INTERNATIONAL DESIGN CONFERENCE - DESIGN 2014
Dubrovnik - Croatia, May 19 - 22, 2014.

INFORMATION MANAGEMENT IN PRODUCT DEVELOPMENT WORKFLOWS – A NOVEL APPROACH ON THE BASIS OF PSEUDONYMIZATION OF PRODUCT INFORMATION

D. Gerhard, G. Reinauer, A. Krumboeck and R. Ljuhar

Keywords: product development, information management, design knowledge and collaboration, pseudonymization, access control

1. Introduction

Damage caused by economic- & industrial espionage as well as product piracy leads to a total economic loss of several hundred billion euros per year with an increasing trend [International Chamber of Commerce 2011], [Corporare Trust 2012], [Zimmermann 2012], worldwide. According to estimates by the Austrian Federal Office for Constitutional Protection [2010], companies and organizations from in particular Southeast Asia and Eastern Europe take great efforts in gaining access to Western product technologies, manufacturing techniques and scientific research. Different sources estimate the potential economic damage for Austria alone from 880 to five billion euro annually [Austrian Ministry of the Interior 2008], [University of Applied Science Vienna 2010]. The German Federal Ministry of the Interior [2013] estimates the damage caused by industrial espionage in Germany to around 50 billion euro annually. Several key drivers have been identified responsible for this development:

On one hand, the increased competition from emerging economies has changed the parameters of the competition. The DACH region (Germany, Austria, Switzerland) is known for its strength in research and development, especially in the field of mechanical engineering [Deutsche Bank 2008], responsible for innovations in fields ranging from aerospace to automotive and a key driver for exports and employment. While the manufacturing is often relocated to low cost countries abroad, the research and development departments remain resident in Europe. This valuable knowledge acquired over years of R&D is in demand worldwide. Emerging economies using at increasing rate economic and industrial espionage as well as direct copying of existing products to overcome technological deficits and catch up to the leading industrial nations, which thereby secures an advantage in the intense global competition [German Ministry of the Interior 2013]. On the other hand, the increasing integration of manufacturing locations, distributed product development scenarios, international collaborations and joint ventures result in an environment in which it is increasingly difficult to control and track the flow of product and design information effectively across the product lifecycle. Without adequate organizational and technical measures, effectively preventing an internal or external abuse of sensitive know-how becomes nearly impossible. Employees and their specific knowledge and expertise are often not the most important values in a company anymore, but rather the existing electronic documents as carriers of the intellectual property [Corporate Trust 2007]. As such electronic media can be exchanged easily, mailed or copied, there is an increasing need to properly protect these values by technological and organizational security measures.

Know-how theft can occur in different ways [KPMG 2013], for example by poaching employees, through skilled social engineering or by retrospectively analyzing products. However, the most accurate information about a product or technology at the earliest possible time in a development phase can be best achieved through the theft of electronic documents such as engineering drawings, product specifications, and the like. Studies [Ernst and Young 2011], [Corporare Trust 2012], [KPMG 2013] show that in a significant number of cases even the own employees or partners such as suppliers, contract manufacturers and the like are responsible for the unauthorized disclosure of valuable information. Yet extensive and complex product development scenarios demand that information required for the different tasks of the product development phases is made available to the variety of internal and external stakeholders. Information management systems, such as Product Lifecycle Management Systems, allow a far-reaching and powerful management of product information as well as built-in advanced access control schemes. Furthermore, such systems offer the tools and features to capture, edit, share and store all information involved in the product development process. The challenge for any information management system rests in balancing the required information security against the required flexibility in sharing intellectual property with internal and external stakeholders.

Appropriate organizational and technical information security concepts must ensure that access to information managed by such systems is specifically controlled and information theft can be ruled out in advance. Especially in distributed product development scenarios it is imperative that critical product information is only exchanged in a secured manner and access is limited to the extent necessary to complete a certain task or project [Ernst and Young 2011]. In this regard, a number of data (not information) security concepts for an application in product development environments are presented [ProSTEP iViP 2008], [Anderl 2010], [Henriques 2012]. These concepts address different layers of protection and not all are aligned on a sheer product development application. As a minimum demand for an appropriate protection concept for the use in the field of product development, it must be ensured that confidentiality, integrity and the availability of the underlying information is ensured. This publication introduces a new method for secured access, distribution and management of product information. In particular, this concept enables a fine-grained protection of sensitive documents, by offering a user-dependent level of product information without the need for a filter or the likes. By virtualizing the information from the document, even sensitive documents can be made accessible for collaborations. The concept of pseudonymization allows a secure management and sharing of information based on a multilayer-access scheme [Riedl et al. 2007].

2. Related Work

As the basis for a secured management of information, it is necessary to first classify information into definable sensitivity-classes and to define the extent of which it can be shared/made available to stakeholders in the organization/project. As product development and related tasks are increasingly performed not only as an internal development project, but involve increasingly suppliers and outsourced manufacturing facilities, an implemented concept must be dynamic enough to encompass all aspects of such a complex environment. In particular, product information must be managed flexibly enough so that it can be made accessible to the extent required to different project partners. For product development applications, there are, besides legal means of protecting sensitive know-how, a number of technical methods to securely exchange, manage and access-control product information:

- (Role-based) access control models (RBAC) manage the access to documents or directories based on a person’s role in the enterprise. Once the user has authenticated himself against the system using a user name and password, the system will grant access based on the defined role. However, once the system has granted access, no control regarding the intended use of the information is possible. For this reason, the use of RBAC for the specific protection of product information is only applicable to a certain degree and should be combined with additional concepts to achieve an acceptable level of information security.
- Digital watermarks provide an identification of origin of a document that remains a part of the document even once it is made accessible beyond the company borders. Therefore, the root of

a document can be clearly identified. However, the major shortcoming of digitally watermarking a document is that this does not prevent anyone from using the information in an unintended way (i.e. copying or distributing).

- Unauthorized information outflows at interfaces can effectively be prevented through data leakage prevention (DLP) solutions. Similar as before, the drawback of such a tool is that it is not adequate to secure sensitive documents outside the corporate perimeters nor does it provide protection against internal information theft.
- In contrast, data filtering is helpful to reduce (irreversibly) the degree of information in a document by removing selected sensitive elements. But using data filtering in a collaborative environment is all but straightforward: different partners each have different tasks and objectives, thus will need their own batch of information in order to complete the project. This requires independent versions of the original document – each consisting of the project relevant level of information. Merging or tracking of changes carried out by the involved (internal or external) stakeholders back into one master document is a complicated task and can potentially lead to a lack of information integrity.
- Cryptographic schemes offer a powerful method to secure information within and outside a company. In product development applications, such concepts are implemented in particular through enterprise rights management (ERM). Using ERM [ProSTEP iViP 2010], documents are encrypted already during the creation process and can be decrypted only after authentication against the central ERM server. The protection is firmly connected to the document and is maintained over the entire life cycle. A central ERM server manages and controls the user authorization and handles the user key management. ERM does not allow the definition of an information level within a document without applying an additional data filter.

Table 1 gives an overview of the presented security concepts for a use in product development applications and the targeted level of security:

Table 1. Level of protection based on different information layers

Application Level	RBAC	Watermarks	DLP	Data Filter	ERM
Application	x	-	-	-	-
Document	-	x	-	x	x
Transport	-	-	x	x	x

Of the presented methods, data filtering and ERM offer from a security point of view an advanced protection of sensitive information, even in distributed product development scenarios. The major drawback for both methods can be found in the fact that each for itself has specific shortcomings. For data filtering it is evident, that usability and information integrity can be influenced in an unfavorable way if a well-defined concept is not implemented. As with any cryptographic method, the strength of ERM rests in the strength of the keys not the algorithm itself [Schneier 1995]. Once a key has been compromised, the assurance of the concept is lost. This, among the fact that an encryption based on a definable information level cannot be established, is seen as a significant shortcoming of ERM.

