 1).

Portability - Time shifting

This feature facilitates users to access the digital content whenever the user wants to. Because it is impossible to provide security it is necessary for users to be online while saving digital content. Online and offline should be supported, but with a secure way of working. Offline usage outside the company is quite insecure, but nowadays many people work at home and should be provided (importance: 2).

Integration with existing applications

There is need to support Aia Software's ITP server. This server platform can be installed on a diversification of platforms. It is necessary to support communication and EDRM compatibility such that created office documents are secured by ITP. This server based solution creates digital content and should be secured by the EDRM system. In this way, there is need to communicate and receive digital content from the platform. Next to this, the EDRM system should work with other Microsoft Office digital content as Word, Excel, Powerpoint, XPS, PDF and Outlook to secure digital content as an output from these applications. These file types should be supported by user creation and security and ITP creation and security (importance: 2).

8.4 Conclusions

In this chapter, the developed *selection criteria model* from Chapter 5 is used on the business case Aia Software. Several people are used for inputs to create business specific criteria by answering business case questions from that model. The previous sub sections result into describing these criteria. The Director of Aia Software (Paul Dirven) answered all questions. During the research project a meeting with engineers from Microsoft was scheduled and discussions were held about certain mechanisms. Inputs from these discussions were used as well to develop specific requirements. Because it is not possible to interview real customer stakeholders, this method is used. The developed results can be used and altered when real customers

are available for Aia Software. This advantage would offer customer satisfaction and all experiences with these customers should be added to the model. In this way, an iterative process for developing an updated model and more specific requirements can be used in the future. Because questions were answered these must be compared to the properties from the EDRM systems. There is a risk that these answers are not gathered in the EDRM system properties. In that case, it would be necessary to do more research and gathering more information about the relevant subjects.

To be able to use these criteria, the results from the EDRM system properties (phase 5) per EDRM system were compared with the results from this chapter (phase 6) and are described in the following chapter as an evaluation (phase 7). All phases are used in the final Chapter to discuss Conclusions and Recommendations as an advice for related stakeholders.

Chapter 9

EDRM system evaluation

The goal of the research project is to compare EDRM systems and create an appropriate advice for Aia Software. In the previous chapters business case specific results are gathered from the selection criteria model. Next to this, EDRM systems are gathered with corresponding properties. In this chapter both results were used to compare the EDRM systems and to enlighten the similarities and differences. After this chapter, conclusions and recommendations are given by using this phase.

9.1 Research method

The set EDRM systems were compared according to the selection criteria of Aia Software. The resulting criteria from Aia Software where assigned to a *degree of importance*. The first step in this section is to gather all essential criteria from these Aia Software results. These criteria where marked with an importance of two as a result of the selection criteria model. In this section these *important* criteria are discussed per EDRM system. In this way, only the properties from the systems were used whereby Aia Software described them as being important. To be able to measure whether an EDRM system fulfils the criteria of Aia Software, another measurement is used. The following indicators are used per criteria on all described EDRM systems, by using the important *EDRM system properties*:

value	**semantics**
-1	The system does not fulfil the criterion
0	The system partially fulfils the criterion
1	The system does fulfil the criterion

Table 9.1: Criteria measurement

After summarizing these criteria, the chosen EDRM systems are discussed. In this way, it was possible to verify, which EDRM system fulfils the requirements of Aia Software. The following section describes the criteria and their measurement per EDRM system in a *detailed way* and uses the result to compare the EDRM systems per criteria for each EDRM system next to the Selection criteria from Aia Software.

9.2 Evaluation functional properties

In this section, the functional properties per category are described for all EDRM systems and degrees are given if they fulfill the requirements from Aia Software.

9.2.1 Content management

This sub section describes the evaluation about content management.

Content creation

Content creation is concerned with in what way users have the ability to create content.

Microsoft
Only authorized users are able to access digital content. During the research project, the system was tested when creating digital content. The local client was observed with tracking tools and leakage was not discovered. Created content was directly encrypted by using its application layer and underlying operating system. For Aia Software, there is need to prevent users to create insecure digital content. Microsoft Word can be advanced by preventing users to save digital content on a normal way, but by manually renaming a text file into a MS Word document and opening it in MS Word, we can conclude it is very hard and probably impossible to prevent users from creating insecure digital content (unless users cannot write to hard disks or other media). Creation of secure digital content is in this way almost impossible to request from a client system, unless people cannot create digital content on the client system on any other way. During this investigation, content creation is judged by creation of content by the client software. It seems impossible to request from a system, that users must not create insecure content. RMS can be combined with a content management system called SharePoint to distribute digital content among other users. When the content is not distributed to the SharePoint system, the author has the ability to distribute it manually to a few other users in case

of classified information. In this way, digital content cannot be searched for and only the necessary users have the ability to access digital content according to the prescribed rights. The content is created locally and the policies are described inside the secured container. When it is possible to secure the client systems from creating contents in other ways besides the EDRM compliant applications, it is possible to only create digital content (evaluation: 1 point).

DOFS

When using DOFS, all content is created directly on the server in a secure way. The digital content is provided with rights to assigned users. In this way, other users have the ability to use their rights on the same way via a terminal session. When created content is classified, it should only be available for the authorized persons. Although the server uses file sharing mechanism, there is not really a database which can be used by users to search through data. Creation of secure content can be forced, because all data is stored on the server (evaluation: 1 points).

Authentica

Content creation can be done by users with the office clients as Aia Software requires. Authentica delivers a plug-in, which can easily be installed on the client. This plug-in software is used as the EDRM controller and renders the content according to prescribed rights. Authors are required to create and save digital content locally and secure it by using the EDRM controller. In this way, it is always necessary for users to safe their contents first before encrypting. In this way, it is possible for authors to keep copies of the initial content. This is not desired at Aia Software, because this could (unintentionally) lead to leakage of critical information in the first phase. If there cannot be created a temporary insecure content file, the plug-in cannot secure it (evaluation: 0 points).

Adobe

Like Authentica, this plug-in needs to save the digital content first on a temporary location before encrypting it. Adobe introduced Document Center, a web-based service that will allow business users to safeguard, share and trace the usage of Adobe PDF, Microsoft Office documents. In this way, the content can be looked up at the document center only by authenticated users. This is against the requirements of Aia Software, because there is need for users not being able to create insecure content (evaluation: 0 points).

Uniquely identifiable content

All content should be uniquely identified by the EDRM system.

Microsoft

All created digital content is unique and prescribed with users and assigned rights

by XrML. Encryption and hashing techniques are used to create a unique content id. XrML is a standard to describe rights combined with a user and condition bound to content. In this way, users have the ability to create the same document with different policies, because the policies of users are not stored on the server, but only the keys. When a user tries to access digital content, the RMS licensing services on the RMS cluster issues a unique use license that reads, interprets, and applies the usage rights and conditions specified in the publishing licenses. In this way, each content file contains its own particular rights with assigned users (evaluation: 1 points).

DOFS

Created digital content is created in a unique way and protected with rights assigned to users. This information is secured with the digital content and remains on the server. After authentication, the user terminal displays the application and forces the prescribed rights on the server via this terminal session. All content is stored at the server on a unique way (evaluation: 1 point).

Authentica

All created digital content is uniquely identified and all policies are stored on the server. The system uses a hash function (SHA) to create a unique id of digital content. Because the policies of all users to assigned content is stored separately from the file itself, it is necessary to identify each file to be able to assign the correct rights with the correct user and thus the encryption key. Fingerprint technology is used on the content to create a unique id (evaluation: 1 points) [RD03, Aut05b].

Adobe

The plug-in creates a unique id from the secured digital content and stores it in a data file locally and secured where only the plug-in can use it to authenticate the digital content to the Policy server. Hash technology is used (like Authentica) about digital contents to verify a unique number of the document. As long as the client plug-in remains safe, the content stays uniquely identifiable (evaluation: 1 point) [Ado07e].

Distribution model

For distribution, users have the ability to encrypt digital content and distribute it manually or use the content management system which offers other users to search for (full text search). In this way, classified information should remain safe and does not exist for unauthorized users.

