

# A Multi-Agent Model for Secure and Scalable E-Business Transactions

Jacques Calmet<sup>1</sup>, Regine Endsuleit<sup>1</sup> and Pierre Maret<sup>2</sup>

1:University of Karlsruhe (TH), IAKS, 76131 Karlsruhe, Germany  
{calmet, endsuleit}@ira.uka.de

2: LIRIS UMR CNRS 5205, 69621 Villeurbanne Cedex, France  
pierre.maret@insa-lyon.fr

**Abstract.** E-business applications require not only effective security mechanisms but also sufficient system resources to make them fast and reliable. We propose an e-business model that is highly decentralized and robust against attacks. The model is well suited for distributed environments like a Grid and is based on a multi-agent system. This underlying multi-agent system relies upon a fully generic approach called Agent-Oriented Abstraction. This enables to define different needs and requirements of an e-business model that are then assigned to decentralized instances like e.g. an instance supporting contract negotiations. Security features support the agents contributing to this e-business model with regard to legal aspects of their contract negotiations. One such feature is achieved by using so-called agent Alliances. Since an Alliance uses secure multi-party computations an instance that is realized by an Alliance of  $n$  agents is robust against up to  $n/3$ -corrupted members. The main other characteristics of our model are as follows: corporate knowledge is defined through distributed virtual knowledge owned by the agents, the utility of decisions is assessed through a choice of models and trust is achieved through security and legal validation.

*Keywords:* Computational Economics, Agent Societies, Agent-Oriented Abstraction, Corporate Knowledge, Security.

## 1. Introduction

Computational economics are usually based on market mechanisms. The World Wide Web with the adjunction of the multi-agent methodology is gaining widespread acceptance as a medium where the so-called e-technologies can be designed and implemented. This has already changed the way we think about information. Information on the web is distributed, updates are made asynchronously and resources are available both online and offline. This information is however mostly static in the sense that we rely on stored information sources and ontologies. Global networking will similarly drastically change our view of information technology by adding dynamics to distributivity.

A fundamental capability that is required is a semantic broker that dynamically matches user requirements and available resources. While on the web search engines perform this brokering task, in a mobile agent system one has to design an object request broker. Examples are found in Jini (Edwards, 1999) and RETSINA (RETSINA homepage). These approaches have their root in the object-oriented programming paradigm and simulate the well-known CORBA functionalities. There have been some attempts to depart from this methodology such as the functional validation presented in (Jiang and Cybenko, 2004). In this paper we introduce an economic model that is issued from the Agent-Oriented Abstraction (AOA) (Calmet et al, 2004). AOA is a step toward the definition of a new paradigm for multi-agent methodology. It is an abstraction formalism that addresses knowledge and its possible annotations (e.g. ontology, communication and negotiation) together with a decision mechanism based upon the available knowledge and also the utility functions associated to decisions reached. The concept of utility is also annotated to enable the various facets that are available from Pareto optimality or the Nash equilibrium to the mathematical modeling of utility functions. This makes this abstraction suitable for modeling in economy. It

has already been used to model corporate knowledge (Maret and Calmet, 2005). Moreover, it is suitable to define virtual knowledge communities and strict security mechanisms for dynamic and/or mobile distributed systems.

The paper is structured as follows. The next section gives a brief overview of the AOA paradigm. Section 3 surveys the concept of virtual knowledge communities. In section 4 a framework providing security is more extensively described. Then, a sketch of an economic model for distributed systems is presented. We conclude in section 6 with some open problems and on-going works.

## **2. Agent-Oriented Abstraction**

The AOA paradigm covers the concepts of agents, annotated knowledge, utility functions and societies of agents (Calmet et al, 2004). AOA associates to agents the usual features (ability to perceive, reason, act, communicate (Huhn and Stephens, 1999)) and it is compliant with a societal approach of agents. Indeed, AOA is based on Weber's classical theory of Sociology (Weber, 1986). Very briefly, it can be said that Weber states that a society is the result of the actions of individuals.