A promising approach provides a combination of both, ERM and data filtering [Henriques 2010]. This makes it possible to implement not just a protection on a file level basis but instead a fine grained access and safeguard of selected elements within a document. Through the filter application, sensitive elements are removed at first. Subsequently, the remaining elments are secured using ERM based policies. Depending on the the extent of the required information exchange/depth of the collaboration, a user can now be authorized to access different levels of the information contents. Sensitive elements are no longer part of the shared information which offers a significantly higher level of enterprise information protection. However, using such an approach is not without drawbacks: the creation of requirement-specific versions of an original information demands a well defined reqirements concept (*who needs to access which information and to what extent*) and can result in a complex information management, including tracking and sharing of multiple versions of the original information. Without a well-defined concept, this could thereby greatly impact information consistency and integrity.

Based on the mentioned shortcomings of the concepts described in this paragraph, this paper defines the following demands for a novel information management concept that should allow a secured storage and management of information on one hand and a fine grained information sharing based on roles and objectives on the other hand:

1. The security system shall separate information and the corresponding information identification
2. The information itself shall further be separated into independent data-fragments which can be re-assembled into partial or complete information based on the demands of the organization
3. The reference-information (referred to as *information/frag-links*) required for a re-assembly of the fragments to complete or partial information shall be administered and managed securely (i.e. encrypted)
4. The reference-information shall be securely stored so that only authorized users gain access.
5. Each user in the system shall have a personal set of secret keys, stored on a secured device (Smartcard, USB Token, etc.)
6. No administrator shall have access to the user keys
7. The data-fragments shall be stored in an unordered manner so that without access to the reference-information, a manual attempt to re-assemble the data-fragments becomes too burdensome
8. No centralized key management repository shall exist
9. As a fall back mechanism in case of loss or damage of a user key, a number of randomly selected users can re-assign a user key (referred to as "Operator Principle" [cf. Riedl, Gascher and Neubauer 2007])
10. Existing organizational forms and processes shall not be changed or altered when implementing the security system

The subsequent section introduces an overview of the designed system based on the demands stated in the enumeration above.

3. System Overview and Functionality

Sharing product information to the extent required (*on a need-to-know basis*) while simultaneously maintaining a secured management of the very same, is the core demand of the presented security concept. By separating the critical pieces of information from a document - depending on the requirements and objectives assigned - a user can be authorized to re-assemble the critical information elements of the document in full or limited extent. No filtering process is applied, but instead a separation of information into independent data fragments allows a customizable re-assembly of the original information for different user groups. The re-assembly of these fragments is controlled by *information-links*. Such a link consists of pairs of pseudonyms which are used as fragment identifiers (a pseudonym is defined in this context as a unique random number), similar to instructions on how the fragments must be re-assembled in order to regain meaningful information. The concept of pseudonymization [Riedl et al. 2007] is applied to securely access, manage, distribute and recover these information-links. Every user (internal or external) within the system controls a set of personal information-links that will re-assemble documents to a defined information level. By concealing the information-links with a personal user key, it is only possible for the user himself to utilize these links for information retrieval. Once information is added to the system, it is disintegrated into a definable number of fragments. Each fragment is assigned a pseudonym name and stored randomly among all other fragments. Thus, it is no longer possible to link a fragment to a document by its original file name or search for specific information within the fragments. Without access to the (decrypted) information-links, it becomes nearly impossible as well as pointless to copy or steal the fragmented information. The corresponding information-links are always needed to regain interpretable information. However, only the user with the personal keys is able to retrieve the concealed information.

As an example given, an engine assembly could present the top-level information, consisting of a number of sub-level information. The sub-level information may encompass various components (parts) and documents. After separating the top-level information from the corresponding sub-level parts, information-links can be set in a way, that an (e.g.) internal user has access to a different level of information than an external supplier. The supplier only gets access to those parts needed to complete the task.

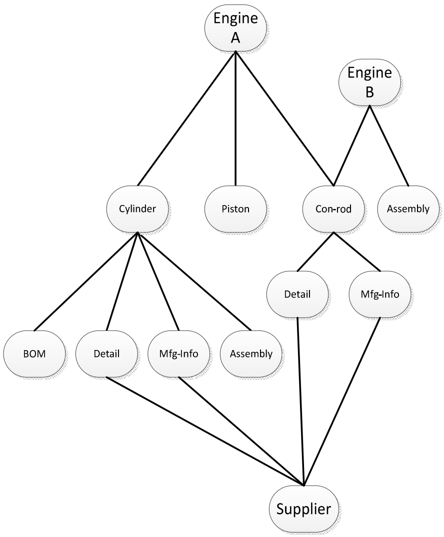

Figure 1. Information structure based on different requirements

For an integration of the presented method in a PDM system, it is necessary to apply a different approach to the way information is managed and stored within such a system: the PDM system no longer manages *coherent* documents as before, instead so called “starting-links”, consisting of a single pseudonym are used. Such as “Start-Pseudonym” (Start-PSN) allows to query and retrieve all information-links that are connected to this specific PSN, thus providing the required references to find and retrieve the fragments for a re-assembly of the selected document.

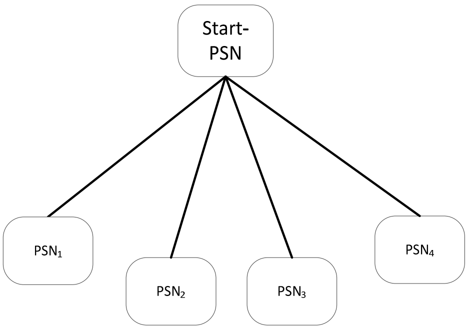

Figure 2. Information structure for a PDM application

On the other hand, integration into (CAD) applications can be most efficiently achieved by using already built-in application interfaces. The majority of commercial CAD systems do have such an interface built in (e.g. Creo Elements/Pro offers a proprietary Java Toolkit Interface), which allows to change the information handling of the application without the need for an extensive and time consuming integration effort or changes to the application itself. An example of a possible system architecture and its components is given below:

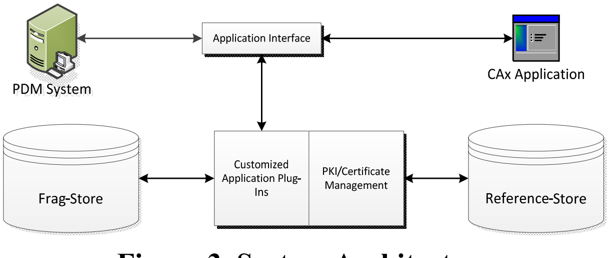

Figure 3. System Architecture

The system architecture consists of the following components:

1. **Frag-Store:** storage area for the fragmented information (using only pseudonym names for the fragments). The more fragments there are, the lower the probability that an attacker unveils possible relationships/references. The Frag-Store does not necessarily have to be a central repository, but can instead be distributed over various independent locations. For an additional level of security, the fragments can (but don't necessarily have to) be encrypted
2. **Reference-Store:** central database for the secured storage of the concealed information-links. The Reference-Store does not *know* what information-links belong to which user but instead ensures the safety and integrity of the stored information
3. **Customized Application plug-ins:** application-specific functions that are required for the separation of information and storage of the fragments
4. **PKI / Certificate Management:** managing the user specific information-links, issuing of user keys and pseudonyms
5. **Application interface:** required set of functions for the communication with a PDM/CAD application

4. Implementation of a use case based on the neutral 3D data format JT

The neutral, ISO-standardized data format JT ("*Jupiter Tessellation*") has become a popular format especially for visualization of product information (with a focus on applications in the automotive industry) [Ding 2007], [Anderl 2011]. An essential characteristic of the JT format is the scalability of the geometric information content [Kingston 2007] based on the user requirements thereby reducing the degree of information while at the same time accurately representing large and complex geometries [Ding 2007], [Kingston 2007], [Attfield 2010]. The JT format is supported by the JT Open initiative, which includes a number of prominent industry and software companies as well as academic institutions. Joining this initiative allows members to access the JT technology in form of proprietary C++ libraries (JT Open Toolkit). These enable participating members to create their own, customized JT-related applications [Siemens PLM 2013].