Microsoft

Users can create digital content by using client software. After creation of classified information, it can be distributed among all users who need it. SharePoint can be

used to share digital content with other users. In this way, the author could create a group with only users who have the ability to access the content. Other users should not be authorized to use the SharePoint system, which is easily possible (evaluation: 1 point).

DOFS

All content remains on the server and authorized user can be assigned with certain rights. All other users don't have the ability to access the digital content. Users have the ability to email other users an encrypted package, which contains a location on the server. After another user receives the digital content, it is decrypted (when authorized) and this user has the ability to access the digital content via a terminal session. In this way, digital content could not be distributed to unauthorized users (evaluation: 1 point).

Authentica

The distribution can be done by manual sending it to authorized users or by using the Content management such as Documentum, IBM Content Manager or Hummingbird Enterprise. Although SharePoint will work with the EDRM architecture, it does not include a full integration with rights management. The system provides an additional right as embargo date, which could be used to provide classified digital content readability after a certain period (when it is not classified anymore). The distribution model in this way fulfils the requirements from Aia Software (evaluation: 1 point).

Adobe

The distribution model is managed the same as for RMS and all distribution strategies can be used to distribute documents. Adobe developed an own web based application called Document Center to share digital content (evaluation: 1 point).

Searchability

Searchability is necessary to provide authorized users certain digital content.

Microsoft

Digital content can be distributed by using SharePoint. In this case, one content version is used at SharePoint and users have the ability to search through the digital content. When unauthorized users want to access it, they need to ask for permission from the author. In this way, users could create multiple SharePoint environments with users who are authorized to access the content. The SharePoint uses a super user-key which enables users to search through digital content, but offers no further access to the digital content. Because SharePoint can be used as often as users want, it is always possible to create multiple groups with different users (evaluation: 1 point).

DOFS
Users have the ability to browse for digital content, but cannot use full text search mechanisms to find digital content. There aren't search facilities available in DOFS (evaluation: 0 points).

Authentica
Searchability is possible by using Documentum, IBM Content Manager or Hummingbird Enterprise. In this way, it is possible to share digital content among authorized users (evaluation: 1 point).

Adobe
Searchability can be done by using the document center. Just like with Authentica and RMS it is possible to use it to share contents within multiple groups (evaluation: 1 point) [Ado07e].

User access to information about rights

Even when users are not authorized, it is necessary to reveal certain information.

Microsoft
A user who is not allowed to access digital content can retrieve information about the author, who could be contacted for rights approval (evaluation: 1 point) [Mic06d].

DOFS
When a user tries to access digital content without access, information can be received about the author as well with the DOFS system. In this way, the author can be requested for permissions (evaluation: 1 point).

Authentica
The system reveals the identity to unauthorized users when access is denied. In this way it is possible to request rights by contacting the author (evaluation: 1 point).

Adobe
Users have the ability to review the metadata from any secured digital content. In this way, rights can be requested by contacting the author of certain digital content (evaluation: 1 point).

9.2.2 Tracking and control management

This sub section describes the evaluation about tracking and control management.

Logging content usage

Logging content usage is one of the important tracking and control facilities.

Microsoft
When creating digital content, a user needs to authenticate to the RMS server to request a certain key. Each time contact is made with the server and logs are made about who enters which content file (evaluation: 1 point).

DOFS
Because all events happen on the server, all actions from users are tracked and logged (evaluation: 1 point).

Authentica
All keys and policies are gathered on a central server. In this way, the user must contact the server to authenticate and receive the key. Each action from a user is tracked and recorded by the server (evaluation: 1 points).

Adobe
All actions with digital content are stored by the Adobe LiveCycle and Document Center, because all data besides the content itself is stored on the server (evaluation: 1 point).

Watermarking

Watermarking can be used to reveal distributers to unauthorized users.

Microsoft
It is only possible to use watermarking when printing documents, but programmatically it could be possible to foresee digital content of watermarking techniques (evaluation: 0 points).

DOFS
The system offers a watermarking technique at the terminal session. In this way, illegal captured images (e.g. via analogue attacks) can be traced as well (evaluation: 1 point).

Authentica
Watermarking can only be provided on PDF files or printed office documents (evaluation: 0 points).

Adobe
Watermarking can only be provided on PDF files or printed office documents (evaluation: 0 points).

9.2.3 User management

This sub section describes the evaluation about user management.

User registration

User registration is important, because it should not be possible for users, who don't have privileges to access digital content.

Microsoft
For user registration the active directory should be used at organizations according to Aia Software. The demand from Aia Software is that the system should not allow super-users to capture content that they wish for. Active directory can be used by system engineers to create and delete accounts. In this way it is possible for an engineer to change the account of a user to be able to capture rights about certain digital content. In this way, it is almost impossible to create a completely safe protocol unless you can trust certain employees. Next to this, it is possible to create a super-user, which has the possibility to access all digital content. In this way it is necessary to keep classified digital content only among the necessary users. This is possible, because it is not necessary to share secured digital content in a central deposit and all rights and privileges are secured in the digital content. When classified digital content is only distributed to authorized users, it is possible to keep the digital content secure (evaluation: 0 point).

DOFS
For user registration the active directory mechanism can be used as well. In this way, the same problems occur with domain administrators like the RMS system. These domain administrators have possibilities to authenticate as another user. In this way, they have the possibility to capture copying rights and to create a new insecure file on the server. In this way, it should not be very hard to capture the insecure digital content (evaluation: 0 point).

Authentica
The same problem occurs as described for other EDRM systems. Because Active Directory provides certain privileges to domain administrators, it is always possible to capture digital content by these users. The difference with RMS provides system administrators another feature. All usage is logged and can be captured by these system administrators. Next to this, rights can be captured because these are located on the server. When these administrators manage to steal the digital content, they always have the possibility to access the content. In this way, it should be necessary to split up administration for Active Directory and the Policy server. This should lower the risk, but when an active directory administrator reveals who has full

control about certain content, it is possible to change credentials and capture the content by its author rights (evaluation: 0 points).

Adobe

Adobe LiveCycle uses an administrator, which can be used to change policies on digital content and next to the domain administrator, these administrators have many privileges. As the same for other EDRM systems, illegal usage by these administrators is possible (evaluation: 0 points).

Unique identifiable users

Users should be uniquely identifiable.

Microsoft

Authentication of users is done by Active Directory or .NET passport mechanisms. For certificate usage and server/client verification, Microsoft as a certificate authority is used as a trusted party and organizations can use this Certificate Authority to identify their own RMS server as a trusted party. The RMS server receives a signed certificate which allows it to issue licenses. In this situation the local RMS server is trusted and can be used to trust other servers and clients. All clients must be trusted first before they can participate within the network. Clients must be activated before participation as well by using client software, which creates a unique certificate per system. In this way, the client system contains a unique identifier and can be used by authorized users to secure and receive digital content. It contains a public key of the device (client as a system), which can be used by an authorized user. The first time a user uses an authenticated device, the server uses a private key (RSA) to communicate with the client. The combination of the device its public key and the private key enables the user to encrypt the symmetric key for the encrypted digital content. XrML certificates are used to specify the rights and are forced by client controllers. The RMS server uses important services for the process: certificate and licensing service. The certificate service issues trusted servers and clients and the licensing service is used to provide rights or use rights by users (evaluation: 1 point).

DOFS

Users are identified in a unique way by active directory or other secure authentication mechanisms. After authentication by using the terminal software all actions are forwarded to the server (evaluation: 1 point).

Authentica

Users are uniquely identified by the active directory server. Other authentication possibilities can be implemented easily as with other EDRM systems. Authentica offers an online authentication mechanism as well (evaluation: 1 point).

Adobe
All users are uniquely identified by using Active Directory as requested by Aia Software. Furthermore, LiveCycle Security Services (online authentication protocol) can be used to authenticate users as well (evaluation: 1 point).

Scalability

Systems should be scalable regardless the growth of the organization.

Microsoft
RMS can be expanded by creating clusters of servers, which ensures an adjustable scalability. Processes like encryption are the most consuming mechanisms of the system, but are taken place at the client. According to Microsoft, scalability is not an issue. Microsoft developed a document with instructions to support server clusters (evaluation: 1 point).

DOFS
Because the most events are processed by the server, the server must be load balanced with multiple servers. Each organization should be calculated first before providing the system. In this way, the scalability risk can be limited. Because of the high impact on the servers, it is not recommended to use the system with many users. Next to this, the producing organization does not provide a load balance plan (evaluation: 0 points).

Authentica
Scalability is maintained in the same way as with other EDRM systems and can be scaled. Authentica recommends clustering of servers as well, which should balance the workload. The server stores all keys and privileges and has more workload compared with MS RMS, but this will not be a problem when adding more servers to the cluster (evaluation: 1 point).

Adobe
Scalability should be no problem, because servers can be clustered to balance load. Adobe developed a cluster plan as well (evaluation: 1 point).

9.2.4 Rights management

This sub section describes the evaluation about user management.

Rights per digital content and user

Rights like view, edit, print and copy-paste with expiration date are recommended to be provided.

Microsoft
EDRM systems offer techniques to assign rights to users and digital content. The following rights: view, edit, print, email, copy-and-paste, screen capture and expiration can be used with RMS. RMS supports all rights for recipients when securing digital content which are requested (evaluation: 1 point).

DOFS
Rights like read, copy-paste, write, email, copy and expiration are available for authors to assign to users (evaluation: 1 point).

Authentica
Like other EDRM systems, it is possible to assign the requested rights to digital content. As mentioned before these rights are directly stored on the policy server per digital content and assigned user. The rights required by Aia Software can be used by authors when using Authentica. Authentica even provides embargo dates for classified content (evaluation: 1 point).

Adobe
There are several different kinds of rights possible to use on digital content like full rights, read, print, copy, transfer rights, expire dates (evaluation: 1 point).

Limited document usage

Limited document usage can be used to restrict rights to users.

Microsoft
It is possible for authors to set an expiration time to digital content as a condition. Next to this, it is not possible to specify an embargo date and time combination, but this was not requested by Aia Software. Users need to go online to verify authentication and in this way expiration dates can be compared (evaluation: 1 point).

DOFS
Authors have the ability to use expirations on digital content. Because the client users can never reset the system time on the server, these are secure as well (evaluation: 1 point).

Authentica
The policies concerning digital content can as well be advanced by conditions. These conditions e.g. expiration date or embargo date can be used to expand rights with

extra conditions. Next to this it is possible to use policy templates, which can be used on a group level within organizations. This helps organizations to prescribed usage of rights for authors within defined groups (evaluation: 1 point).

Adobe

The policies concerning digital content can as well be advanced by conditions. These conditions e.g. expiration date or embargo date can be used to expand standard rights. Next to this it is possible to use policy templates, which can be used on group level within organizations. This helps organizations to prescribed usage of rights for authors within defined groups (evaluation: 1 point).

Transferring rights

When users leave the company or a certain project, it is recommended to transfer rights from one person to another.

Microsoft

When an author creates digital content, this user is defined as the author with full rights. This user has the ability to assign other users the available rights. Because the rights are stored in the digital container, each copy could contain several rights. When a user wants to have more rights, he could contact the author and the author could prescribe more rights by sending a web link (URL) or a new copy. Another possibility is to contact a system administrator. The system administrator has the ability to add conditions to a revocation list. In this way, privileges can be restricted when authenticating. The disadvantage of this system is that a system administrator must be contacted and the administrator must be able to now the XrML language to enforce rights by using a computer language. This is not very convenient and is a disadvantage for encrypting the rights per document. The rights are not stored on a central database like with other EDRM systems, which is a major disadvantage (evaluation: 0 points).

DOFS

There are possibilities for the users to transfer rights to other users. In this way, domain administrators have the ability as well to transfer rights (evaluation: 1 point).

Authentica

Because the rights per digital content are stored on the central policy server, it is possible to transfer rights on a central way. It doesn't matter how many copies are distributed among users, because all users must authenticate themselves at the policy server before accessing digital content to receive the keys and rights (evaluation: 1 point).

Adobe
Because the rights per digital content are stored on the central LiveCycle server, it is possible to transfer rights on a central way by users or administrators (evaluation: 1 point).

Dynamical rights

Dynamical assignments of rights provide authors to reassign prescribed rights. This would be necessary to revoke rights.

Microsoft
Like discussed at *transfer of rights*, it is not possible for users to dynamically change the rights. Authors have the ability to assign other users with certain rights. Because the rights are stored in the digital container itself, each copy could contain several rights. When a user wants to have more rights, he could contact the author and the author could prescribe more rights by sending a web link (URL) or a new document copy. Another possibility is to contact a system administrator. The system administrator has the ability to add conditions to a revocation list. In this way, privileges can be restricted when authenticating. The disadvantage of this system is that a system administrator must be contacted and the administrator must be able to now the XrML language to enforce rights by using a computer language. This is not very convenient and is a disadvantage for encrypting the rights per document. The rights are not stored on a central database like with other EDRM systems, which is a major disadvantage (evaluation: 0 points).

DOFS
Users or administrators have the possibility to change rights dynamically, because all rights are stored on the server (evaluation: 1 points).

Authentica
Users or administrators have the possibility to change rights dynamically, because all rights are stored on the server (evaluation: 1 points).

Adobe
Users or administrators have the possibility to change rights dynamically, because all rights are stored on the server (evaluation: 1 points).

9.3 Evaluation non-functional properties

In this section, the non-functional properties per category are described.

9.3.1 Security management

This sub section describes the evaluation of security management.

Key individualization

Encryption keys should be individualized. In this way, it is necessary to create unique keys for content items.

Microsoft
All digital documents are secured by symmetric key encryption. This symmetric key is furthermore secured by PKI encryption provided by a RSA 1024 bits key mechanism. Encryption is done at the client by using the private RSA key, which is received when authenticated. The rights are assigned to the users and the content and each user receives an appropriate key per digital content according to the prescribed rights by the author. All rights are gathered into two licenses. The first issuance license is used by the author. The author defines the rights and users and sends it to the RMS server. The RMS server sends a signed issuance license back. This signed license is bounded to the encrypted document and distributed among users. When a user wants to read the document, the signed license is sent to the RMS server. After authorization the RMS server sends an end user license back with granted rights. These rights are used by the application next to the received decryption key (evaluation: 1 point).

DOFS
On the server, digital documents are secured by symmetric keys. Both remain on the server and users are identified by using the terminal session. The pointer files which are encrypted and used for email purposes don't have to remain on the server, because the real content is not inside this encrypted file. After a user wants to access digital content, the server verifies the rights from a database. After authorization, the server uses the rights inside the applications. During the session a decryption key is used per particular document. Next to this, less encryption mechanisms are necessary, because data and keys remain on the server. When a document is altered and closed, the same key is used for encrypting the document again (evaluation: 1 point).

Authentica
Each user which is authenticated by for example Active Directory uses a temporary session key to communicate with the policy server by Secure Socket Layer (SSL). The content contains a unique identification and is received from the server next to the symmetric encryption/decryption key. The EDRM controller (client plug-in) uses these credentials to render the content. In this way, key individualization is handled

per session for authentication and for encryption of digital content (evaluation: 1 point).

Adobe
Each user can be authenticated by Active Directory and uses a temporary session key to communicate with the policy server by using Secure Socket Layer (SSL). The content contains a unique identification by using hashing techniques and is received from the server next to the symmetric encryption/decryption key (AES). The EDRM controller (client plug-in) uses these credentials to render the content. In this way, key individualization is handled per session for authentication and for encryption of digital content (evaluation: 1 point).

Decryption keys non-disclosure

Decryption keys should not be disclosed to unauthorized users.