AOA assumes that agents are entities consisting of both a knowledge component and a decision mechanism system. The knowledge component covers any piece of information available in an enterprise from the technology required to design and produce goods to management decision policy through human relations and internal or external communication. It is partitioned into four components, also called annotations: ontology, communication, cognition and security. An agents decision mechanism system is related to its tasks and goals. It generates utility functions. Utility functions measure the efficiency of the decisions, for instance choosing the next task to execute or choosing a parameter value within a task. Utility functions are structured into classes. The decision-making system is based upon the knowledge component. Agents are then abstractly defined in terms of knowledge and utility. Specializations are made through implementations.

The AOA model extends the abstraction capabilities of the existing Agent-Oriented Programming paradigm (AOP) of Shoham. While AOP does not duplicate what OOP is for programming languages, it is purely a societal approach of the design of MAS relying on a BDI (Belief, Desire, Intention) knowledge approach, AOA does it. In this paper, we are investigating the application of this model as a foundation for an economic model for distributed systems.

## **3. Virtual Knowledge Communities**

One of the main components of the economics of social systems consists of knowledge exchanges. It is not necessary to describe the so-called "knowledge society". Considering a society as a distributed computational paradigm, multi-agent systems can be proposed to address knowledge related issues. Processes tend to make agents produce and exchange knowledge with each other. Virtual knowledge communities (VKCs) are a construct that enables agents that share their common interest in some ontology or knowledge to decide to pool and to collaborate on problems related to this common interest. A more detailed definition can be found in (Maret and Calmet, 2005; Maret et al, 2004). These communities are virtual ones since their duration depends on the persistence of the common interests of some agents to share some of their specific knowledge.

The concept of virtual knowledge communities is a convenient concept for modeling knowledge exchanges within economic systems. It is well suited to filter the amount of knowledge that is

transmitted throughout a society, from nodes to nodes, or from agent to agent. The concept of community (of interest or of practice) is central in the knowledge management area. Examples are (Bonifacio et al, 2002) and (Gordon et al, 2003). It seems that this concept has hardly been addressed in the framework of agent societies and in the economics of it. We notice that individuals, computer systems and even Internet nodes are autonomous and heterogeneous. This is very well suited to agent-oriented systems and modeling. Moreover, relative to traditional approaches, agent-based modeling introduces openness and dynamics, which is highly compatible with knowledge processes. Agent societies therefore constitute the right level of abstraction for modeling and engineering knowledge systems, which are complex, articulated systems.

The concept of a virtual knowledge community is a mean for agents to exchange knowledge. Agents are in charge of tasks within a society, and they are provided with knowledge and decision mechanisms (Agent-Oriented Abstraction approach). We consider that agents have the ability to act as members of knowledge communities. Membership in a knowledge community does not replace the intrinsic goal of an agent for which it was introduced into the society. The concept of virtual knowledge community aims to increase the efficiency with which information is made available. This leads firstly to a more efficient achievement of the goals assigned to the agents, and secondly, provides a learning or data-mining mechanism. Thus, agents ought to be able to create, join, feed, mediate and use knowledge communities dynamically.

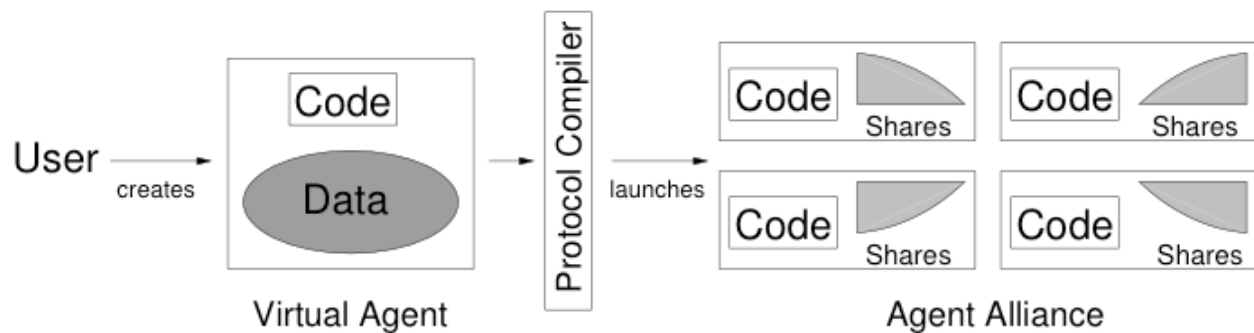
Considering knowledge as a first class issue in the economics of distributed systems, the virtual knowledge community approach sketches a generalization of knowledge exchanges based on the agent paradigm. A last comment is that virtual knowledge communities are well suited to the grid methodology since they can be dynamically created.