Using the APIs provided in the JT Open Toolkit, selected use cases based on NX 8.5 have been realized. The deciding factor for choosing JT is - next to the open format and the Toolkit libraries - that changes made in JT files get (almost) entirely transferred back to the native CAD format. In these use cases selected information levels (attributes such as dimensions and PMI) were assigned to user groups without the need for a filter program. Subsequent changes to those attributes were executed directly in the JT file and could be transferred back to the native format if needed.

In order to analyze and disintegrate a JT file into independent data blocks, a suitable product structure-to-JT file structure mapping is required. Within JT, the following three common product structure-to-file structure mappings are defined:

1. **Per Part** – an assembly is stored in an individual JT file and parts are stored as an individual subdirectory JT file
2. **Fully Shattered** – the entire product structure is disintegrated and stored in individual JT files
3. **Monolithic** – the entire product structure is stored in one single file

The JT Open Toolkit provides libraries needed to create appropriate JT file content based on user specific demands. For the selected use cases, the following criteria were chosen:

- *The native CAD file shall consist of an assembly with several parts*
- *Attributes such as dimensions and PMI shall be added to the parts*
- *A "Fully Shattered" conversion native CAD-to-JT is needed*

An authorization based on different information-links results in different views of the underlying CAD assembly when visualizing the file (e.g. using the JT2Go viewer). Figure 5 gives an example of a specific user who has been authorized to visualize the graphical representation of the entire assembly (including all parts) but without any attributes like dimensions or PMI.