Microsoft
The symmetric encryption keys remain safe per digital content and are used to encrypt and decrypt the digital content. The private RSA keys are sent via a secured http protocol after authentication and cannot be captured during transfers, because of SSL support. The only way to capture the key is to perform reverse engineering techniques. Because the symmetric key must be stored at the client software, it should theoretically be possible to reverse engineer the client software and capture the decryption key. In this way, the client software is relative safe but 100% safety cannot be guaranteed. Because RMS is integrated in the underlying operating system, the mechanism is the safest way by using keys and the encrypted content at a relative insecure environment (evaluation: 1 points).

DOFS
Non-disclosure of decryption keys is maintained and is never transferred to the client side (evaluation: 1 point).

Authentica
The symmetric decryption/encryption key is transferred by a SSL communication protocol secured by an asymmetric session key. The decryption key remains secure as long as the plug-in is safe. This plug-in is less integrated with its applications and concerns more risks. Compared to RMS this plug-in only operates on the application layer. All underlying layers could be used to capture information. Because reverse engineering practices can result into revealing the decryption key, non-disclosure of decryption keys cannot be completely met (evaluation: 0 points)

Adobe
The symmetric decryption/encryption key is transferred by a SSL communication protocol secured by an asymmetric session key (RSA 512 - 2048 bits key space).

The decryption key remains secure as long as the plug-in is safe. This plug-in is less integrated with its applications and concerns more risks just like Authentica. Compared to RMS this plug-in only operates on the application layer. All underlying layers could be used to capture information. Because reverse engineering practices can result into achievement of the decryption key, disclosure of decryption keys cannot be completely met (evaluation: 0 points).

Renewability

Renewability concerns the possibility for providing updates in case of security breaches.

Microsoft
Microsoft offers windows updates to install updates to prevent or repair new security issues. When a critical update is available, it is necessary to update first before content can be accessed (evaluation: 1 point).

DOFS
DOFS does not provide an update mechanism. Although Microsoft components are used, there isn't information available about security breaches (evaluation: 0 points).

Authentica
Authentica offers online updates to install new security issues. When a critical update is available, it is necessary to update first before content can be accessed or secured (evaluation: 1 point).

Adobe
Adobe offers online updates as well to install new security issues. When a critical update is available, it is necessary to update first before content can be accessed or secured (evaluation: 1 point).

Tamper resistance

Tamper-resistance is important to protect content at the client EDRM controller.

Microsoft
The client receives a combination of a signed issuance license and encrypted document from the author. The receiver sends the signed license to the RMS server. The server verifies the authorization and sends a user license to the client with related rights next to the decryption key. During the research project the system was tested when securing content. It was not possible to capture the data with tracking tools, because the client encrypts the data directly into a secured document. Next to this, macros were used to created backups of the secured digital content, but it was im-

possible during the project to create an insecure file in an illegal way. According to literature it should be possible in theory by using reverse engineering practices to capture the original content, but practice was not done during the research project. Next to this, RMS uses kernel interaction to verify inputs and outputs with the digital content. In this way, it is hard to reverse engineer the applications, because of integration with the operating system and application layers (evaluation: 1 point).

DOFS

There could be multiple possible attacks on the client, but none of them should result in receiving the actual bits of the digital content. Inside attackers could try to bypass the client control for example, but this could only result into losing the connection with the server. Attackers could also try to infiltrate Trojan horses, but usage of firewalls and virus scanners should limit these risks. Because no bits actually leave the server, it is not possible to capture information by using the terminal sessions and remains secure in comparisons with other client software (evaluation: 1 point).

Authentica

The plug-in is deployed on the application level of the system. This level is not explicitly safe against reverse engineering. After reverse engineering practices it is possible to develop another plug-in, which can be installed on clients to capture the symmetric encryption/decryption key. Therefore this system is not fully tamper-resistant (evaluation: 0 points).

Adobe

The plug-in is deployed on the application level of the system as well. This level is not explicitly safe against reverse engineering. After reverse engineering practices it is possible to develop another plug-in, which can be installed on clients to capture the symmetric encryption/decryption key. Therefore this system is not tamper-resistant (evaluation: 0 points).

No single point of failure

Single points of failures should not be allowed, because the system produces important documents. When organizations cannot create these documents because of failure of the EDRM system, continuity of the organization will be in danger.

Microsoft

The RMS server seems to be a single point of failure, because it should be online when creating or consuming digital content. The Active Directory is in this way a single point of failure, since it is used for authenticating users. The RMS server needs to secure the keys in a configuration database, which is always required for encryption or decryption of digital content. The RMS server uses a cached version of the active directory, which ensures to provide services when the active directory

server is temporarily offline. Microsoft acknowledges these single points of failures and recommends to use clusters of severs to balance load the traffic. Next to this, it is necessary to use backup mechanisms to create backups of all data like Active Directory, licensing service, certificate service and databases. When the active directory is corrupt and none backups were made, all digital content could be lost. This assures an organization to recover backups when the system is down, clusters can be used directly to substitute down services. In this way, single points of failure can be taken away. Microsoft developed a document for scaling disasters and recovery plans. It seems that problems can be reduced to the minimum and there does not have to be a single point of failure (evaluation: 1 point).

DOFS
The DOFS server is certainly a single point of failure and therefore clusters of load balancing servers and backup servers should be used to reduce the limit, but when the server remains down users cannot do anything. The producing organization of the mechanism does not provide backup and load balancing documents (evaluation: 0 points).

Authentica
The policy could become a major single point of failure as well. Documentation is provided by Authentica for clustering servers to achieve balance loads, provide backups and keep services online (evaluation: 1 points).

Adobe
The policy could become a major single point of failure as well. Documentation is provided by Authentica for clustering servers to achieve balance loads, provide backups and keep services online (evaluation: 1 point).

9.3.2 Other non-functional properties

This sub section describes the evaluation about other non-functional properties.

Simple installation

To integrate EDRM with current information technology infrastructure, it should be relative easy to upgrade the current platforms.

Microsoft
The RMS system can be implemented very easy by using RMS service packs on windows clients and windows servers. Databases can be created automatically and used by MS SQL server. SharePoint can be installed easily and used for defining groups and sharing digital contents on a very easy way by users. Administrators

need to enroll the servers and clients, but when the Microsoft platform is used, this all should not be a problem (evaluation: 1 point).

DOFS

The implementation for DOFS could become quit complex when more users use the system. Most organizations use normal client-server installations and not terminal sessions. In this way all servers and clients need to be restructured and therefore installation becomes quite complex in comparison with other EDRM systems (evaluation: 0 points).

Authentica

The implementation of Authentica is simple as well. The client plug-in is compliant with all office versions and can be used on all operating systems. Active Directory can be used for authentication and the policy server can be installed by following installation manuals (evaluation: 1 point).

Adobe

The implementation of Adobe is easy as well. The plug-in is compliant with all office versions. Active Directory can be used for authentication and the policy server can be installed by following installation manuals (evaluation: 1 point).

Time shifting

It should be possible to use secured digital content online and offline, inside and outside the organization.

Microsoft

It is possible to create and read digital content from outside an organization. RMS uses Active Directory or the .NET passport to verify users and their privileges. Active Directory at other organizations (e.g. partners) can be used and connected to provide support at these locations. Outside an organization it is possible to use the .NET passport mechanism when internet is available. Next to this, it is possible as well to use offline usage on a trusted (enrolled) client. A user has the possibility to use the trusted laptop at home. In this way, the user uses offline usage and the system downloads the requested keys. Next to this, the expiration date is set and the user has the ability to access the document for a certain period. The system uses a micro safe with a time tampering mechanism. When the user tries to manipulate the system time or something related, the client will not allow any more access, till the user goes online to verify authorization (evaluation: 1 point).

DOFS

DOFS uses terminal sessions and these can be used remotely as well. Next to this, it is possible to work offline too. The server creates an executable file with prescribed rights. In this way, the actual bits of the digital content will leave the

server. This mechanism is not really safe, but offers at least the possibility to work offline. It is also possible to disable the function, such that the feature is disabled. Administrators have the ability to activate this feature (evaluation: 1 point).