## **4.Security in E-Business**

E-business requires strong security mechanisms since on the one hand money and digital signatures are an attractive aim for attacks and on the other hand it is important to create trust in the system. We tackle these challenges by differentiating internal, external and legal security.

### **4.1 Internal Security**

Internal Security is concerned with the protection of the system against threats from inside such as malicious servers and users. In this section we highlight the most important mechanism of our model, the so-called *Secure Mobile Multi-Agent Computations*. This concept of co-operating agent Alliances has been introduced in (Endsuleit and Mie, 2003). The idea has been motivated by the fact that it is very difficult to secure a single mobile agent against threats from its current host or other agents. From cryptography we know protocols for secure multi-party computation (see e.g. (Ben-Or et al, 1988) and (Goldreich and Micali, (1987) for synchronous networks and (Ben-Or et al, 1993) for asynchronous networks). Those protocols allow the robust computation of a function within a group of  $n$  non-trusted parties as long as a specific upper bound of corrupted parties (depending on the protocol) is not exceeded. This property is very useful for mobile agents. Instead of sending a single agent in order to perform a task the originator generates an Alliance of  $n$  agents, which does all necessary computations by following such a protocol. (Endsuleit and Mie, 2003) uses the protocol from (Hirt and Maurer, 2001) which seems to be optimal with a communication and computation complexity of  $O(mn^2)$ .



**Figure 1:** Creation of an Alliance

An Alliance is able to correctly compute a wished function as long as not more than  $t < n/3$  members have been corrupted. In addition, it is guaranteed that all data stay private as long as this upper bound is not exceeded. The latter results from the secret sharing scheme (Shamir, 1979) on which the protocol is based. These properties make agent Alliances suitable to be used in an untrusted environment and especially for VKCs requiring strong security as for instance those, which are responsible for legal security as presented later on.

## 4.2 External Security

External Security in our sense is defined as protection of the system against outside threats. For this kind of security there are satisfying and well-known methods available. Firewalls can be used to protect the system against un-authorized access. Communication is encrypted to prevent an attacker from collecting secrets and from gaining information about the contract negotiations. This can be done with well-known and reliable standards like the secure socket layer (SSL) that allows communication partners to agree on a specific symmetric encryption method (e.g. AES) for their communication session.

To be sure that negotiations take place between the right parties and no man-in-the-middle is able to interfere there should be a possibility to authenticate contract partners temporarily. This can be done by the standard authentication mechanism based on RSA (PGP). Powerful VKCs like the one presented in the next section must always be well authenticated and all messages coming from them must be correctly signed.

## 4.3 Legal Security

E-business includes transactions like building and signing contracts or like accounting in order to achieve valid contract conclusions. For instance buying a stolen item is no legal transaction if one follows most national laws. Even if the purchaser has paid for the item he is not its legal owner. Therefore, a VKC must provide a legal instance whose actions are similar to those of a notary and which on the one hand assures the purchaser that the seller is really authorized to sell the item and on the other hand supports contract negotiation, building and conclusion. This instance might be different for different countries, states or even companies, depending on local law or policies, but it always requires security in order to protect the contract partners. Malicious attacks and software errors are increasing. While industry and government rely more than ever on online information services malicious attacks are very attractive for entities willing to threaten and the con-

sequences of a successful attack are serious. A powerful entity such as a VKC, which is in charge for the negotiations, is a rewarding target for any kind of attack. Therefore, our design follows the principles of VKCs by introducing a VKC that is distributed over some servers and responsible for any kind of legal support for contract negotiations. We call it a *Legal Virtual Knowledge Community* (LVKC).

