8-7-2011

Managing knowledge distribution to prevent product imitation and counterfeiting

Julian Bahrs
Chair of Business Information Systems and Electronic Government University of Potsdam, julian.bahrs@wi.uni-potsdam.de

Norbert Gronau
Chair of Business Information Systems and Electronic Government University of Potsdam, norbert.gronau@wi.uni-potsdam.de

Gergana Vladova
University of Potsdam, gergana.vladova@wi.uni-potsdam.de

Managing knowledge distribution to prevent product imitation and counterfeiting

Julian Bahrs
Chair of Business Information Systems and Electronic Government
University of Potsdam
julian.bahrs@wi.uni-potsdam.de

Norbert Gronau
Chair of Business Information Systems and Electronic Government
University of Potsdam
norbert.gronau@wi.uni-potsdam.de

Gergana Vladova
Chair of Business Information Systems and Electronic Government
University of Potsdam
gergana.vladova@wi.uni-potsdam.de

ABSTRACT

Product piracy poses an existential threat to many companies. Juristic property rights, which are currently dominantly put to practice, do not suffice to combat this threat. The rise in cases of piracy and the increasing professionalism of the counterfeiter, give grounds for effective methods of prevention. Based on the gap of existing approaches identified we evaluate how knowledge modeling could help to design preventive measures. We develop a novel approach which makes information and knowledge leaks transparent, analyzable and controllable. The approach is based on modeling the interactions and transfers of information and knowledge between departments of a company with internal and external business partners. For this purpose, a modeling process for knowledge-rich business interactions is used and modified for the specific purpose. Choosing dynamic assessment questions allows to on the one hand establish the level of risk of information and knowledge on piracy and on the other hand to prioritize measures specific to a company. In addition, the procedure reappraises companies' existing modes of prevention. Based on this analysis, the method helps to develop and rank measures to hinder the theft of information by pirates. The introduced approach fills the gap in known concepts of protection, which are used only after a case of piracy has taken place. The approach also adds a new perspective in knowledge management.

Keywords: modeling, knowledge activities, protecting knowledge, chinese walls, evaluation of knowledge

PRESENT STATUS: PROBLEM PRODUCT COUNTERFEITING

Knowledge Management typically focuses on the identification and sharing of knowledge among groups of people, e.g. the employees of a company with the ultimate goal to increase process efficiency and quality of results. However, there are downsides in making knowledge freely available, even within closed groups or among the value chain. This is not only the risk of information overload (Eppler and Mengis, 2004), but also the potential of knowledge misuse or product counterfeiting, which has not been respected within the discussion of knowledge management so far.

Nevertheless product piracy or counterfeited products have become commonplace (Barboza, 2009; OECD). Often the term product piracy is used to describe a mixture of counterfeiting and piracy. Counterfeiting aims to imitate the original and disrespects trademarks, copyrights or patents. Often the producers use their own name as authorship. Knockoffs and Nearbrands often refer to gray market plagiarism and may be legal. Piracy refers to the stealing of brand names, the producers claim different authorship, as for example brand piracy (Neemann, 2007; Jacobs, Samli and Jedlik, 2001). Product piracy has meant severe financial consequences for companies, whose products or brands have been copied (OECD; Chaudhry and Zimmermann, 2009). On the one hand, a company directly loses in turnover and earnings, on the other hand

the image of a company may suffer on account of cheap copies or potentially face legal claims (OECD). The buyer also does not necessarily profit from their purchase. Although, the price may be lower, pirated versions will typically have inferior insurance through guarantees or accountability by the producers. In many cases, pirated copies are qualitatively worse which may lead to additional damage for the brand. If for example, fake spare parts are used in machines, there is a possibility that the entire machine will be damaged. Furthermore, security problems can arise, up to a life-endangering level, when copies are implemented, often unknowingly, as shown by reports of brake pharmaceuticals (Fenoff and Wilson, 2009).

Product piracy has progressed enormously due to increasing levels of organization of counterfeiters and growing profitability (Jacobs, Samli and Jedlik, 2001). Various studies estimate the damage caused by piracy as between five and nine percent of the trade volume (Jacobs, Samli and Jedlik, 2001; International Chamber of Commerce, 2007).