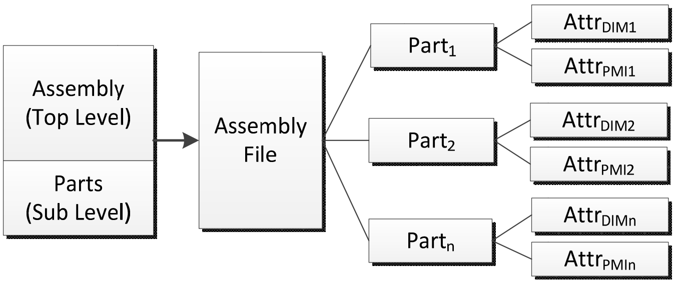

Figure 4. Fragmented JT File Structure

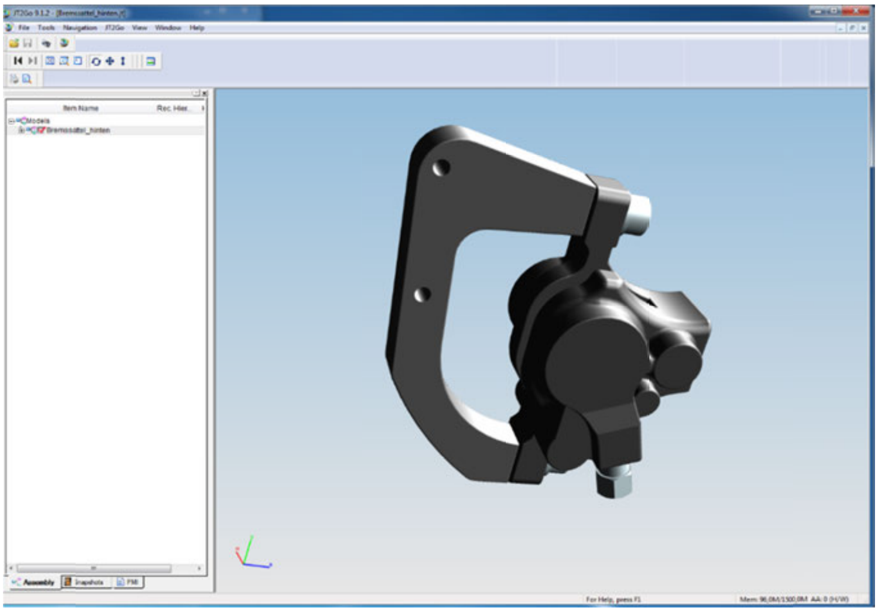

Figure 5. Assembly w/o Dimensions and PMI

Figure 6 shows another user who has been authorized to access sub-level information (i.e. just specific parts) only, including dimensioning and manufacturing attributes of the respective part.

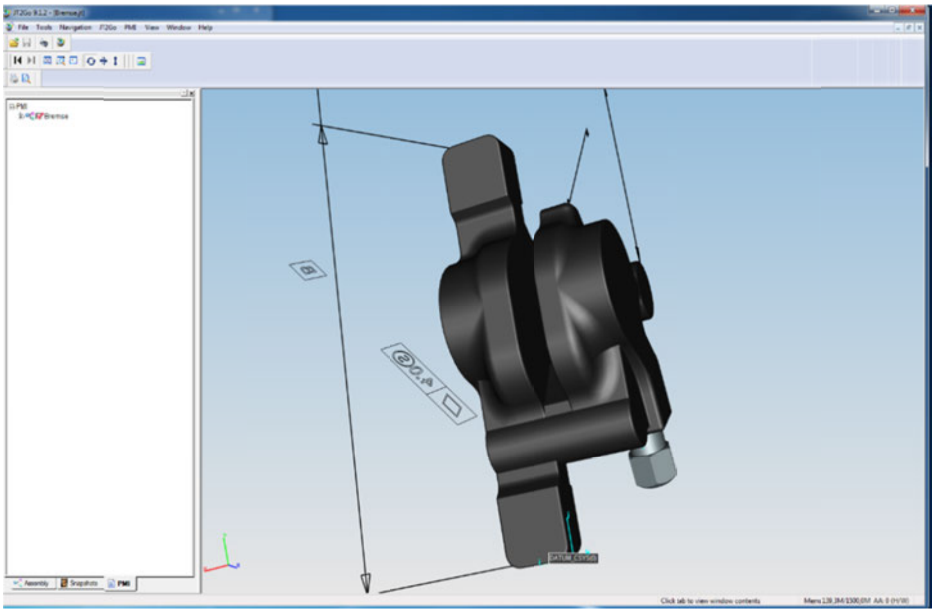

Figure 6. Part with Dimensions and PMI

As an additional example, yet another user has equally been authorized to access sub-level information only, including dimensioning attributes of the part. However, as shown in figure 7, manufacturing information (PMI) is not apparent.