In order to protect the privacy of contract partners a LVKC must have the possibility to guarantee privacy of the stored data. We propose the use of an agent Alliance (Endsuleit and Mie, 2003; Endsuleit and Wagner, 2004). Using an Alliance to build a legal VKC implies the LVKC to be tolerant against up to  $t$  Byzantine faults while providing privacy of all data. For security reasons the agents must be hosted by different servers. Knowledge, like for instance legal regulations, that is supposed to be public is replicated on each server. Also, there must be an appropriate approach for data replication. We propose to follow (Castro and Liskov, 2002) which offers a non-private replication method. It is very efficient while offering the same guarantee for correctness of the data as the Alliance framework does. Private knowledge such as details about specific contracts is supposed to be kept in  $t$ -shares and computations on this knowledge must follow the model presented in section 4.1.

Shared knowledge can be accessed by any subgroup of  $t+1$  non-faulty agent Alliance members. In addition, it might be necessary to allow other authorized VKCs like the contract partners (probably restricted) access. In principle, one could provide each partner with  $s < t+1$  shares. One partner is supposed to cooperate with at least  $t-s+1$  members of the LVKC to access the information. Unfortunately, this is a high security risk since it is possible that  $t-s+1$  faulty nodes of the LVKC together with a hostile contract partner manipulate the contract. Therefore, we propose to use an additional access control mechanism, which is external in the sense of concerning VKCs outside the LVKC. In case of contract negotiations between  $n$  VKCs one could think of a  $k$ -out-of- $n$  secret sharing that enables arbitrary subgroups of size  $k$  to reconstruct jointly an access key. Also, it is possible to provide some specific contract partners with more authority e.g. more than one share. This could be compared with access control in hospitals in which the chief physician has a higher access authority than a nurse.

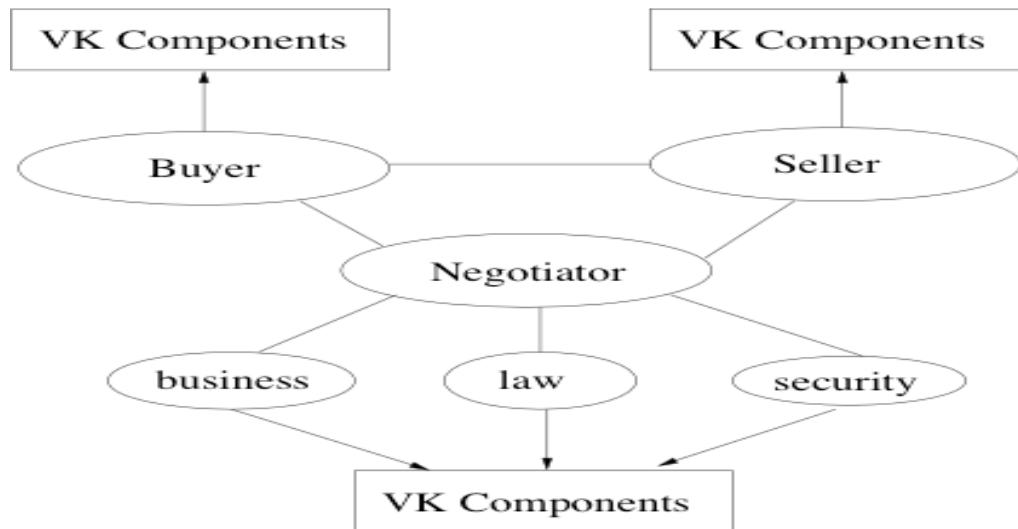
## 5. Business Model Shell

The basic skeleton of e-business on the web is the triple {seller, buyer, and negotiator}. The seller and the buyer are agents with associated ontologies, a catalog and an order list respectively. Whereas, the negotiator checks that the ontologies of the buyer and seller are compatible. We will keep this model but embed it into a much richer and dynamic environment resulting from the AOA paradigm. A preliminary remark is that AOA is set in the context of Weber's approach to sociology. This approach is the one used by (Ekeland, 1998) in a mathematical modeling of micro-economy that generates macro-economy. This is thus a solid foundation. A second remark is that we present a generic model that can be specialized to specific cases. Figure 2 gives an overview of our model. The main components are as follows:

- Corporate knowledge defined through virtual knowledge communities
- Utility of the decisions assessed through a choice of models

- Trust achieved through security and legal validation.

Trust is a pre-requisite for e-business. Indeed, customers are sometimes reluctant to trust the WWW. They will be even more reluctant to trust a dynamic distributed system. Any such economic model must address the mobility of specific resources. We have already proposed a model for corporate knowledge based upon virtual knowledge communities (Maret et al, 2005) and we have implemented it on a web platform (Maret et al, 2004).



**Figure 2:** E-Business Model

In addition, the mechanisms that define a required virtual knowledge community for a specific piece of knowledge provide a brokering system to allocate resources and data as mentioned in the introduction.

In AOA (mobile) agents base their decision on their built-in or externally available knowledge as illustrated in figure 2.

In economy or finance there are a variety of possible assessments of the utility of a decision mechanism. This can be a true mathematical function (although it is so difficult to find such functions that this option is seldom used), a heuristic modeling of the utility, a well-known optimality principle such as Pareto's or Nash equilibrium. Our model enables any of them. The link between “buyer” and “seller” through “negotiator” enables to include virtual knowledge communities which are in charge of legal aspects of (contract) negotiations, security and the transaction itself. The rationale is that decisions affect customers but also customers will affect decision making.

The architecture shown in figure 2 is in fact a shell to generate economic models in distributed systems. Corporate knowledge can indeed be understood as truly corporate knowledge of a company but also as a simulation of a problem in economy. For instance, we might see the corporate knowledge kernel as describing the risk evaluation in an insurance company.

A side remark is that the concept of VKCs can be extended to the concept of virtual organizations. This is possible within our shell since it is necessary and sufficient to redefine the relevant knowledge required by each concept.

## 6. Conclusions

We have outlined a shell architecture generating economic models suited for distributed systems. The main features allowing to state that this shell is suited for such systems are on one side the scope of the security and trust related features and on the other side the mechanisms producing virtual knowledge communities. An aspect has been mentioned but never explicitly described: the concept of trust. This is mandatory to design any system aiming at being used in economy or finance. In our approach trust results from several features:

- Engineering design of the system itself,
- The abstraction paradigm that is available through AOA,
- The security based upon alliances and thus the sharing of data among different agents,
- The legal services available in our environment.

A model of trust has to be formalized. It is relatively straightforward to think of a model based upon the existing technology (both software and hardware). It is much more difficult to assess the different rights that must be enforced, insured and protected such as privacy right. It is known that P2P file sharing is a problem in business; it is lesser known that the legal definition is also a challenge. This is one of the many research problems on our agenda. Another is the fact that trust has features linked to what could be called "common sense reasoning" but then implicit reasoning has been recognized as a contributing factor and is not that easy to formalize. VKCs have to be further investigated and implemented in different frameworks. AOA will be described in more details in forthcoming publications. Then, the link to what is known as ambient intelligence must be investigated. Finally, utility aspects are to be investigated either in the framework (as a resolution algorithm) or in an algebraic setting (as solution of polynomial equations).

## 7. References

Ben-Or, M., Canetti, R. and O. Goldreich (1993); Asynchronous secure computations; Proc. of 25th Symposium on Theory of Computing (STOC) (pp. 52-61)

Ben-Or, M., Goldwasser, S. and A. Wigderson (1988); