Enterprise Rights Management: A new technology for safe collaboration in the Product Development

Prof. Dr.-Ing. Reiner Anderl, anderl@dik.tu-darmstadt.de
Joselito Rodrigues Henriques, M.Sc., henriques@dik.tu-darmstadt.de
Technische Universität Darmstadt - Department of Computer Integrated Design, Petersenstraße, 30 D-64287- Darmstadt - Germany

Abstract. *The cooperation between companies in the product development process is well-established worldwide. The necessity to increase the productivity and reduce the costs leads companies to focus on their core competences and to cooperate with other partners in different areas to improve their products. An appropriate example for instance is the automotive industry where an OEM needs to collaborate with several suppliers in different places of the world to make the development of a new car possible.*

Together with the collaboration process comes the necessity to exchange and share digital documents with the partners. Besides the technical difficulties to exchange documents like CAD files for example, another important factor appears regarding the security of the document exchanged between the partners. Nowadays, in most companies that exchange data, the security is just kept by contracts and law and not by technical or organizational mechanisms that really could guarantee the security of the data being exchanged. The security just based on contracts is not sufficient; as soon as the data crosses the border of the company there is no way to control what is being done with the document.

A method to ensure that only authorized people can access distributed documents, no matter where they are located, is provided by Enterprise Right Management (ERM). With an ERM solution, the system protects the file as soon as the document is created. Several approvals can be granted or denied, e.g who is allowed work with the document, how long it can be accessed, which actions can be performed. The owner of the digital document now is able to control it everytime, even if the document crosses the borders of the company. This paper presents this new technology, its components, functionality, processes and also an analysis of ERM solutions available in the market.

Keywords*: Enterprise Rights Management, Product Development, Data Exchange*

1. INTRODUCTION

Since the CAD system was introduced at the end of the 60s [1], product development completely changed. Information which used to be stored in a piece of paper (drawings) or in a physical model (physical mockup) can be saved digitally today. Digitalized product information means more flexibility and efficiency for product development. A digital document can be easily stored, accessed, reproduced and integrated into the process chain.

After the digitalized product had been developed, the new target was to improve CAD systems in a way that each model would contain more information and thus to integrate it into the subsequent processes of product development like manufacturing and assembling.

With the development of several CAD systems with its proprietary format a new difficulty arose for data exchange: Data only could be read by using the same system. In order to solve this problem some research was done which aimed at generating neutral data exchange format which support exchange between different CAD systems. Different exchange format like IGES [2], SET [3], VDA-FS [4] were developed and in 1994 different countries decided to create norm ISO 103003 [5] "International standard for the data exchange of product data model" (well known as STEP). The application protocol AP214 [6] was created especially for automotive industry.

The STEP standard was very important for the CAD data exchange process since it meant improvement in the quality of 3D model exchange. Information like product structure, name, position and material could act as transferee between different CAD systems.

Improvement of CAD systems and data exchange brought economical and technical [7] benefit to collaboration in product development. More information could be integrated to the 3D CAD model which on one hand accelerates the generation of models and on the other hand integrates into the product lifecycle.

Integration of knowledge into the digital product and efficient data exchange do not just mean benefit but also loss for companies which have know-how integrated in a digital product document. It makes innovations and know-how of those companies an easy target for external and internal espionage. In 2008 a study [8] concluded that over a period of four years there were more than 500 cases of data espionage.

Figure 1 shows the result of analysis which identifies the initiators of data breaches and how many median records were compromised. It confirms loss of information is found internally and externally of companies.

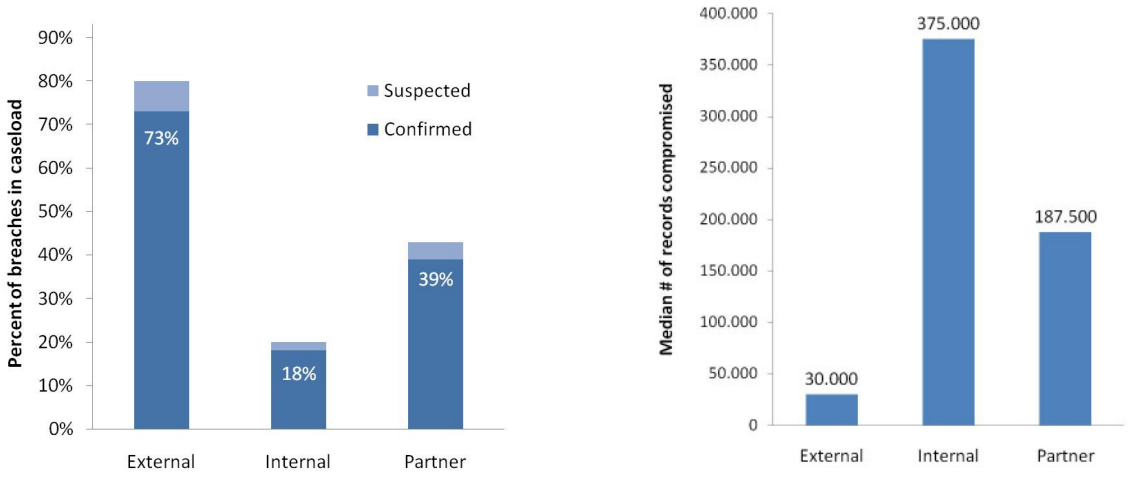

Figure 1- Sources of Data Breaches and Median Number of Records Compromised [8]

Although the percent of breaches in caseload inside are smaller than the outside the median of records compromised is more than 10 to one. The incidents involving partners tend to be substantially larger than those caused by external sources. It shows that the privileged parties are able to do more damage to the organization than outsiders, this can be seen in the Table 1 that shows the calculation of risk (likelihood x impact).

Table 1- Calculation of risk (likelihood x impact) [8]

Source	Likelihood	Impact(# of Records)		Risk (Pseudo)
External	73 Percent	30.000	=	21.900
Internal	18 Percent	375.000	=	67.500
Partner	39 Percent	187.500	=	73.125

The damage caused by industrial espionage and product piracy has increased continually in the last few years. Without a technical solution it is not expected that this trend will diminish in the near future. Damage caused to German companies by industrial espionage costs around 20 billion Euro per year [9]. This causes considerable damage to German automotive industry. Illegally spied out information on product and production allows competitors to copy company´s innovative products.

Economical and industrial espionage affects businesses of all sizes. In 2007 a study even showed small and medium enterprises the ones to be most affected. Over the years large companies have developed a very good security structure, protecting themselves against an unwanted extensive information flow. Medium-sized companies are significantly more at risk to become victims of espionage, because they concentrate more on developing innovative know-how, so there is less time for security arrangements.

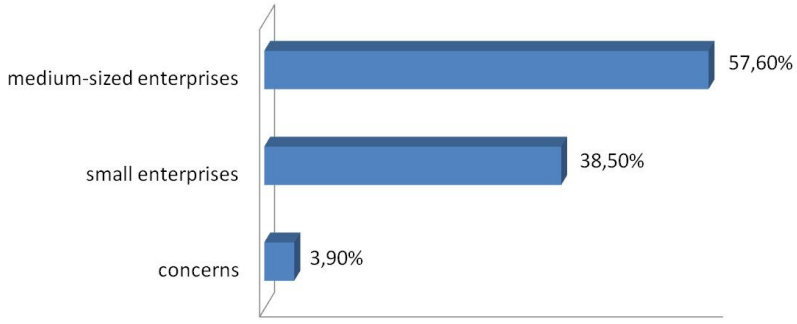

Figure 2 - Damage by company size [9]

Cooperation between companies in the area of product development is well-established world-wide. The necessity to increase productivity and to reduce costs forces companies to focus on their core competencies and makes those companies cooperate with other partners in different areas for the benefit of better products. The automotive industry, for instance, is a good example. In order to develop a new car an OEM needs to collaborate with several suppliers in different countries.

Now that collaboration needs to happen in different places of the world and digital data with know-how of companies need to be exchanged, the challenge is how to work efficiently and at the same time ensure security for intellectual property (IP).

2. TECHNICAL APPROACHES TO PROTECTING INTELLECTUAL PROPERTY

There are different approaches to secure the IP of the company. One approach is the legal level which is based on contracts and the other approaches based on technical solutions. The legal level is very important and should be done to secure the IP, but it will not be covered in this paper due this method alone is not efficient to really protect the IP, the contract agreement between two partners is not able to keep the date security inside and outside of the company, each person with bad intention can easy abuse of the data.

Technical solutions should be implemented to minimize the ways in which intellectual property can be lost. The following methods are commonly used:

- **Terminal servers (**Figure 3**a)** allow to retain complete control over data but can only be used if the data a user generates the user's own company. This technical method is very good to protect the IP inside the company but does not cover the data exchange that is necessary for the collaborative product development [10].
- **Data Leakage Prevention** (DLP) (Figure 3**b):** This method is used in order to control which data can be exchanged through a transfer point like e-mail, network or external storage devices etc. This solution allows protecting data only via controlling the users software environment. As soon as the data is copied via an uncontrolled interface or leaves the company it can be distributed to anybody [10].
- **Data filtering (**Figure 3**c):** This method consists of reducing the information inside the data files which should be transferred; it is used by the automotive industry to transfer CAD data between partners during the development of the product [11, 12, 13]. This method is efficient to protect IP for the data exchange but does not protect the IP inside the company and also does not offer support to control the information when it leaves the company. Another important disadvantage is when the data has been modified by a partner company, the preexisting information which was deleted by the own company cannot be easily recovered from the modified file anymore.
- **ERM (**Figure 3**d):** In this method the data is protected and monitored as soon it is generated and this protection is kept for its complete life cycle [10, 14]. It is the only method that offers IP protection inside and outside of the company.

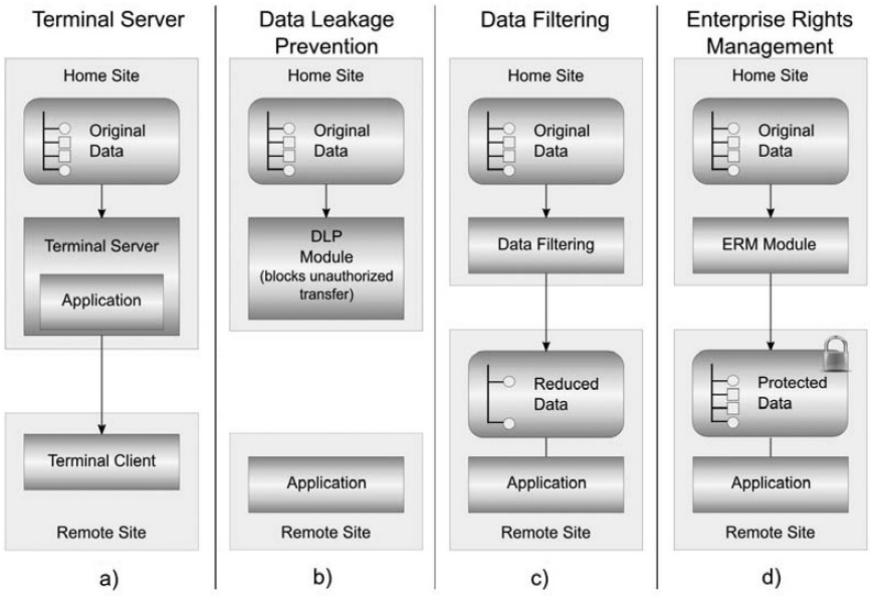

Figure 3 - Technical approaches to protecting intellectual property [10]

3. ENTERPRISE RIGHTS MANAGEMENT (ERM)

Enterprise Rights Management (ERM) is a technical solution, based on cryptography, that supports IP protection in a distributed development scenario. It ensures that only authorized people can access distributed documents, no matter where they are located. With ERM, the system protects the file as soon as the document is created. Several types of approvals can be granted or denied, e.g who is allowed work with the document, how long it can be accessed, which actions can be performed. The owner of the digital document is now able to control it all the time, even if the document crosses the borders of the company.

ERM provides protection directly for the content that requires protection using cryptography and ensures that the protection cannot be removed; it means that the content only exists in encrypted form during their entire lifetime. The rights to access a document or their contents can be defined for a specific user but also for a group of users like a CAD department. The right can be changed anytime and the effect is (almost) immediately. Therefore, if a member of the staff leaves the company, all their rights to access data can be withdrawn from them. Also local data storage is protected by the ERM solution.

Users must authenticate themselves each time they access the data according to obtain authorization to view or process the data. ERM also has a logging function for recording every access to the document or its contents, it stores the user, time and which action has been done with the document. With the log function it is possible to identify any information leaks and pursue them at a later stage. This also increases the possibility to identify the specific member of the staff involved in the know-how theft and attributes it to them [10].