Authentica

Offline usage is possible and the necessary keys are stored on the local client system (which is not 100% safe), where the client plug-in can use it. A certain expiration time is used when accessing digital documents and the user must go online within a certain period to verify whether the policies are still valid. Online access can be done by using the online security service or LDAP and Active Directory authentication (evaluation: 1 point).

Adobe

Offline usage is possible and the necessary keys are stored on the local client system, where the client plug-in can use it. There is need to use a certain expire time for accessing and the user must go online within a certain period to verify whether the policies are still valid. Online access can be done by using the online security service or LDAP and Active Directory authentication (evaluation: 1 point) [Ado07c, Ado07d].

Integration with existing applications

Aia Software developed ITP, which produces digital content. There is need to secure digital content by ITP.

Microsoft

There is a Windows Rights Management SDK available at Microsoft, which enables software developers to add RMS functionality to other applications. Many organizations that create digital content use applications that were not developed by Microsoft. The availability of the RMS SDK enables a more comprehensive solution. For the recipients of rights-protected information who do not have access to RMS-enabled programs, a trusted RMS-enabled browser, the Rights Management Add-on (RMA) for Microsoft Internet Explorer, is available too. Software engineers are able to use API's to make an application RMS compliant. Next to this, SOAP can be used for interaction with RMS servers to retrieve keys and other necessary data. In this way all kinds of applications can be made RMS compliant to support EDRM at the client side. SDK are available with detailed documentation (evaluation: 1 point).

DOFS

It is possible to connect with the DOFS server and use existing applications on other servers to secure digital content in theory, but in practice there are none working examples available. There are none SDK's available to make existing applications

DOFS compliant and therefore this mechanism is not usable for Aia Software (evaluation: 0 points).

Authentica

There is need to support Aia Software's ITP server. All Microsoft operating systems are supported and a server-side SDK can be used to communicate with the server and secure digital content. Windows NT Server 4.0, Windows 2000 Server, Windows Advanced Server, Windows Server 2003, and Sun Solaris 2.8 and 2.9 are the supported operating systems as a server (evaluation: 1 point).

Adobe

All Microsoft operating systems are supported and server-side SDK by using .NET or Java API's can be used by developers to create secure digital content (evaluation: 1 point).

9.4 Overview results

The following figure 9.2 describes an overview of all criteria, the important ones and the assigned values in which way they fulfill the requirements. All important criteria where marked and the related values whether EDRM systems support the requirement are marked as well. The first column describes the criteria. The second column (i) describes the importance provided by Aia Software. The third column describes a 1 when RMS does fulfill the criteria and a 0 when it does not. The fourth, fifth and sixth column describe whether DOFS, Authentica or Adobe fulfill the criteria. According to the model, RMS receives 18 point, DOFS 15 points, Authentica and Adobe 17 points.

This part of the table describes the results of Content management.

Criteria	**i**	**RMS**	**DOFS**	**Authentica**	**Adobe**
Content	-	-	-	-	-
Content creation	2	1	1	0	0
Content metadata	0	-	-	-	-
Uniquely identifiable content	2	1	1	1	1
Distribution model	2	1	1	1	1
Searchability	2	1	0	1	1
Partial asset protection	0	-	-	-	-
User access to information about rights	2	1	1	1	1
Personal backup	0	-	-	-	-

This part of the table describes the results of Tracking and control manage-

ment, user management, rights management, security management and other non-functional properties.

Criteria	**i**	**RMS**	**DOFS**	**Authentica**	**Adobe**
Tracking and control	-	-	-	-	-
Logging content usage	2	1	1	1	1
Watermarking	2	0	1	0	0
Rights and protected content recovery	0	-	-	-	-
User	-	-	-	-	-
User registration	2	0	0	0	0
Uniquely identifiable users	2	1	1	1	1
Scalability	2	1	0	1	1
Rights	-	-	-	-	-
Rights per document and user	2	1	1	1	1
Limited document usage	2	1	1	1	1
Rights transfer	2	0	1	1	1
Dynamical rights	2	0	1	1	1
Rights templates	1	-	-	-	-
Usage rules	0	-	-	-	-
Content versioning	0	-	-	-	-
Security	-	-	-	-	-
Key individualization	2	1	1	1	1
Decryption keys disclosure	2	1	1	0	0
Renewability	2	1	0	1	1
Standard key management	1	-	-	-	-
Tamper-resistance	2	1	1	0	0
No single point of failure	2	1	0	1	1
Other non-functional	-	-	-	-	-
Simple installation	2	1	0	1	1
Portability - Platform shifting	1	-	-	-	-
Portability - Format shifting	1	-	-	-	-
Portability - Space shifting	1	-	-	-	-
Portability - Time shifting	2	1	1	1	1
Integration with existing applications	2	1	0	1	1

Table 9.2: Results selection criteria model Aia Software

9.5 Conclusions

In this chapter the results from the Selection Criteria Model according to Aia Software and the results from the EDRM systems and their properties are compared by using only the important criteria according to Aia Software. In this way, the detailed differences between the EDRM systems according to the requirements of Aia Software are described. The influence of real customer stakeholders could provide other results. In this way, Aia Software must use inputs from real potential customers to create a correct advice. Now only the results of a few people from Aia Software are used to create a measurement and could be different from the wishes of real customer organizations. When using questions on real customers, probably other answers will be given and could eventually influence the measurement. Next to this, updates on EDRM systems by EDRM producing companies could change the results as well. The previous section gives an overview of all related factors. According to this research project, there are several differences between the systems. The overview shows RMS to be the most appropriate solution for Aia Software by using current inputs. Whether this is the case is discussed in the following chapter where all these results are used as an input to create a consult for Aia Software.

Chapter 10

Conclusions and recommendations

This chapter describes the important conclusions and recommendations which were found during the research project. The goal of this research project is to create an advice according to the technical requirements of Aia Software. Therefore first the implications for Aia Software are given as conclusions and related recommendations. Next to this, the research project resulted into implications for science and other organizations too as described in the introduction. Therefore, implications for science and other organizations are described in the remaining sections of this chapter.

10.1 Implications for Aia Software

The previous chapter demonstrated an EDRM system evaluation by using Aia Software as a business case. Business case specific and important criteria where measured with current available EDRM systems and their properties. The evaluated EDRM systems Microsoft RMS, DOFS, Authentica and Adobe LiveCycle have similarities and differences. To be able to compare these systems, all important criteria and system properties were measured. Unfortunately, none of the EDRM systems is considered to be a perfect match. The most important requirements from Aia Software should result into a maximum of 22 points. After comparison the following grades were given per EDRM system:

1. Microsoft RMS 18 points
2. Adobe LiveCycle 17 points
3. Authentica 17 points
4. DOFS 15 points

After the measurements, *Microsoft RMS* can be seen as the *most complete solution* according to this research project. Only a few persons were used for answering the business case specific questions, which results in an advice not suitable for real customer stakeholders. It should be necessary to use real customer stakeholders, for a more correct advice. RMS missed at least 4 essential points when comparing the essential requirements. This implies that none of the current EDRM systems are suitable.

After evaluating these systems, DOFS can be seen as the less appropriate EDRM system, because integration with Aia Software's ITP cannot be established. Next to this, the system suffers from many other described disadvantages. Adobe and Authentica seem to be similar approaches, and are both supported by server-based SDK's, which can be used to support ITP by securing digital content at a server environment. Watermarking techniques are not provided on all documents by RMS, Adobe and Authentica. This is a disadvantage, because during the research project all EDRM systems suffer from print screen attacks. By using virtual machines or other additional programs, which provide screen capturing features, it was possible to capture the content. After capturing the gathered images, it is possible to use text recognizing techniques to recreate textual documents from these images. Watermarking techniques can be used to reveal the malicious user when documents are printed or stored by print screens.

User registration can be seen as a problem for all EDRM systems. Because system administrators have too many privileges, these users have the ability to pretend to be other users as well. Although it is possible to split up EDRM Server and User management roles with multiple administrators, it seems to be always possible for them to capture digital content. These administrators need at least to be trusted, or EDRM systems will not provide a secure solution. Aia Software wanted to force users to only create secure digital documents. Only DOFS and RMS offer direct secured content creation and Authentica and Adobe need to create a temporary document first. Although it looks like RMS and DOFS offer a solution to this problem, as long as users have permissions to create bits on the client system, it is possible to create (insecure) office documents as well. Renaming created text files and opening them in an Office application will result into converting them into an insecure office document. Next to this, it is always possible for users to create other formats when they don't want to create secure content, because none of the EDRM systems provide a solution with for example notepad.

During the research project, macro functions were tried as well for testing tamper resistance, but did not result into creating insecure digital content. Authentica and Adobe can be seen as solutions, which support a broad variety of platforms, but

Aia Software is mainly interested in the Microsoft platform. Next to the described disadvantages about watermarking and user registration, the main disadvantage of RMS is considered to be *transferring rights*. Because all rights and linked users are secured *with* digital content, it is hard to change rights afterwards. To be able to limit rights, system administrators need to use a rights expression language to change the prescribed rights. Microsoft RMS offers a better integration with its applications and operating system compared to all other solutions. When one EDRM system should be considered, RMS would currently offer the best solution.

Because EDRM systems have their own advantages and disadvantages, it is possible to use several EDRM solutions per customer. In this way, it is necessary to use the developed models on each customer. This subject could be used as well to create further detailed research by using the phases and creating *decision trees* to be used by Aia Software on their customers. Such decision trees could be programmed into an application and used by consultants at customers. In this way, the best possible customer solution could be chosen to support security of digital documents. Next to this, such decision tree applications could be used with customers to stimulate intensive relationships. This would offer Aia Software a better position to sell EDRM systems by using two unique selling points: Providing multiple EDRM systems and using the decision tree application as an advice tool. Next to this, per EDRM system custom made software could be offered as an extra service to these customers. Because there are none customer stakeholders available, it is recommended to do research at potential customer organizations to reveal, which requirements are requested. In this way, it is possible to use the results with this research project to support potential and new customers.

10.2 Implications for Science

During the project, research was done by using technical aspects from literature about EDRM systems categorized as functional and non-functional requirements. According to literature, it should be necessary to investigate *law and social aspects* as well to be able to integrate EDRM systems properly in a current existing organization as described in the definition analysis. The results were based on literature, but because of fast innovations, it is hard to keep up with made progressions offered by EDRM producing companies. Therefore it is recommended to keep up-to-date with potential new innovations. Next to this, it is possible as well, that other companies come up with new EDRM systems, which offer solutions that could perform more properly in the working environment. Other EDRM systems could be analyzed

and added to the phases 4 and 5 as well to create a more complete model. Next to this, it is possible to use the research model for other types of IT systems as well to provide a scientific comparison mechanism like I did on EDRM for Aia Software. In this way, all phases should be redeveloped to provide a new framework. This would offer scientists to improve current existing EDRM systems on all properties.

During the research project some attacks were analyzed and tried on these environments. Analogue attacks seem always to be possible by making pictures of the screen. Print screen captures are possible as well by using virtual machine or screen capturing applications and can never be protected as long users have enough privileges to install software on their local clients. For further research it is possible to analyze attacks and create a model as was done during this research project. In this way, it is possible to develop attacks and create a more detailed advice about the security aspects for EDRM systems. This model could be used on other systems from information technology as well and could be used as a dynamical *security analysis model*.

When comparing EDRM with DRM, DRM offers the same kind of protection on Audio and EBooks. Because of the many similarities it could be possible to reuse the model from this project as well for other types of DRM systems. The definitions analysis (phase 1) could be used by gathering differences with EDRM as described in that chapter.

The subject could lead to further detailed research by using the results and conclusions by creating *decision trees* to be used by organizations for customers. Decision trees could provide a detailed overview on the different EDRM systems to support improvements.

10.3 Implications for other Organizations

Other organizations have the ability to use this research project as well. By using the *selection criteria model* it is possible for them to create own business case specific selection criteria. These results can easily be used by comparing the EDRM system properties for creating an own advice. Because the developed models can be used for business case specific advice, the results from this document could be used to create competitive advantage. The implications for Aia Software could offer the same advantages to other organizations as well.

In the Netherlands EDRM systems are only installed at a few organizations. There is uncertainty whether EDRM systems will be used more often in the future. Acceptance by customer organizations is rather difficult to measure. In this way, there is need to learn from experiences after implementing EDRM systems. By using the developed models and upgrading them using experiences, the implementation phase could be improved. Better implementations at customer organizations could result into increasing sales. Social and legal aspects of EDRM systems have an influence on the success which could be achieved. Because the success of EDRM systems is not determined yet, evolution of EDRM systems and development of models, which improve implementations at organizations, could have major influence on a new IT infrastructure and innovativeness of these organizations by limiting illegal distribution of digital documents.

Bibliography

[Ado07a] Adobe. Adobe livecycle. Adobe white paper, 2007.

[Ado07b] Adobe. Adobe livecycle weblog. `http://blogs.adobe.com/livecycle/`, 2007.

[Ado07c] Adobe. Configuring livecycle policy server clusters. Adobe white paper, 2007.

[Ado07d] Adobe. Deployment strategies with adobe livecycle security services. Adobe white paper, 2007.

[Ado07e] Adobe. Livecycler - a primer on electronic document security. In *Digital Rights Management*. Adobe, 2007.

[Ado07f] Adobe. Understanding and using security features with adobe reader and adobe acrobat. Adobe white paper, 2007.

[AH04] Alapan Arnab and Andrew Hutchison. Digital rights management - a current review. In *Digital Rights Management*. ACM, 2004.

[AH05a] Alapan Arnab and Andrew Hutchison. Fairer usage contracts for DRM. In *Digital Rights Management Workshop*, pages 1–7. ACM, 2005.

[AH05b] Alapan Arnab and Andrew Hutchison. Requirement analysis of enterprise drm systems. In *Digital Rights Management*. ACM, 2005.

[App03] Apple. Apple drm system itunes. `http://nl.wikipedia.org/wiki/iTunes`, 2003.

[ASF04] Habtamu Abie, Pal Spilling, and Bent Foyn. A distributed digital rights management model for secure information-distribution systems. *Int. J. Inf. Secur.*, 3(2):113–128, 2004.

[Aut05a] Authentica. Authentica: Enterprise digital rights management. `http://www.authentica.com`, 2005.

[Aut05b] Authentica. Enterprise digital rights management for document protection. http://www.authentica.com, 2005.

[BBGR03] Eberhard Becker, Willms Buhse, Dirk Gnnewig, and Niels Rump. Digital rights management: Technological aspects. *Digital Rights Management: Technological, Economic, Legal and Political Aspects*, 4:3–62, 2003.

[CDl05] CDlabs. Digital rights management. http://www.cdlabs.co.uk/, 2005.

[DRM07] DRMWatch. The leading resource for digital rights management. http://www.drmwatch.com/, 2007.

[eBo06] Planet eBooks. United states patent and trademark office. http://www.planetebook.com/, 2006.

[EBR03] Dirk Gnnewig Eberhard Becker, Willms Buhse and Niels Rump. Requirements for a rights data dictionary and rights expression language. In *Digital Rights Management: Technological, Economic, Legal and Political Aspects*. Reuters, 2003.

[Fri04] I. Fried. Apple goes to court to smoke out product leaker. C-Net News.com, 2004.

[Guo01] Heng Guo. Digital rights management using xrml. *Seminar on Network Security*, 2001.

[HW03] Tobias Hauser and Christian Wenz. Drm under attack: Weaknesses in existing systems. In *Digital Rights Management*, pages 206–223, 2003.

[Inc05] Rether Networks Inc. Display only file server. http://www.rether.com/DOFS.htm/, 2005.

[Inf06] European Information. Communications and consumer electronics technology industry association. http://www.eicta.org/, 2006.

[JM03] H.L. Jonker and S. Mauw. Core security requirements of drm systems. In *Digital Rights Management*, ICFAI, 2003.

[Law06] San Diego Business Law. Legal definitions and terms. http://www.sandiegobusinesslawfirm.com/, 2006.

