Security integration in inter-enterprise business process engineering

Frédérique Biennier
INSA de Lyon – PRISMa, 69 621 Villeurbanne Cédex – France.
Email: biennier@if.insa-lyon.fr

Abstract

New organisational trends as alliances, virtual enterprises or extended enterprises make an heavy use of the information and communication technologies. This involves both the integration of the enterprises "personal" information systems, which exhibits important security requirements, and the definition of dedicated inter-enterprises business processes, respecting each enterprise autonomy and bringing an efficient collaborative framework. Based on actors models, our approach to couple closely a multi-levels workflow description of the distributed business processes and access controls descriptions on the information system so that a global and consistent security policy can be set.

Keywords

Virtual enterprise, security, distributed business process, workflow, PKI.

INTRODUCTION

Networks of firms, alliances and other instances of virtual enterprise organisation consist in a group of complementary or concurrent enterprises, mixed together to achieve a particular short-term, mid-term or long-term project. These virtual enterprises superimpose a new organisation to the enterprises existing own ones and provide a flexible and reactive structure, well adapted to a changing economical environment. In such organisations, the stress is put on inter-enterprises value flows and heavy use of the new information and communication technologies is involved. The Inet tools, as the web technology, favour this vision of an unlimited information space. Nevertheless, technical problems as the interconnection of different information management systems as well as organisational problems remind the limit of a simple "technological integration". Consequently, a particular attention must be paid on the virtual enterprise own organisation.

Inter-organisation business process engineering relies mostly on workflow-based approaches, describing consumer / provider relationships. Well suited to capture inter-enterprise "formal collaboration", these modelling approaches do not take into account "informal collaboration". Crossing the enterprises boundaries, a shared information system is an efficient support for informal collaboration. Nevertheless, it must be organised formally to protect each enterprise own

H. S. Jagdev et al. (eds.), *Collaborative Systems for Production Management*

patrimony. For this purpose, we propose a generic framework based on a SDL description of both workflows and information life cycle management. These specifications are then used to organise a physical collaborative infrastructure. Based on groupware servers, our solution makes heavy use of controlled replication processes and partitioned both the communication network AND the shared information system into several sub-areas (Demilitarised Zone or DMZ). The security architecture, workflow description and authentication constraints are integrated in a common information system. Consequently, access controls are controlled according to both access rights on the information content and on the user authentication based on a Public Key Infrastructure (PKI). The different authentication levels, that may be attached to a PKI signature, are then coupled to the inter-organisational business process specification so that the global workflow can be continuously enriched by integrating the sub-workflows that can be seen only by the concerned enterprise so that the enterprise autonomy requirement is totally fulfilled whereas consistency controls and precise synchronisation can be achieved.

CONTEXT AND REQUIREMENTS

Inter-organisation business process modelling

Built contextually to achieve a particular project or organised according to a long term inter-enterprise collaboration strategy, network of firms, alliances, extended enterprises can be seen as particular instances of the virtual enterprise (VE) paradigm. Each partner can be seen as a particular node, interacting with the other so that the VE organisation can be described as an organisational network [Tidd *et al.* 1997]. In such organisation, a distributed decision system is set, requiring a shared information system with dedicated Information Technology (IT) tools [Malone 1997] as well as inter-enterprise business processes organisation.

Quite different from a classical Business Process Reengineering process, this Distributed Business Process Engineering process involves modelling the inter-enterprise collaboration process. Such models can partly capture inter-enterprise formal coordination thanks to workflow-based descriptions using various methods as IDEFxx as proposed in [Presley *et al.* 2001] or CIMOSA [Bruno & Torchiano 1999]. Nevertheless, these workflow descriptions must take into account each partner' autonomy. Different strategies can be used to solve the multi-level workflow description: for example, [Casati & Discenza 2001] propose a framework including workflow hierarchies and "events management system", whereas [Aalst 2000] proposes a generic framework, based on Petri nets and on message sequence chart, to model and analyse inter-organisational workflows. Nevertheless, these description tools do not provide easily different abstraction level in the workflows descriptions.