An ERM System has two main components, the rights server and a client application. The server stores a key used to decrypt the data for the protected document as well as the rights assigned to particular users. The application is responsible for decrypting the document but still keeps it in a secure environment and restricts the users' access according to his permitted rights, and also encrypts the document again when the data leaves the application environment.

If a document requires protection, its author encrypts the data with the help of the rights server. The recipient then receives the decoding key from the server. Figure 4 shows the steps involved in encryption and decryption. The document's author then requests the server to encrypt the contents, or to send them a key to encrypt the document (1). The server returns the protected document or the key which the author then uses to encrypt the contents (2) and stores the decoding key. After this, the document is sent to the recipient (3). The recipient then asks the server for the decoding key (4). If the recipient has the appropriate access rights, the server sends them the key (5). This enables the recipient to decrypt the document (6).

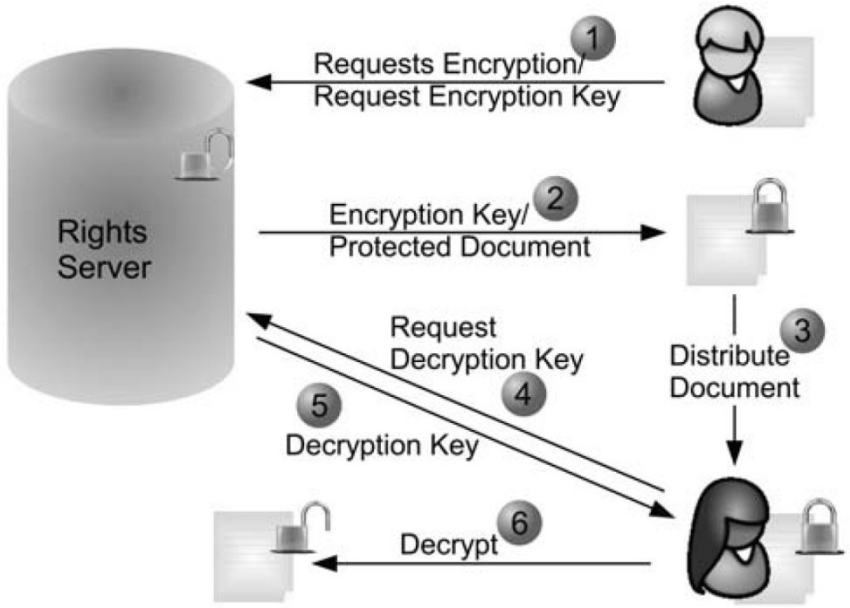

Figure 4 - Security with ERM solution Sever-Centered Approach [10]

4. ERM REQUIREMENTS

An ERM solution should provide protection for all critical data to achieve maximum protection for a company's intellectual property. Critical data includes office format, design ideas in pictures format and also projects data that are in CAD format.

In the study done by Prostep iViP [10] the requirements for ERM solutions were divided into the following six categories:

- **Right Expressivity**: This category includes requirements relating to the effectiveness with which rights can be defined - the extent to which access to data can be restricted. There should be different rights to define which data-related operations a user may perform on the data they are permitted to access. It must be possible to assign separate rights for reading, saving, and editing data, or converting data to a different format.
- **Format/Application Support**: In this category the most important applications and format that should work together with ERM systems are defined. It defines two CAD systems (Catia V5 and Pro/E), Acrobat Reader, Microsoft Office (Excel, Word and PowerPoint), JT/VisView and also three formats: STEP, TIFF and JPEG.
- **Integration & Interoperability**: This defines the requirements relating to the integration & interoperability of ERM in the companies. It requires that the solution should be easy and quick to be implemented, that support different external certificates, must run in batch and bulk process, offer integration with PDM/PLM systems, support automatically data exchange process, offer integration with the exiting user group of the companies and has interoperability between the different ERM systems.
- **Functionality**: Here the requirements regarding the functionality of an ERM Solution are defined. The following functions are expected: Apply and withdraw rights to a date, check a user's rights online every time he/she accesses the protected files, permit user work offline for a specific time, log check a user's rights online every time he/she accesses the protected files, transfer rights control to the contractor, all the rights should be managed centrally in one place. It should also be possible to combine a number of rights to form a rights group (for example, confidential, internal, and public), integrate external encryption algorithms, import external certificates to the system, or to implement a hardware-based certification solution.
- **Usability**: This category defines usability requirements of an ERM solution: The following requirements are defined: The system should involve as little administrative effort as possible, rights should be assigned simply and efficiently, solutions to apply the rights automatically should be also implemented if possible.
- **Organizational**: This category describes the organizational requirements and includes: Infrastructure that makes external users available to the ERM system for authentication, support for subsequent versions of the application and work independently of the firewall.

For collaboration in the product development there are specific requirements that an ERM system needs to cover to be able to protect IP. The IP in a CAD model is spread in different areas. In this paper fifteen areas where identified for the analysis of the actual ERM systems as presented in Figure 5.

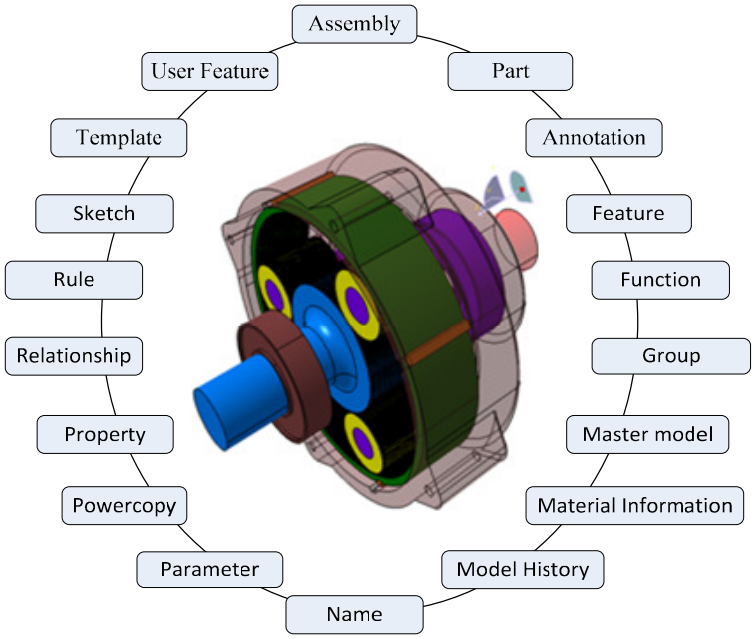

Figure 5 - IP in CAD Data

5. ANALYSIS OF ERM SYSTEM REGARDING IP PROTECTION FOR 3D CAD DATA

For CAD data in particular, as showed in Figure 5 there are specific ERM requirements that still have not been evaluated in current commercial ERM solutions.

Some previous DRM system evaluations e.g. [15] and [16] do not satisfy current requirements and therefore cannot be used as a base for the CAD data exchange in collaborative product development. In the product development, it may be necessary to assign specific access rights which go beyond access rights for the entire document. For example, all users should be authorized to read the document, but only specific groups of designers should have a write authorization. In order to do that, a solution must be able to assign individual rights to specific parts of a document. It should also be possible to restrict access to particular information, such as material, weight, or geometry [PROSTEP].

There are two primary motivations behind this analysis: Firstly, to identify if the current ERM systems are able to protect IP in 3D CAD data used in the collaborative product development. Secondly, an evaluation framework allows developers of existing and future system to address the various gaps in exiting systems. This is also a necessary step in any standardization process.

The CAD system considered in this study was CATIA v5 R16 from Dassault Systèmes. It was evaluated two commercial ERM systems that support protection for CAD data:

- Adobe LiveCycle ES Rights Management from Adobe Systems Incorporated [17,18]
- Microsoft Right Management Services from Microsoft Corporation [19,20,21]

Table 2 shows the result of the analyses done in this study.

Table 2 - Summary of the requirement rating for the two ERM systems

	ERM Systems	
Requirements	**Adobe**	**Microsoft**
Assembly	✔	✔
Part	✔	✔
Annotation	✘	✘
Feature	✘	✘
Function	✘	✘
Groups	✘	✘
Master Model	✘	✘
Material Information	✘	✘
Model History	✘	✘
Names	✘	✘
Parameter	✘	✘
Powercopy	✘	✘
Property	✘	✘
Relationship	✘	✘
Rules	✘	✘
Sketch	✘	✘
Templates	✘	✘
User Feature	✘	✘

The result shows that both ERM solutions offer protection only for Assemblies and Parts. Each Part and Assembly is saved in a single file. Currently the ERM solutions are only able to protect file-based CAD data. The other requirements cover the actual knowledge stored inside the CAD files together with the geometry information. The evaluated ERM solutions currently do not meet those requirements.

Therefore it is necessary to improve current ERM solutions in order to provide security of the knowledge stored in the 3D CAD Part files.

6. CONCEPT FOR AN ERM SOLUTION TO PROTECT IP IN 3D CAD DATA

The 3D CAD data exchange is a necessary and one of the main parts in the development of the product in the collaborative product development. The companies need to share 3D CAD data with partner companies during the development of the product, but at the moment the method to protect their IP is not efficient. On the one hand companies use data filtering (Figure 6a), which amounts to a partial deletion of the knowledge of the file while the remaining information is being left entirely unprotected

On the other hand the ERM solution (Figure 6c) protects the data just at file level while a lot of information is not protected.

In this paper a new ERM concept is presented, that also protects the knowledge and information saved in inside a 3D CAD file or embedded within the representation of 3D CAD model. This concept is based on a fusion of those two complementary technologies, namely data filtering and ERM.

The new concept for IP protection in 3D CAD data utilizes the data filtering technology to trace and identify the knowledge information in the CAD model, while the former deletion of the information is now replaced by ERM technology to protect the intellectual property. Figure 6b illustrates the new concept based on these two existing technologies described in section 2.

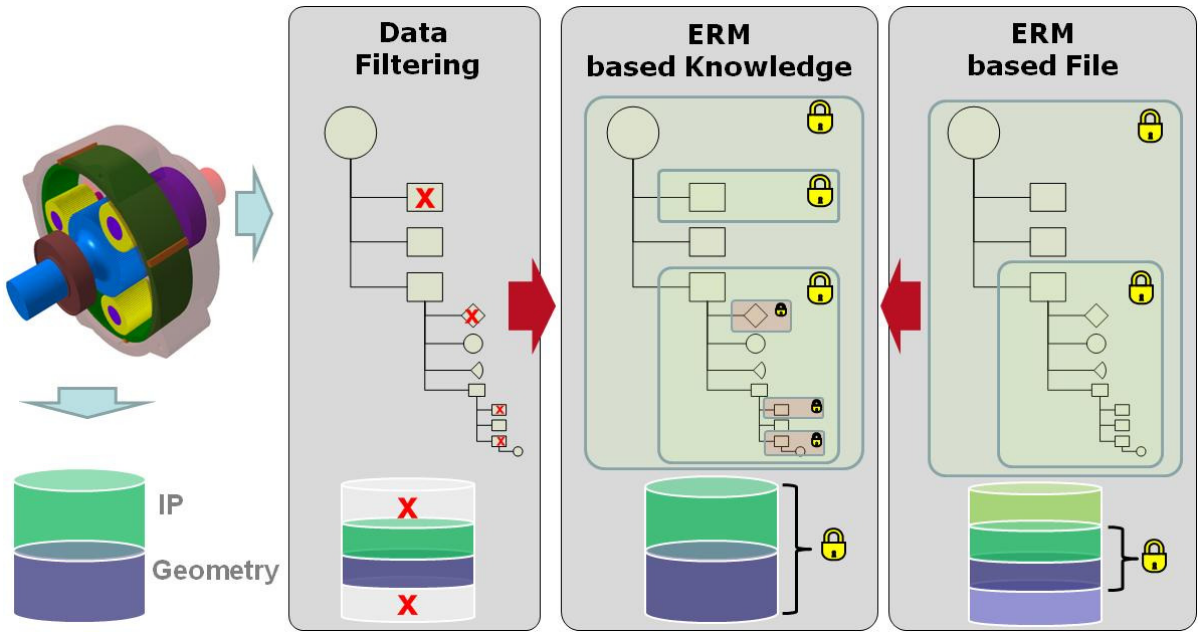

Figure 6 - Concept for an ERM solution for Knowledge in 3D model data

The implementation of this concept in the ERM solution represents a major technological progress regarding the safety in the collaborative product development process. It makes it possible to realize the collaborative product development in a confidential and safe way, secured by a technically robust, low-level and efficient solution. The new concept will outperform state-of-the-art approaches e.g. mutual, but simple contracts between the development partners or inefficient, crude and incomplete technical methods in terms of reliability and efficiency while operating on fairly more advanced security level.

The next step of this research intention is to conduct the proof of concept and implementing a software prototype and setting up a validation szenario with the following modules:

- **Open-Source 3D CAD System**: With an open-source CAD system, it is possible to alter and refine the low-level functions as the source code is free to be changed.
- **Known file format**: As it is necessary to rework the file format, a well known file will make the work possible.
- **Commercial ERM System**: As an ERM system is a complex tool that involves several technologies and yet there is no open-Source ERM system, a commercial ERM system will be applied. The ERM can be customized, adapted or single functions can be used by connecting the software prototype to the API (Application Programming Interface) of the ERM system or by the use of its SDK (Software development kit).

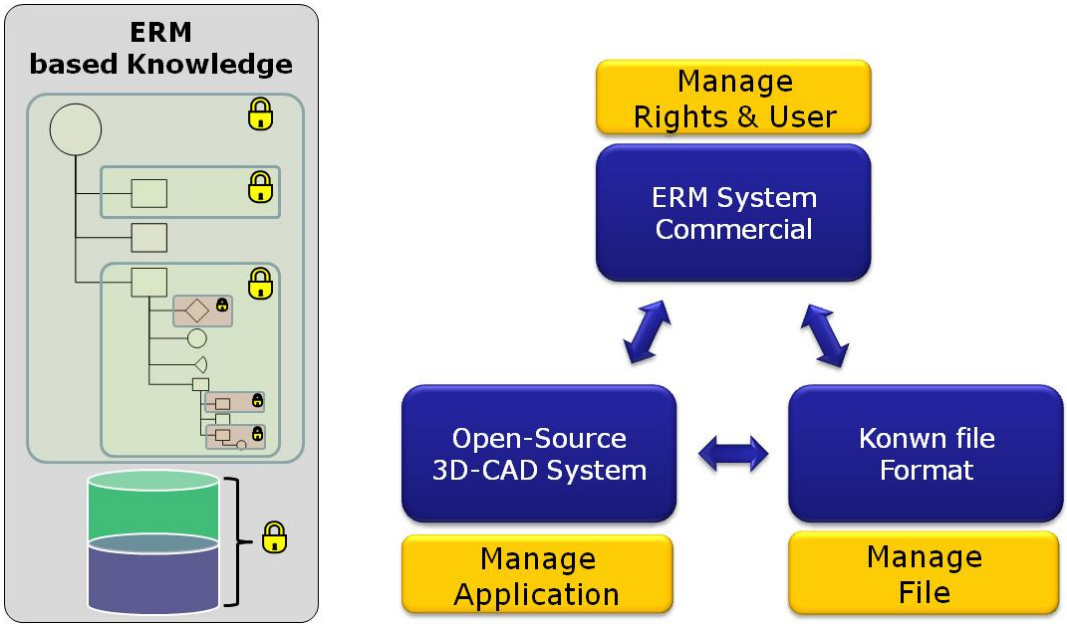

Figure 7 - Component for the implementation of the new ERM concept

7. CONCLUSION

To assure the 3D CAD Intellectual Property in a collaborative product development nowadays, it is necessary to combine a variety of technical methods. For example, data filtering can first be used to reduce know-how contained in issued data. Data can then be provided with ERM protection. Finally, a DLP solution can analyze data transfer and ensure that only ERM-protected files leave the company.

This study shows that the ERM solutions analyzed just protect 3D CAD data at a file level. This is the first step for protection but this is not enough to protect IP in the 3D CAD data in a collaborative product development because the knowledge inside files is still not protected.

A new concept for the ERM solution was developed based upon two existing technologies: Data filtering and ERM. Its implementation represents a big technological progress regarding the safety in the collaborative product development process. It will make it possible to realize the collaborative product development in a safe way based upon a technical and efficient solution.

8. ACKNOWLEDGEMENTS

The work described in this paper has been funded by CASED Center for Advanced Security Research Darmstadt (www.cased.de) supported by the Federal State of Hessen, Germany, through the LOEWE program.

9. REFERENCES

[1] Sutherland I. E: Sketchpad. In: Annual ACM IEEE Design Automation Conference: New York, 1964. p. 6.329 - 6.346.

[2] IGES, Initial Graphics Exchange Specifications 5.3. ANS US PRO/ IPO-100-1996. National Institute of Standards and Technology, US Pro, US, http://www.uspro.org/documents/IGES5-3_forDownload.pdf.

[3] ANDERL, R. Externe CAD-Schnittstellen. Methoden und Werkzeuge zur CA-Integration. Germany: HANSER, 1993. cap.8.

[4] SPUR, G.; KRAUSE, F. Das virtuelle Produkt: Management der CAD-Technik. Germany: Hanser, 1997. cap.4.9.

[5] ANDERL, R.; TRIPPNER, D. Architektur und Organisation der technischen Datenverarbeitung. In: STEP standard for the exchange of product model data: Eine Einfuhrung in die Entwicklung, Implementierung und industrielle Nutzung der Normenreihe ISO 10303 (STEP). Germany: Deutsche Bibliothek, 2000. cap. 3.

[6] ISO 10303-214, Industrial automation systems and integration -- Product data representation and exchange -- Part 214: Application protocol: Core data for automotive mechanical design processes, 2003.

[7] GALLAHER, M. P.; O´CONOR, A. C. Economic impact assessment of the international standard for the exchange of product models data (STEP) in transportation equipment industries: final report. Gaithersburg: National Institute of Standards and Technology, 2002.

[8] BAKER, W., HYLENDER, C. D., VALENTINE, J. A. 2008 Data Brach Investigation Report, Verizonbusiness, 2008. URL: http://www.verizonbusiness.com/resources/security/databreachreport.pdf.

[9] Industriespionage: Die Schäden durch Spionage in der deutschen Wirtschaft, Studie, Corporate Trust, 2007, URL: http://www.corporate-trust.de/pdf/STUDIE_191107.pdf.

[10] PROSTEP iVip, Secure Product Creation Processes (SP2), White Paper, ProSTEP, 2008.

[11] Kleiner, S., KRASTEL, M., Diebstahlsicherung, Digital Engineering Magazin Zeitschrift, Vaterstetten 2007.

[12] CLASSEN, E. Protection of Intellectual Property in the Product Development Process. In: Proceedings of the 11º Seminário Internacional de Alta Technologia, Universidade Metodista de Piracicaba, Brasil 2006.

[13] LIESE, H., Spitznagel, P., Know-how-Schutz für CAD-Entwicklungsdaten, Bericht, ProSTEP iVip Symposium, Berlin 2008.

[14] Hartmann, Michael / Bitz, Gunter: Enterprise Security – Informationsschutz im Unternehmen, in: Pohlmann, Norbert / Reimer, Helmut (Hrsg.): Trusted Computing – Ein Weg zu neuen IT-Sicherheitsarchitekturen, Wiesbaden: Vieweg, 2008, S. 125 - 139.

[15] ARNAB, A., HUTCHISON, A. An Evaluation Framework for DRM. Proceedings of the 6th International Workshop for Technical, Economic and Legal Aspects of Business Model for Virtual Goods incorporating The 4th International ORDL Workshop. October 16-18, 2008, Poznan, Poland/ ed by Rüdiger Grimm and Susanne Guth, Poznan University of economics publishing house. Poznan, Poland, pp 176-199. ISBN 978-83-7417-361-2, 2008.

[16] Mulligan, D., HAN, J. and Burstein, A. How DRM Based Content Delivery System Disrupt Expectations of "Personal Use". Proceedings of the 2003 ACM workshop in Digital Rights Management (2003), ACM, pp. 77-89.

[17] ADOBE, Adobe LiveCycle Rights Management ES for CATIA for multiformat design collaboration. URL: http://www.adobe.com/products/livecycle/pdfs/lces_rtsmgtcatiamulti_es82.pdf.

[18] ADOBE, Delivering an information risk management strategy across the heterogeneous enterprise. URL: http://www.adobe.com/products/livecycle/pdfs/95011600_lc_rightsmgmt_wp_ue.pdf.

[19] MICROSOFT, Windows Rights Management Services.
URL: http://www.microsoft.com/windowsserver2003/technologies/rightsmgmt/default.mspx.

[20] MICROSOFT, Microsoft Identity and Access Solutions.
URL: http://www.microsoft.com/windowsserver2008/en/us/ida-information-protection.aspx.

[21] ROSENBLATT; B. Technology Comparison: Authentica Active Rights Management and Microsoft Windows Rights Management Services. White paper, Giantseps Media Technologiy Strategy, 2005.

10. RESPONSIBILITY NOTICE

The authors are the only responsible for the printed material included in this paper.