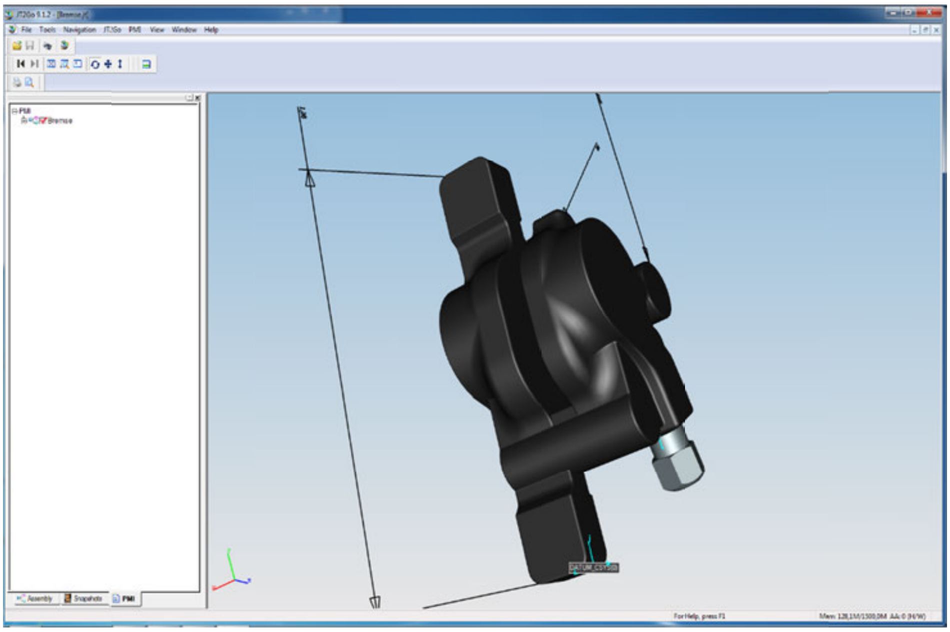

Figure 7. Part with Dimensions but no PMI

5. Conclusion

Unauthorized information leakage and theft of sensitive know-how in product development scenarios is a growing problem. Product development is no longer done exclusively within the company boundaries but has become a widespread and complex task with different internal and external stakeholder united in a common project. The various development sites create, exchange, and alter the information required for the development of a product. The provision, exchange and secure management of information throughout the entire product development process are key criteria for the success of such an endeavor. Those involved in the product development process require the necessary information in sufficient extent as distributed product development scenarios make an intensive exchange of know-how all but indispensable. However, information needs to be shared and made accessible on a need- to-know basis in order to ensure that only this level of information is being shared, which is indeed necessary to finish the task.

Different methods exist to ensure the confidentiality and integrity of sensitive product information. But as described earlier, there are several significant shortcomings to these concepts. Therefore, this paper presents a novel method for a secured information management. Based on the separation of information into independent data fragments, the level of information within a document can be adjusted based on requirements of a certain task. The unordered storage of those fragments using only pseudonyms instead of descriptive files names prevents any linking of the fragments to a certain document or file – this provides additional safeguard against internal information theft. Only an authorized user with the matching personal keys can again derive interpretable information from within the set of fragments. The concept does not apply any filtering as this is would add significant overhead to ensure information integrity. An encryption of the fragments is not considered necessary in case of a well-thought separation of information – however, the information-links need to be managed encrypted within a secure area.

The integration into commercial CAD software is to a high degree dependent on the availability of built-in, application-specific interfaces. Such interfaces generally allow a seemless intergration of outside programs/routines into the existing CAD application. By doing so, the CAD files can be modified without the need to make changes to the functionality of the application itself.

The concept presented in this paper differs from comparable concepts in the way how information security is achieved and thus opens up new options and scenarios for a secured and save form of information exchange and management. The required steps for an implementation of this concept into a PDM/CAD environment still need to be specified in detail and subsequently formulated and are subjected to a review in pilot projects. Investigating the appropriate steps for a successful integration of this concept into PDM/CAD applications and workflows were only partially covered by the research objectives of this paper. Further work is needed to investigate how large scale assemblies consisting of a multitude of parts and attributes can be separted using automated procedures. This could significantly reduce the amout of time needed to implement and customize the concept into existing environments.

Acknowledgment

We want to thank Braincon Technologies and Siemens PLM Austria for their support in providing the necessary soft- and hardware to design and test our use cases. Further we want to thank Davul Ljuhar for his input and critical review of our research strategies. This work is the result of a joint research project between Braincon Technologies and the University of Technology Vienna. Our research was supported with a grant by the Technology Agency of the City of Vienna (ZIT).

References

Anderl et al., "Analyse des unternehmensübergreifenden Visualisierungs- und Strukturdatenaustausch", White Paper, ProSTEP iViP Publication, 2010.

Anderl, R., Malzacher, J., Ufer, A., "Analyse des unternehmensübergreifenden Visualisierungsdaten- und Strukturdatenaustausch", White Paper, ProSTEP iViP

Attfield, A., "JT Validation – Panel Session", Sept 12-14, 2010 Siemens International Conference.