Moreover, informal collaboration can not be formalised and modelled directly by such Distributed Business Process approaches but required a flexible and open framework. This can be achieved by providing an open information space where the different actors can freely access or exchange the information they need. For this purpose, CORBA based architecture [Zhang *et al.* 2000] or dedicated distributed frameworks [Sandakly *et al.* 2001] can be used. In such collaborative framework the stress is usually put on actors definition as in the OSSAD system [Nurcan 1998]. Such indirect cooperation can be integrated in a project organization, providing a bounded and generic framework for inter-enterprise collaboration [Volkoff *et al.* 1999]. Then to adapt a modelling framework for such "semi-formalised", open process description, built as "ad hoc" workflow" can be used. In this case, the modelling framework requires reflective and adaptive definitions so that workflows can be refined and extended according to the demand [Edmond & Hofstede 2000]. Nevertheless, the enterprise information patrimony is not taken easily a priori into account by this modelling approach.

Trust, interdependencies and firms relationships

The way the VE information system is organised and managed is heavily coupled to VE internal organisational policy. Distributed among the VE partners, the common information system is not a simple addition of the partners own information systems: it must integrate a consistent security policy to protect each enterprise own system.

Such a strategy involves that each enterprise split its Information System into different areas (enterprise private area, VE area, external area). Pieces of information migrate from one area to the other according to their importance, confidentiality level (enterprise point of view) but also according to the VE goals (used to define the necessary information) and mostly according to the trust and reputation of the partners [Ching *et al.* 1996]. For example, [Tomkins 2001] proposes a typology of un-sharable / sharable information according to the VE internal relationships, collaboration planned duration as well as trust level between partners.

This organisation relies mostly on a contractual definition of the inter-enterprise relationships: as in the generalised EDI approach (with the interchange contracts), the security policy and specially the access rights are well codified in either "VE internal rules" or inter-firms contracts. Of course, such contractual relationships are mostly designed for mid or long term collaboration, i.e. the VE planned duration should be longer than the partnership definition and the contract negotiation phase. This constraint excludes shorter term VE, and specially those supported by e-business and the net-economy. In order to address these e-business VE, [Hoffner *et al.* 2001] proposes to couple a contract enactment infrastructure to the e-business infrastructure. Thanks to "contract templates", the partners can express their own constraints and are guided to generic contracts, quite similar to the EDI interchange ones, defining the "service" (or process organisation) brought by each partner. According to this "contractual" organisation of the VE, the stress is put on the inter-organisation business process and information flows definition, which is quite close to a contractually defined workflow model between the different entities, each entity representing a partner of the VE.

INTER-ENTERPRISE BUSINESS PROCESSES

The inter-enterprise business process engineering specification has to satisfy the opposite goals: respecting each enterprise autonomy and patrimony AND building a consistent super-enterprise organisation which involves a common information system and well defined processes, able to support efficiently both formal and informal collaboration.

As the previously presented approaches do not take into account all those VE business process engineering requirements, we propose here a complementary strategy to organise the VE business process. Based on the VE security policy definition, this approach preserves each enterprise' autonomy and information patrimony and takes also into account both formal and informal collaboration.

Business Process engineering framework

Specifying an organisation involves to take into account how its actors are organised, the role they take in the common goal achievement as well as the way they dynamically adapt the existing structure [Rolland *et al.* 1999]. Depending on the autonomy let to the different actors, two main descriptions can be set: tasks precise specifications can be used for well formalised processes whereas information flows and information access rights are sufficient for less formalised or non formalised exploratory processes. Both of these descriptions are taken into account to build the enterprise own security policy, i.e. defining the way information can be shared and accessed.

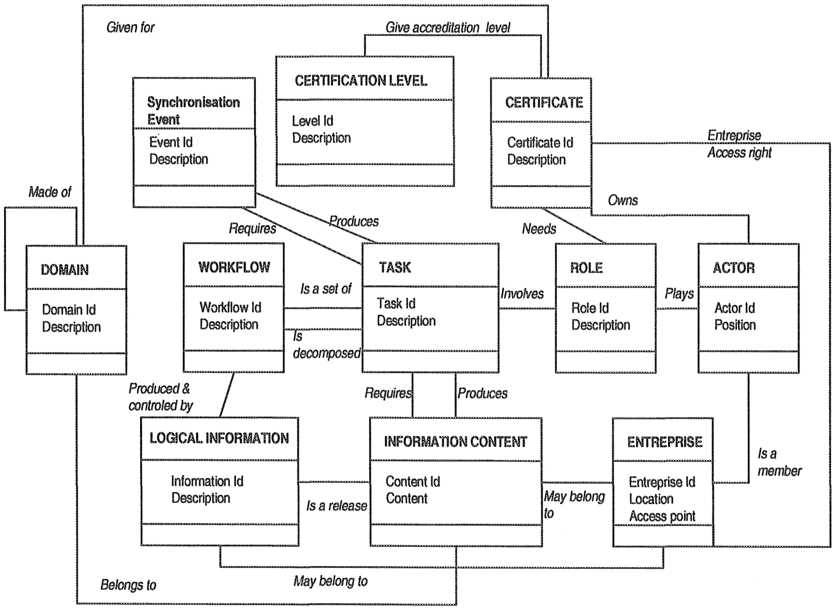

Figure 1 - Information control and business process description data model

As far as a VE organisation is concerned, the main problem consists in federating these security policies. For this, we propose to organise a meta-model shared by the partners, describing globally the distributed business process (Figure 1).This architecture is built around the actor description (person or part of an enterprise). The security policy is defined at two levels: first access controls on informational resources are described, second a multi-areas infrastructure is proposed. By developing adapted replication processes, the access control system represents a convenient basis for the global security system.

The access control system uses a PKI certification architecture coupled to the organisation of access areas on the information system. Access rights are described thanks to "certificates", associated to a set of pieces of information (called domain) and an accreditation level (called a certification level according to the PKI organisation). By this way, for each actor and each requested piece of information access rights can be computed and checked dynamically. The certification process is defined by a workflow controlled by the information Security Officers. Stored on the different authentication servers, cross controls on access rights insure the global consistency of the system.

As far as the distributed business process specification, our description environment includes both the formal and informal process specification. On one hand, formal collaboration can be described precisely thanks to a classical workflow approach. Nevertheless, this inter-enterprise business process organisation must respect the enterprise autonomy constraint. For this purpose, a multi-level workflow description relying on an embedded description of treatments (i.e. providing different abstraction / service levels) and on synchronisation points inside a treatment is necessary. These points have been studied for a long time in telecommunications software development and have lead to the specification and development of graphical and textual tools, as the functional Specification and Description Language (SDL) [CCITT 1985], to organise treatments into services and to define precisely synchronisation between treatments. These description consist into different automata with structured and well defined interactions. Moreover, as SDL provides macro-operations description, abstraction levels can also be integrated in this architecture : depending on the actors they involve, macro operations can be described according to a more precise automaton or, if they involve different actors and responsibilities, they can represent a more precise workflow (Figure 3 presents in a reflexive way the certification process agreement).

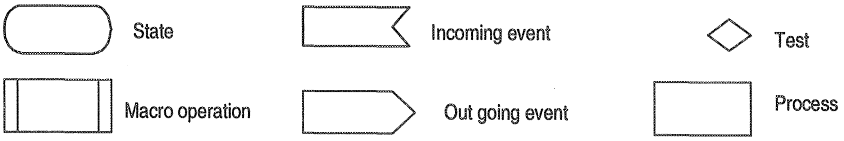

Figure 2 - Main SDL graphical elements

On the other hand, informal collaboration is taken into account thanks to an ad-hoc workflow organisation. Based on the segmentation of the information systems into different domains, this data driven approach, describes the organisation thanks to information flows. To be applied to the business process specification, this involves to take into account the information life cycle to control the business process achievement. For this purpose, we split each par of information into a "logical information" and contents which may evolve according to the information status. Then access rights are devoted to the actors according to the work they should do and to their certification level for the information domain. The global system consistency is provided thanks to:

1. Transaction Processing (TP) based management of the information life-cycle [Biennier *et al.* 1996] controls the information consistency (Figure 4)
2. Workflow organisation of the certification process, stored on each authentication server (see Figure 5) controls the global security policy consistency.

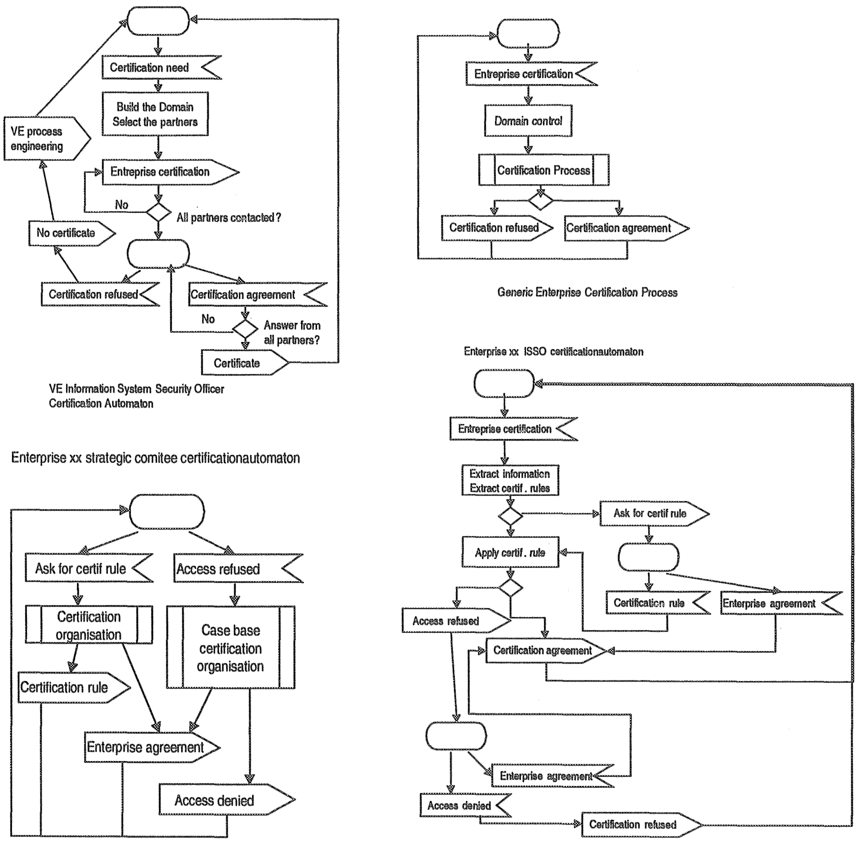

Figure 3 - SDL specification of the distributed certification process

The certification processes are managed by the different Information System Security Officer (ISSO). The VE certification process is built according to a generic model of enterprise validation process. Then for each enterprise certification workflows can be developed. In our example, the enterprise xx certification workflow involves the enterprise ISSO who may apply directly the enterprise certification rules or request a strategic committee for a case-based certification.

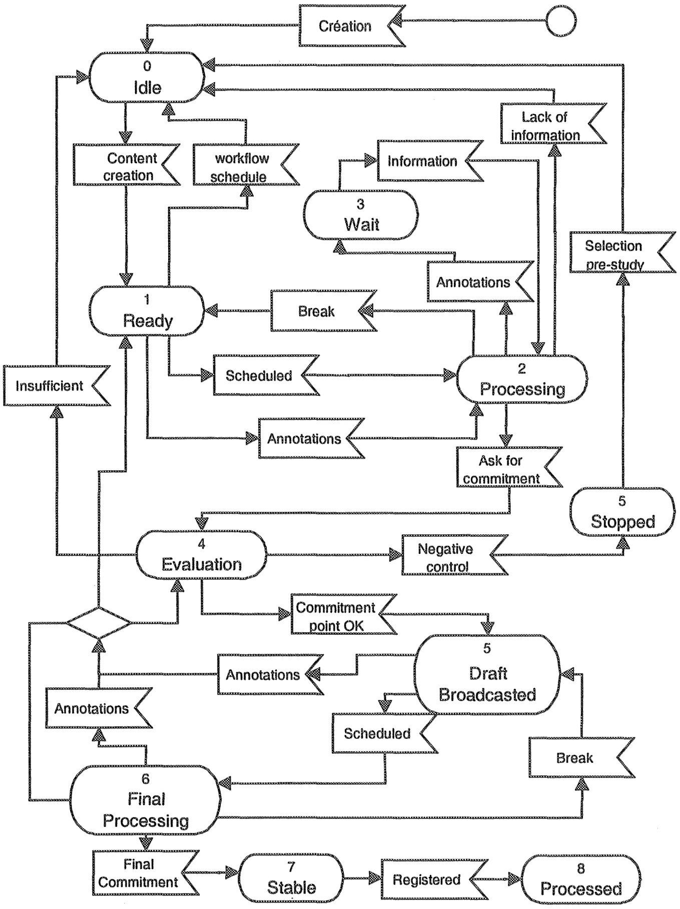

Figure 4 - Information life-cycle

From its creation (idle state), each informational content evolves from stable state to stable state and is controlled by a strict process to certify it. By this way, all the transactional constraints are associated to the information itself instead of the business processes, so that all pieces of information are certified according to the same rules without setting constraints on the enterprise (or inter-enterprise) business processes.

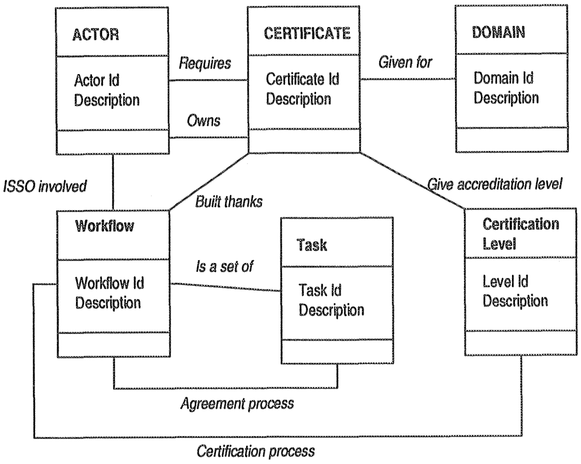

Figure 5 - Data model storing the information validation workflow

Implementation infrastructure for the Security-based organisation

The general security policy defined previously leads to a specific alliance information system. This system is built by extracting convenient information from each partner own information system and transferring it to the actor who needs it. This constraint involves managing an adapted replication system, able to take into account both the formal and informal cooperation as well as an authentication service. The replication control system we propose provides a global protection mechanism on the information system and is quite close to the DCOM access control proposed by [Ahn 2000]: the information is protected thanks to adaptable access rights devoted to the different actors. Flexibility is achieved by a generic replication policy based on import/export mechanism [Biennier *et al.* 1995], similar to those defined in SDL [CCITT 1985] or to the communication channel in ESTELLE [ISO 9074]. First, workflows are used to define how data are exchanged between partners and who is responsible of information at a time, and then a simple replication policy is used: a process is the owner of the information it has to produce. Consequently, when « external data » are needed, they can not be modified directly, the modified data are considered as annotations that are taken into account or not by the owner of the information. This approach is quite close to those introduced in multi-authoring systems [Pinon & Biennier 1991, Vishik 1997] or client and server defined in MMS [ISO 9506] and provides a "task based" access control policy. The authentication servers, managed in each area, register the actors' certificates on the information they manage AND are also used to report the information accesses (Figure 6). Cross-controls between the VE authentication and enterprise server insure the global consistency of the different security policies: by this way, each enterprise can master its own security policy on its own information. By building new certificates, changes in the inter-organisation business process can be reported by all the involved partners.

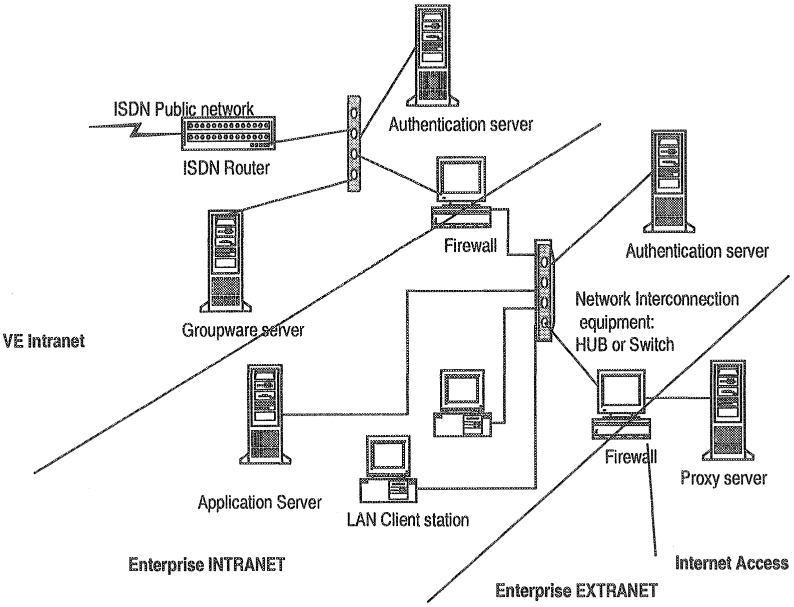

Figure 6 - General infrastructure

By organising the physical network in 3 separate areas the virtual enterprise organisation does not increase risks for the different partners. Moreover, the replication processes associated to the groupware and proxy servers allow each enterprise to define is own security policy.

CONCLUSIONS

Setting a VE consists in defining a new organisation made of entities belonging to concurrent and / or complementary enterprises. This flexible organisation requires a dedicated organisation and particular distributed business processes. We propose a business process engineering support supporting both formal and informal collaboration. Based on the specification and implementation of a global security policy, our framework is built around the actor's specification.

Nevertheless, the distributed processes are built step by step. Further work will study how "organisational patterns", inspired from the information sharing topology proposed by [Tomkins 2001] can be introduced in the actor model so that distributed processes can be designed easily. Then these patterns could be used to guide a Distributed Business Process Re-engineering process by setting different VE collaboration models.

ACKNOWLEDGEMENT

This work is associated to the GRECOPME II project, supported by the Rhône-Alpes area council.

REFERENCES

[1] van der Aalst W., 2000. Loosely coupled interorganizational workflows: modelling and analysing workflows crossing organizational boundaries. Information and management (37). pp. 67 - 75.

[2] Ahn G.J., 2000. Role-based access control in DCOM. Journal of systems architecture (47). pp. 1175 - 1184.

[3] Biennier F., Coquard P., Beuchot G., 1995. Information sharing for synchronous and asynchronous work in concurrent engineering. Concurrent Engineering: Research and Applications 95 proceedings, Technomic. pp. 203 - 214.

[4] Biennier F., Beuchot G., Favrel J., 1996. Integration of the information cycle of life in concurrent engineering. CE'96 proceedings, Technomic. pp. 304 - 311.

[5] Biennier F., Beuchot G., Favrel J. 1998. Tasks vs Data driven organisations in concurrent engineering. CE'98 proceedings, Technomic. pp 545 - 553.

[6] Biennier F., Favrel J., 2001. Secure collaborative information system for enterprise alliances: a workflow based approach. ETFA'01 Proceedings. Vol. 2, pp. 33 - 41.

[7] Bruno G., Torchiano M., 1999. Making CIMOSA operational: the experience with PrimeObjects tool. Computers in industry (40). pp. 279 - 291.

[8] Cassati F., Discenza A., 2001. Modelling and managing interactions among business processes. Journal of systems integration (10). pp. 145 - 168.

[9] CCITT, 1985. Red Book, vol. VI.10, «Language for Description and Functionnal Specification (SDL) », Advices Z.100 to Z.104.

[10] Ching C., Holsapple C.W., Whinston A.B., 1996. Toward IT support for coordination in network organizations. Information & management (30). pp. 179 - 199.

[11] Edmond D., Hofstede A.H.M., 2000. A reflective infrastructure for workflow adaptability. Data and knowledge engineering (34). pp. 271 - 304.

[12] Hoffner Y., Field S., Grefen P., Ludwig H., 2001. Contract driven creation and operation of virtual enterprises. Computer networks (37). pp. 111 - 136.

[13] ISO 9074, ISO/ JTC 1, 1997. ISO/IEC 9074. Information technology - Open Systems Interconnection - Estelle: A formal description technique based on an extended state transition model Amendment 1, 2nd edition. 241 pages.

[14] ISO 9506, ISO/ TC184 / SC 5, 1990. ISO/IEC 9506-1. Industrial automation systems - Manufacturing Message Specification - Part 1: Service definition, 316 pages.

[15] Malone T., 1997. Is empowerment just a fad? Control, decision making, and IT. Sloan Management Review 38 (2). pp. 23 - 35.

[16] Nurcan S., 1998. Analysis and design of co-operative work processes: a framework. Information and software technology (40). pp. 143 - 156.

[17] Pinon J.M., Biennier F., 1991. Systèmes de gestion d'hyperdocuments multimédia. BD'91 proceedings. pp. 162 - 215.

[18] Presley A., Sarkis J., Barnett W., Liles D., 2001. Engineering the virtual enterprise: an architecture-driven approach. The international journal of flexible manufacturing systems (13). pp. 145 - 162. Kluwer academic publishers.

[19] Rolland C., Nurcan S., Grosz G., 1999. Enterprise knowledge development: the process view. Information & management (36). pp. 165 - 184.

[20] Sandakly F., Garcia J., Ferreira P., Poyet P., 2001. Distributed shared memory infrastructure for virtual enterprise in building and construction. Journal of Intelligent manufacturing 12). pp. 199 - 212.

[21] Tidd J., Bessant J., Pavitt K., 1997. Managing innovation. John Wiley and sons.

[22] Tomkins C., 2001. Interdependencies, trust and information in relationships, alliances and networks. Accounting, organizations and society (26). pp. 161 - 191.

[23] Vishik C.M., 1997. Internal information brokering and patterns of usage on corporate Intranets. GROUP'97 proceedings, ACM. pp. 111 - 118.

[24] Volkoff O., Can Y.E., Newson E.F.P., 1999. Leading the development and implementation of collaborative interorganizational systems. Information and management (35). pp. 63 - 75.

[25] Zhang Y.P., Zhang C.C., Wang H.P., 2000. An internet based STEP data exchange framework for virtual enterprises. Computers in industry (41). pp. 51 - 63.