The motivation for the forger is the absorption of profits in the short term (Jacobs, Samli and Jedlik, 2001; Staake, and Fleisch, 2008). The profit probability is increased by (illegally) taking advantage of services, especially those which in the life cycle of a product are immediately connected to production. Counterfeited products evade the cost of product development whereas pirated products additionally avoid the costs of market launch as well as warranty, liability and other post sale services (Staake, and Fleisch, 2008) . Accordingly, the products most affected by piracy are those for which the markup on production costs for development and profit is especially high. This is often the case for spare and wear parts, which sometimes even serve to subsidize primary products (for example, printers which are sold under value and the matching, expensive ink cartridges which generate the profit). For the producer of the original product the time at which the pirate product is introduced onto the market is key; the later this happens, the smaller is the financial loss.

In this contribution we focus on starting points for the acquisition of know-how of the Forgers: these are the finished products, which are analyzed through reverse engineering, but also any attainable information, know-how and the knowledge holders themselves. To obtain missing knowledge, any freely available information may be of value, as well as that which is acquired through tricks, under false pretenses or even through industrial espionage.

Enterprises are Tied in Value Webs

Taking this into consideration, the point of departure for our deliberations are in particular the relationships between companies and the fact that producers are today often involved in complex value added networks. For this purpose, information and knowledge and in some cases even corporate secrets are shared to varying degrees (Normann, and Ramírez, 1993). For example, the exchange of information throughout a supply chain, including suppliers, logistics service providers and customers, are automated using IT-systems (Hendricksa, Singhalb, and Stratman, 2007). An enterprise's intellectual property can be attacked at many points along the chain. This was confirmed by a qualitative appraisal of six companies in context of the method development. The assertion was reached by semi-standardized depth interviews to the issue of product piracy, in which vulnerable relationships to employees, competitors, certification bodies, consultants, and so on where identified, where in the past there had been suspicions of malpractice. These theoretical considerations and the explorative approach have lead to a checklist of over 20 categories of network partners. From the company's point of view these can be marked as information or knowledge receivers. The network environment of an enterprise therefore creates the conceptual basis of our approach to control the outflow of know-how.

Known approaches to stop product piracy

A multitude of measures have been proposed to eliminate or reduce as far as possible the threat of product piracy. None of these have singularly been able to guarantee complete safeguarding. In the past, the main focus was on legal safety measures, especially securing industrial property rights; however these can only provide sanctions against cases of piracy which have already occurred. Particularly in the early phases of product development, securing property rights is difficult due to costs and enforced disclosure, for example when obtaining patents (Berrier, 1996). For this reason, it has become increasingly important for enterprises to systematically confront information and knowledge outflow. However, there still exists considerable mystification concerning the breadth of the information which is made available as part of regular business activity and about which information is worth safeguarding.

Fig. 1. exemplarily shows known approaches to impede product piracy by the three areas "juristic", "organizational" and "technical" (OECD; Neemann, 2007; Jacobs, Samli and Jedlik, 2001; Staake, and Fleisch, 2008). It further shows whether an

approach is preventative or whether it comes into effect after a case of piracy has occurred (marked "piracy occurs" on the axis "time of effectivity"). The security concepts marked in color in Fig. 1. are influenced by the method introduced in this contribution. The goal is to safeguard a company already before a case of piracy has occurred and accordingly integrate the means of defense into the company's business strategy.