Austrian Federal Office for Constitutional Protection, Constitutional Report 2010.

Austrian Ministry of the Interior, "Industriespionage: Firmen unterschätzen die Gefahr", Press Release in the newspaper Wirtschaftsblatt, 14.02.2008.

Corporate Trust GmbH, "Industriespionage – die Schäden durch Spionage in der deutschen Wirtschaft", Study, Online Publication, 2007.

Corportate Trust GmbH, "Industriespionage 2012 – aktuelle Risiken für die deutsche Wirtschaft durch Cyberwar", Study, Online Publication, 2012.

Deutsche Bank Study, "Deutscher Maschinenbau macht Wirtschaft fit für die Zeit nach dem Öl", October 2008.

Ding, L., Ball, A., Matthews, J., McMahon, C. A., Patel, M., "Product Representation in Lightweight Formats for Product Lifecycle Management (PLM)", 4th International Conference on Digital Enterprise Technology, 2007.

Ernst & Young, "Datenklau: Neue Herausforderungen für deutsche Unternehmen", Study, Online Publication, 2011.

German Ministry of the Interior, "Wirtschaftsspionage – 50 Milliarden Schaden", Press Release, 28.8.2013.

Henriques, J., Von Lukas, U., Mesing, B., "Schutz geistigen Eigentums mit Enterprise Rights Management in Economic Engineering", 02/2012.

Int'l Chamber of Commerce (ICC) (2011), "Estimating the global economic and social impacts of counterfeiting and piracy", Study, 2012.

International Standards Organization (ISO), "Industrial automation systems and integration – JT file format specification for 3D visualization", ISO/DIS 14306, 2011.

Kingston, K., "Supplier Collaboration", Siemens PLM Conference Presentation, 2007.

KPMG, "Compliance gegen Kriminalität – Industriespionage, die unterschätzte Gefahr", Study, Online Publication, April 2013.

ProSTEP iViP e.V., "Recommendation - Enterprise Rights Management", White Paper, 2010.

ProSTEP iViP e.V., "Secure Product Creation Process (SP^2) – Sichere Datenaustauschprozesse in der unternehmensübergreifenden Produktentwicklung", White Paper, 2008.

Riedl, B., Gascher, V., Neubauer, T., "A secure e-health architecture based on the appliance of pseudonymization", Secure Business Austria Research, 2007.

Riedl, B., Neubauer, T., Goluch, G., Boehm, O., Reinauer, G., Krumboeck, A., "A secure architecture for the pseudonymization of medical data", Proceedings of the Second International Conference on Availability, Reliability and Security, 2007.

Schneier, B., "Applied Cryptography: Protocols, Algorithms, and Source Code", C. Wiley, 2nd Edition, 1995.

Siemens PLM, "Getting Started with the JT Open Toolkit", JT Open Toolkit V6.3.3.0, Feb 2013.

Siemens PLM, "The JT Open Program Overview – JT Open Factsheet", http://www.plm.automation.siemens.com/en_us/products/open/jtopen/program/index.shtml.

University of Applied Sciences Vienna, "Gefahren durch Wirtschafts- und Industriespionage", Report, 2010.

Zimmermann S., Wiesner M., "VDMA Studie Produktpiraterie, Arbeitsgemeinschaft Produkt- und Know How Schutz", VDMA 2012.

Dipl. Ing. Richard Ljuhar, Project Leader, SecurePLM Research Project
Insitute for Engineering Design and Logistics Engineering, Department of Mechanical Engineering Informatics and Virtual Product Development, University of Technology Vienna
Getreidemarkt 9, 1060 Vienna, Austria
Telephone: +43 161067
Email: Richard.ljuhar@tuwien.ac.at
URL: http://www.ikl.tuwien.ac.at/maschinenbauinformatik_und_virtuelle_produktentwicklung/