[Lew98] Scott M. Lewandowski. Frameworks for component-based client/server computing. *ACM Comput. Surv.*, 30(1):3–27, 1998.

[Mic06a] Microsoft. Deploying windows rights management services at microsoft. http://www.microsoft.com/security/glossary.mspx, 2006.

[Mic06b] Microsoft. Disaster recovery for microsoft windows rights management services. http://www.microsoft.com/, 2006.

[Mic06c] Microsoft. Installing windows rights management services with service pack 2 step-by-step guide. http://www.microsoft.com/security/glossary.mspx, 2006.

[Mic06d] Microsoft. Microsoft rms. http://www.microsoft.com/security/glossary.mspx, 2006.

[oAP07] Association of American Publishers. Digital rights management for ebooks: Publisher requirements. In *Digital Rights Management*. Association of American Publishers, 2007.

[OJR07] OJR. United states patent and trademark office. http://www.uspto.gov/, 2007.

[Oue06] Eric Ouellet. Getting your organization ready for edrm. 2006.

[RD03] Bill Rosenblatt and Gail Dykstra. Integrating content management with digital rights management. In *Digital Rights Management*. ACM, 2003.

[Rus01] Austin Russ. Security essentials. In *Digital Rights Management Overview*. Sans Institute, 2001.

[SN04] Carlos Serrao and Daniel Neves. Open sdrm: an open and secure digital rights management solution. In *Open SDRM*. ISCTE, 2004.

[Som04] Ian Sommerville. Software engineering. volume 6, page 963, 2004.

[Sta04] Mark Stamp. Digital rights management: The technology behind the hype. In *Digital Rights Management*, CA95014, 2004.

[UCL06] UCLA. Ucsc media services glossary. http://media.ucsc.edu, 2006.

[vT03] Henk C.A. van Tilborg. Fundamentals of cryptology. 3(1):147–209, 2003.

[Wik07] Wikipedia. Wikipedia definitions. http://en.wikipedia.org/, 2007.

[YcC04a] Yang Yu and Tzi cker Chiueh. Display-only file server: A solution against information leakage due toinsider attack. In *DRM '04: Proceedings of the 4th ACM workshop on Digital rights management*. ACM Press, 2004.

[YcC04b] Yang Yu and Tzi cker Chiueh. Enterprise digital rights management: Solutions against information theft by insiders. In *DRM '04: Proceedings of the 4th ACM workshop on Digital rights management*. ACM Press, 2004.

Appendix A: Digital Rights Management definitions

This appendix gives an overview of several gathered definitions about DRM and EDRM. These definitions are used in several phases during the research project.

Definition 1. *Any technology used to protect the interests of owners of content and services (such as copyright owners). Typically, authorized recipients or users must acquire a license in order to consume the protected material files, music or movies according to the rights or business rules set by the content owner [Mic06d].*

Definition 2. *A technology that allows content owners to determine and control who and how users can view content such as media files on the Internet [UCL06].*

Definition 3. *DRM refers to the administration of rights in a digital environment. DRM solutions may use technologies to protect files from unauthorized use, as well as manage the financial transaction processing, while ensuring that rights holders are compensated for the use of their intellectual property [Inf06].*

Definition 4. *Digital Rights Management covers the description, identification, trading, protection, monitoring and tracking of all forms of rights usages over both tangible and intangible assets including management of rights holders [eBo06].*

Definition 5. *A variety of systems that enable the copyright owner of a piece of intellectual property (such as music, video, or text) to specify what someone else*

can do with it. Typically, this is used to offer downloads without having to worry that the user is freely distributing the file over the Web without any compensation to the copyright holder [CDl05].

Definition 6. *Any of several technologies used by publishers or copyright owners (rights holders) to control access to and usage of digital data (such as software, music, movies) and hardware, handling usage restrictions associated with a specific instance of a digital work [Wik07].*

Definition 7. *Technology for protecting files via encryption and allowing access to them only after the entity desiring access (a user or a device) has had its identity authenticated and its rights to that specific type of access verified [RD03].*

Definition 8. *EDRM systems protect sensitive information by managing and enforcing access and usage rights to the information throughout its lifecycle, no matter where the information is distributed [YcC04b].*

Definition 9. *EDRM is a category of information protection techniques that aim to manage rights to digital intellectual property and help organizations protect sensitive information from unauthorized use [YcC04b].*

Definition 10. *EDRM provide information owners the capability to specify fine-grained rights with specific files that need to be protected and to enforce these rights at the time when the files are accessed [YcC04b].*

Definition 11. *EDRM consists of the business and technological process for controlling and managing rights to digital intellectual property within enterprises [YcC04b].*

Definition 12. *EDRM systems secure digital content by encryption or isolation to prevent users from directly accessing the content, and enforce access and*

usage rights by trusted EDRM client software that authenticates with EDRM license or policy servers to get the decryption keys and rights policies [YcC04b].

Definition 13. *EDRM is an information protection technique that aims to safeguard digital intellectual property from unauthorized access by providing information owners the capability to specify fine-grained rights to protect the contents and enforce these rights at the time the files are accessed [YcC04a].*

Definition 14. *EDRM combines encryption technologies for confidentiality and authenticity, as well as identity and access management for authentication with detailed authorization privileges in one single package to provide a unified solution that protects data, authorizes users, and grants specific privileges to files and documents [Oue06].*

Definition 15. *A distributed* **DRM system** *is a conglomeration of technologies and processes necessary for enabling providers to specify terms and conditions for digital information objects, to distribute them securely, and to control how they can be used, thus ensuring the persistence and integrity of them and consumers to search provider databases for digital information objects to negotiate special arrangements for usage and to download a digital information object and consume it following the rules specified by the rights holders [ASF04].*

Definition 16. *DRM covers the description, identification, trading, protection, monitoring and tracking of all forms of usage over both tangible and intangible assets [BBGR03].*

Definition 17. *Technology to provide persistent control over files to protect sensitive documents in enterprises by copyrights enforcement or management [RD03, AH04].*

Definition 18. *DRM is to describe and identify information objects protected by IPR, to enforce usage rules set by rights holders and to provide a secure infrastructure for the preparation, distribution, storage manipulation and communication*

of objects in an acceptable trusted and manner [ASF04].

Appendix B: Digital Rights Management functions

General functions

1. EDRM systems are server-client based information technology systems [YcC04b].

2. Provide a secure infrastructure for creation, distribution, storage, manipulation and communication and protect the privacy of users [ASF04].

3. description, identification, trading, protection, monitoring and tracking of all forms of rights usages over both tangible and intangible assets including management of rights holders [eBo06, BBGR03].

4. combines encryption technologies for confidentiality and authenticity, as well as identity and access management for authentication with detailed authorization privileges in one single package to provide a unified solution that protects data, authorizes users, and grants specific privileges to files and documents [Oue06].

5. for enabling providers to specify terms and conditions for digital information objects, to distribute them securely, and to control how they can be used, thus ensuring the persistence and integrity of them and consumers to search provider databases for digital information objects to negotiate special arrangements for usage and to download a digital information object and consume it following the rules specified by the rights holders [ASF04].

6. EDRM consists of encrypting content, applying fine-grained access, authenticate users and tracking content usage [YcC04b].

7. An EDRM system consists of three major components: content server, license server and EDRM client [YcC04b].

8. Security infrastructure [ASF04].

9. DRM permits the smooth, secure, trusted movement of digital works from creator and publisher to retailers and consumers [Guo01].

10. DRM covers the description, identification, trading, protection, monitoring, and tracking of all forms of rights usages over contents and the management of rights holders relationships as well [Guo01].

11. DRM provides greater security, track, persistent protection of content, guarantees the copyright compliance [Guo01].

12. The core entities involved are users, content and rights [Guo01].

13. DRM consists of the following features: Setting and refining rights, management policies, Making and managing agreements, Managing information on acquired rights, controlling and enforcing licenses, Supporting revenue collection and sharing, Risk management [AH05a].

14. DRM systems consist of the following steps: production, digitalization, identification, ascription, description, distribution, usage, monitoring of usage, initiate payment [BBGR03].

15. The EDRM client consists of an EDRM controller that receives the users request and communicates with the license server. After authentication and authorization, the digital content is returned with provided privileges of the particular user [YcC04b].

16. To protect digital contents against all kinds of inside attacks, DRM solutions or other like Display-Only-File-Server should be used, where digital contents is never send to the client software [YcC04b].

17. To enforce access and usage rights by trusted EDRM client software that authenticates with EDRM license or policy servers to get the decryption keys and rights policies [YcC04b].

18. EDRM systems with client software, which encrypts the digital content with certain prescribed rights can be seen as vulnerable, because client software can be reversed engineered [YcC04b].

Stakeholder functions

1. EDRM contains identification and classification of digital contents and users [Oue06].

2. DRM systems give organizations the ability to implement own business models for digital content [RD03].

3. Providing portals for external users like business partners [RD03].
4. Stakeholders of DRM systems: Creator, provider, Consumer [YcC04a].

Rights functions

1. The rights model allows expressions to be made about the allowable permissions, constraints, obligations, and any other rights related information about users and content [Guo01].
2. EDRM provides persistent protection to digital contents [YcC04b].
3. to provide persistent control over files to protect sensitive documents in enterprises by copyrights enforcement or management [RD03, AH04].
4. to protect the interests of owners of content and services [Mic06d].
5. to protect files from unauthorized use [Inf06].
6. for protecting files via encryption and allowing access to them only after the entity desiring access (a user or a device) has had its identity authenticated and its rights to that specific type of access verified [RD03].
7. secure digital content by encryption or isolation to prevent users from directly accessing the content [YcC04b].
8. Allowing access after authentication [RD03].
9. Protection of digital contents via encryption [RD03].
10. Persistent protection is provided by Packagers, Controllers and License servers [RD03].
11. Allow owners of data to prescribe access control rules, which will either work as prescribed, or not allow access at all [YcC04b].
12. Safeguarding digital information throughout its entire lifecycle and preventing unauthorized access even after the protected data has been distributed to end users [YcC04b].
13. An EDRM or DRM system contains a rights model, which specifies the different kinds of rights on digital contents by users which users and for how long these rights can be active [YcC04b].
14. The rights model can be implemented by using a Rights Expression Language [YcC04b].

15. Content owners are users within EDRM who provide certain digital content for other users with certain rights and become in this way rights owner the particular document [YcC04b].

16. that allows content owners to determine and control who and how users can view content [Inf06].

17. the administration of rights in a digital environment [Inf06].

18. that enable the copyright owner of a piece of intellectual property (such as music, video, or text) to specify what someone else can do with it [CDl05].

19. used by publishers or copyright owners (rights holders) to control access to and usage of digital data (such as software, music, movies) and hardware, handling usage restrictions associated with a specific instance of a digital work [Wik07].

20. protect sensitive information by managing and enforcing access and usage rights to the information throughout its lifecycle, no matter where the information is distributed [YcC04b].

21. that aim to manage rights to digital intellectual property and help organizations protect sensitive information from unauthorized use [YcC04b].

22. provide information owners the capability to specify fine-grained rights with specific files that need to be protected and to enforce these rights at the time when the files are accessed [YcC04b].

23. for controlling and managing rights to digital intellectual property within enterprises [YcC04b].

24. that aims to safeguard digital intellectual property from unauthorized access by providing information owners the capability to specify fine-grained rights to protect the contents and enforce these rights at the time the files are accessed [YcC04b].

25. File access permissions [RD03].

26. User and group (role) identifiers [RD03].

27. Provides more sophisticated forms of rules on digital contents than other type of security systems (read, print,,etc.) [YcC04b].

28. different kinds of users can have different kinds of privileges on digital contents [YcC04b].

29. EDRM consists of Multi Level Security (MLS) [YcC04a].

30. The Rights model is the core of DRM and is based on the relationship between users, objects, rights and conditions [YcC04a].

Tracking and control functions

1. Providing persistent protection to digital content by control and track access. [RD03].
2. DRM systems are expanded with tracking access to operations on content [RD03].
3. DRM can be extended with tracking and monitoring usage of data without violating privacy laws [YcC04b].
4. Usage tracking and monitoring module [ASF04].

Content functions

1. The content server contains a content database or file server and DRM packager [YcC04b].
2. The content database or file server is to store the protected content [YcC04b].
3. The DRM packager is for encrypting and packaging digital content and related metadata, and creating rights specifications for the content [YcC04b].
4. Digital content is foreseen of unique identification numbers for recognition and tracking the usage [YcC04b].
5. License server consists of a license generator, key database, rights database and identity database [YcC04b].
6. Licenses from the license generator contain information about the rights specification, identification of the content with certain rights, and the identity of the user or device that wants to exercise rights to the content [YcC04b].
7. Providing rights to digital content by the introduction of Rights Expressions Languages [RD03].
8. DRM systems without license servers install rights descriptions directly with the digital container [RD03].
9. Identification and description of digital contents, Enforcement of fine-grained rules of usage for and of rights of access, Monitor and track usage [ASF04].

10. EDRM systems have different kinds of business models, which can be different per digital content [AH05a].

    Financial functions

1. rights holders are compensated for the use of their intellectual property [Inf06].
2. manage the financial transaction processing [Inf06].
3. DRM systems mostly make use of the rental model or the pay per song/album or document [AH05a].

Appendix C: Definition model

In this appendix the developed definition is translated into a definition model, which can be used for organizations to create an own definition for EDRM. The definition model consists of systematic business case specific questions, which can be used to formulate an appropriate definition. By using inputs from the literature and answering the following questions, it is possible to create an own suitable definition.

The following questions need to be answered:

1. **Is there need for a client-server-based information technology system as described in section 3.3.1?**
2. **Is there need for content management as described in section 3.3.1?**
3. **Is there need for tracking and control management as described in section 3.3.1?**
4. **Is there need for rights management as described in section 3.3.1?**
5. **Is there need for security management as described in section 3.3.1?**
6. **Is there need for stakeholder management as described in section 3.3.1?**
7. **Is there need for persistent protection of digital content as described in section 3.3.1?**
8. **Are the stakeholders described in section 3.3.1 desirable?**
9. **Is there need for enforcement and/or management as described in section 3.3.1?**
10. **What kind of digital content needs to be protected? (use section 3.3.1 as input)**

11. **Against which kind of attackers must the system protect digital content (section 3.3.1)?**

12. **Which goal should the system provide? (chose from section 3.3.1)**

13. **Must the system be operational in a more closed or open environment? (as described in section 3.3.1)**

Appendix D: Degree of importance

In this appendix a list of all functional and non-functional selection criteria are gathered. This list can be used to assign a certain degree of importance per selection criterion. This list can be used on business cases when applying the selection criteria model.

Criteria	**-1**	**0**	**1**	**2**
Content management	-	-	-	-
Content creation				
Content metadata				
Uniquely identifiable content				
Distribution model				
Searchability				
Partial asset protection				
User access to information about rights				
Personal backup				
Tracking and control management	-	-	-	-
Logging content usage				
Watermarking				
Rights and protected content recovery				
User management	-	-	-	-
User registration				
Uniquely identifiable users				
Scalability				

By using the selection criteria model and the related questions, it is possible to determine which specific criteria are important during the comparison of EDRM systems. During the comparison of the EDRM systems for Aia Software only criteria with a degree of 2 were used (high importance).

Criteria	**-1**	**0**	**1**	**2**
Rights management	-	-	-	-
Rights per document and user				
Rights transfer				
Dynamical rights				
Rights templates				
Usage rules				
Content versioning				
Security management	-	-	-	-
Key individualization				
Decryption keys disclosure				
Limited document usage				
Renewability				
Standard key management				
Tamper-resistance				
No single point of failure				
Other non-functional criteria	-	-	-	-
Simple implementation				
Portability - Platform shifting				
Portability - Format shifting				
Portability - Space shifting				
Portability - Time shifting				
Integration with existing applications				

Table 1: Selection criteria with degree of importance