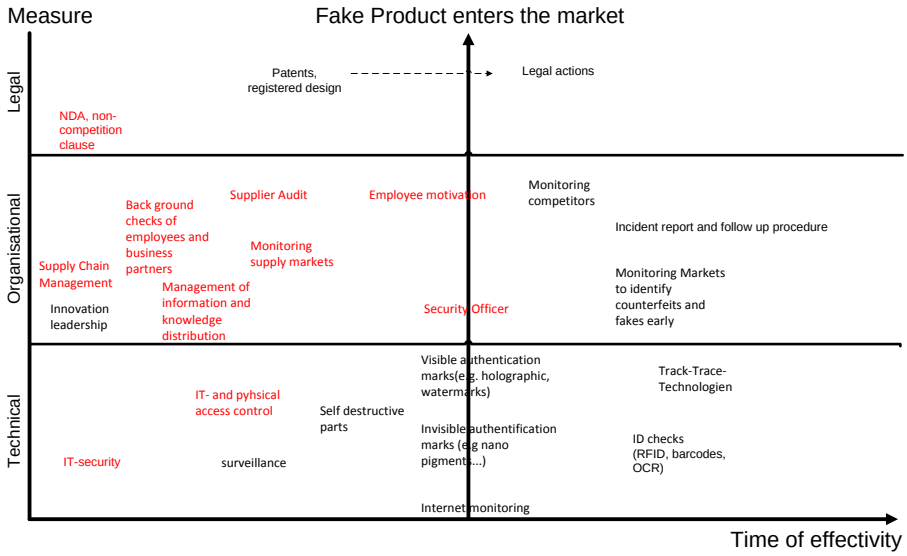

Fig. 1. Examples of approaches to the prevention of product piracy

KNOWLEDGE MODELING TO PREVENT UNWANTED KNOWLEDGE LEAKS

In knowledge management research modeling is widely used for visualization and design for both, knowledge and information flows as well as business processes and actor interactions. This is reflected by various approaches to business process oriented knowledge management (Heisig, 2003; Gronau and Weber, 2004; Woitsch and Karagiannis, 2005). Here we evaluate how these approaches could help in preventing unwanted knowledge leaks. As a starting point we chose the Knowledge Modeling and Description Language (KMDL) (Gronau and Weber, 2004b; Fröming, Gronau and Schmid, 2006) for its ability to reflect individual tacit knowledge as well as its view of knowledge activities. KMDL is an approach to process oriented knowledge management, which, analogous to business process management, analyses actual processes and draws up set-point processes. Contrary to classical approaches of business process modeling, KMDL focuses not only on procedural and information aspects but also on personal knowledge. The original goal of KMDL is the improvement of processes through the conception of demand-oriented measures using the knowledge management method. Semi-formal models are used to visualize and analyze processes. In particular by modeling the activity view, which shows concrete tasks within business processes, the information and knowledge transfers which are informal and often run laterally to the specific business processes become transparent.

Information and knowledge interfaces

The method and modeling language of KMDL is used for illustrating information and knowledge transfer relationships in business networks. To meet the demands of the relationships here in question, the concept of information and knowledge interface (IKI) was developed. For this purpose, all knowledge related activities are shown in a model (as seen in Fig. 2). Individual activity with a common receiver are combined into one IKI. The IKI therefore describes the mono-directional transfer of information and knowledge to this receiver.

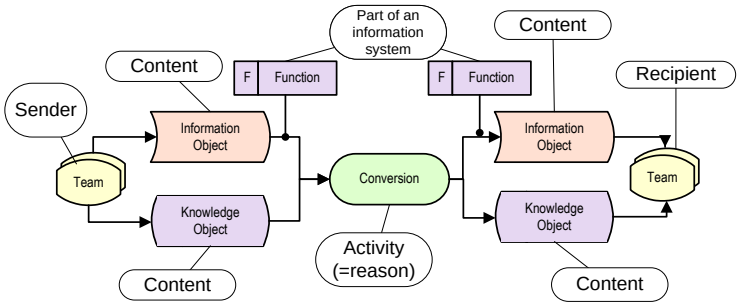

Fig. 2. Individual knowledge activity as elementary component of an IKI

For the specific case of product piracy new assessment and analysis procedures had to be developed. The thereby developed actions are introduced in the method description (Phase 4). The essential difference between the original use of KMDL and this one is the change in the objectives of analysis and evaluation, because the access to flows of information and knowledge is now to be hindered and not facilitated. Further differences exist in the type of questioning. In the process analysis with the goal of improving information and knowledge flow, it is wise to question all of the sides involved. In the case of product piracy this is not possible, because pirates cannot be assumed to give reliable answers. For this reason, the questioning focuses on those parts of an enterprise that are responsible for the transfer of information and knowledge

For the administration of these actors a hierarchical model of actors is used. In this way, the company can be depicted with its departments as well as with its suppliers and customers. By hierarchical depiction of the entire environment and the organization of teams, assertions can be made on type level, as for example the transfer of information to suppliers. By further dividing (refining) supplier relationships, as for example cases where cooperation in development exists with the suppliers and therefore additional information is passed on, specific exceptional cases can be singled out.

CONCEPTION OF AN ANALYSIS AND CONTROL PROCEDURE FOR FLOW OF INFORMATION AND KNOWLEDGE RELEVANT TO PRODUCT PIRACY

The IKI analysis method is described in a procedure model (see Fig. 3.). This procedure is generic and when applied in a company leads to specific IKI models. In the following, the individual steps are explained and supported with examples.

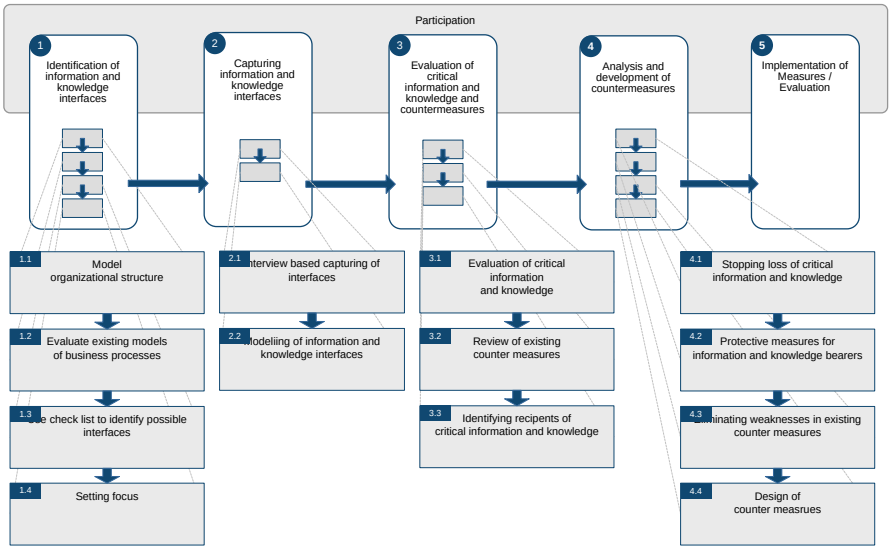

Fig. 3. Procedure model for the analysis and control of information and knowledge flows

In **Phase 1** information and knowledge interfaces of an enterprise are identified. For this purpose, the entire life cycle of a product, from development until it reaches the customer, is taken into consideration. This is assisted by the checklist of the typical classes of receivers. The hierarchical model of actors is developed simultaneously.

In **Phase 2** the actual appraisal of information knowledge transfer per interface occurs. For the actual appraisal, interviews are conducted with the actors on the sender side. "Generalists", such as managers and "specialists" are questioned in detail about the individual interfaces using a semi-standardized questionnaire. Three phases in the life cycle of a relationship between sender and receiver are identified: the phases of initiation, duration and termination of contact. Fig. 4. shows exemplarily modeled sections of interviews, which are combined into an IKI. In the example (Initiation phase) a printed version of a work piece is passed on to a supplier in order to obtain a quote.

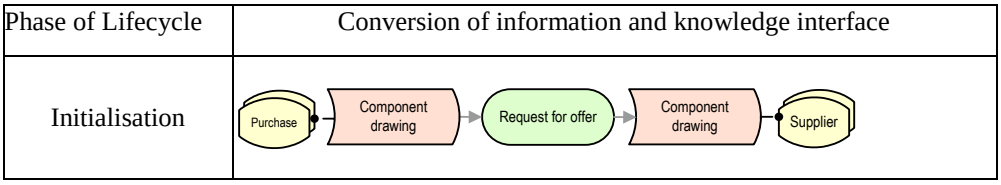

Fig. 4. Example of modeled elements of IKI

The modeled IKI are the basis for the following evaluation in **Phase 3**, the measures of evaluation are:

- The information and knowledge transferred at an interface have differing criticality. The level of **criticality** is established by core know-how, singularity and reproduction relevancy. For each risk factor there exists a series of specific evaluation questions.
- The **existing security concepts** are identified by questions regarding accessibility, copy and reproduction possibilities and traceability of a transfer.

The evaluation is conducted by the actors taking part in a specific action. As this means that actors have to evaluate their personal engagement in an action, the Likert scale is employed for measuring purposes. The scale of assessment has two extreme values: "Completely agree" and "Completely disagree" as well as three evaluation possibilities in between. For the example given above, this means that after the information and knowledge leak is shown in the model (as seen in Fig. 4.), the information and knowledge object is evaluated by a representative of the sender side. Fig. 5. shows the procedure for the evaluation of criticality using the example of the information object "Work piece drawing" specifically for the risk factor reproduction relevancy.

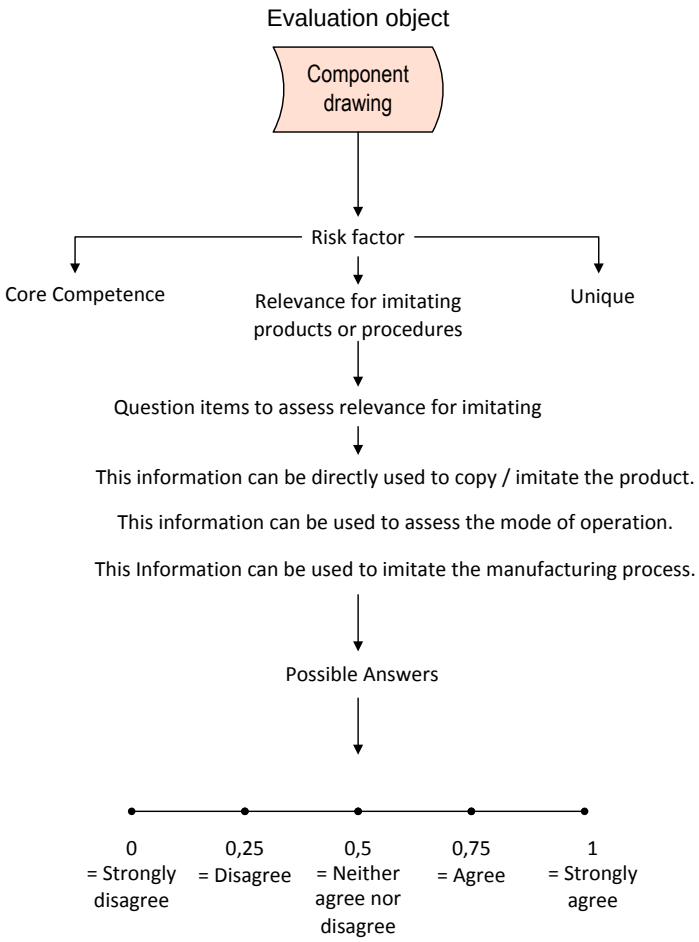

Fig. 5. Example of evaluation of criticality

In the analytical **phase 4** the criticality is established through questions to all three risk factors: know-how, reproduction relevancy and singularity. The aspects worth safeguarding are distinguished with use of the bottom-up list arrived at by this method. When the critical elements regarding product piracy in a company have been identified, those internal or external actors with access to these elements are determined. Therefrom is deduced the relative distance to access of critical know-how. The evaluation is shown in Fig. 6. Receivers are marked in relationship to the critical know-how, to which there is a connection. For our example, the information object "Work piece drawing" was evaluated as highly critical. The receiver "supplier" therefore has access to information which can be classified as corporate secret.

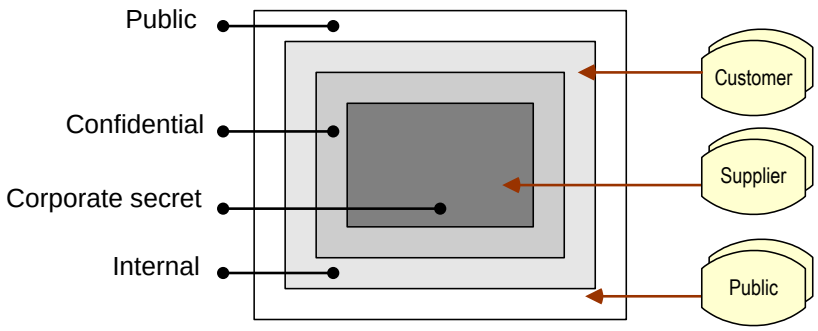

Fig. 6. Interpretation of actor proximity [4]

A polar diagram additionally shows vulnerabilities of individual security concepts based on evaluation questions. It is possible to obtain further insights into deficits by contents and respective to individual information systems.

The proximity analysis serves as the basis from which measures can be deduced. Set-point values are established for the actors on the list, resulting in a list of IKI, which need to be modified to reach set-point proximity. Simultaneously, the security concept can be improved by removing the identified deficits.

As a result, there exists a series of measures regarding the security concept and the modified IKI. To each measure a value indicating the risk reduction can be applied by which implementation can be prioritized in Phase 5. In our example, one solution regarding the information object would be to only pass on excerpts or partially blurred drawings, in order to avoid further copying. Alternatively, the actor related solution could be to only make available drawings to specific suppliers with whom secrecy agreements have been made.

CONCLUSION AND OUTLOOK

Enterprises must meet the challenge given by product piracy with preventative measures. However, since there exists a lack of transparency regarding the flow of information and knowledge, the basis for creating sensible measures is missing. Furthermore, employees often lack understanding of which pieces of content need to be held secret. For this reason, well-meaning but overly general proposals for safeguarding information remain ineffective.

The proposed method leads to a bottom-up analysis of the contents disclosed at intersections and questions these from the perspective of possibilities for product piracy. For this purpose, disclosure of information and knowledge that takes place under regular business activity are taken into consideration. By evaluating criticality of information and knowledge and by reappraising existing security concepts know-how worthy of safeguarding can be identified. Finally, proximity analysis reveals whether individual groups of actors may have more access to critical contents than necessary.

By means of this evaluation, measures are proposed based on the level of risk of product piracy. These serve the design of interfaces in the future and the improvement of security concepts. For instance, carriers of critical know-how can be tied to an enterprise for longer periods as preventative means. For companies, this creates an instrument with which information and knowledge flows can be controlled and measures for the avoidance of leaks can be implemented. A pilot run of the proposed procedure has already taken place in practice. A further development of the proposed method to define the set-point proximity of actors is currently in planning.

Our current research interest focuses on actors that receive knowledge. We are working to develop an indicator based system to identify possible risks, e.g. those with a high probability for the actor to profit from counterfeiting. We expect improvements in the risk calculation by adding this additional information. Furthermore we plan to develop a calculating system that helps to measure which level of secrecy and protection is appropriate.

Even though this work aims at limiting the distribution of information and knowledge, it still contributes to the domain of knowledge management because it provides for protective measures and thus helps enterprises to maintain their competitive advantage through knowledge.

REFERENCES

1. Eppler, M.J. and J. Mengis, The Concept of Information Overload: A Review of Literature from Organization Science, Accounting, Marketing, MIS, and Related Disciplines. Th Information Society, year 20, issue 5, pp. 325-344 (2004)
2. Barboza, D. In: China, Knockoff Cellphones Are a Hit. New York Times 2009, http://www.nytimes.com/2009/04/28/technology/28cell.html
3. OECD. Counterfeitung and Piracy - What we know and what could be done, http://www.oecd.org/dataoecd/11/38/38704571.pdf
4. Neemann, C.W., Methodik zum Schutz gegen Produktimitationen. Shaker, Aachen (2007)
5. Jacobs, L., A.C. Samli, and T. Jedlik, The Nightmare of International Product Piracy. Industrial Marketing Management, issue 30, p. 499-509 (2001)
6. Chaudhry, P. and A. Zimmermann, The Economics of Counterfeit Trade. Springer, Berlin (2009)
7. Fenoff, R.S. and J.M. Wilson. Africa's Counterfeit Pharmaceutical Epidemic: The Road Ahead. 2009, http://www.a-cappp.msu.edu/docs/Africa%20Pharma%20Paper.pdf
8. International Chamber of Commerce. Global Survey on Counterfeitung and Piracy. 2007, http://www.iccwbo.org/uploadedFiles/BASCAP/Pages/BASCAP%20Survey_%20Final%20Report_29%20January07.pdf.
9. Staake, T. and E. Fleisch, Countering Counterfeit Trade. Springer, Berlin (2008)
10. Normann, R. and R. Ramírez, From Value Chain to Value Constellation: Designing Interactive Strategy. Harvard Business Review, year 71, issue 7, p. 65-77 (1993)
11. Hendricksa, K.B., V.R. Singhalb, and J.K. Stratman, The impact of enterprise systems on corporate performance: A study of ERP, SCM, and CRM system implementations. Journal of Operations Management, year 25, issue 1, p. 65-82 (2007)
12. Berrier, E.F.J., Global Patent Costs must be reduced. IDEA: The Journal of Law and Technology, year 36, issue 4, p. 473-511 (1996)
13. Woitsch, R. and D. Karagiannis, Process Oriented Knowledge Management: A Service Based Approach. Journal of Universal Knowledge Management J.UKM, year 11, issue 4, p. 565-588 (2005)
14. Heisig, P., Business Process Oriented Knowledge Management. In: Knowledge Management - Concepts and Best Practices, K. Mertins, P. Heisig, and J. Vorbeck, Editors, p. 15-44. Springer, Berlin (2003)
15. Gronau, N. and E. Weber, Management of Knowledge Intensive Business Processes. In: Business Process Management - Second International Conference, BPM 2004, Potsdam, Germany, June 17-18, 2004. Proceedings J. Desel, B. Pernici, and M. Weske, Editors. p. 163-178. Springer, Berlin (2004)
16. Gronau, N. and E. Weber, Defining an Infrastructure for knowledge intensive Business Processes. In: Proceedings of IKNOW 2004, Graz, Austria. Klaus Tochtermann, Hermann Maurer. p. 424-431 (2004)
17. Fröming, J., N. Gronau, and S. Schmid, Improvement of Software Engineering by Modeling Knowledge-Intensive Business Processes. International Journal of Knowlegde Management (IJKM), year 2, issue 4, p. 32-51 (2006)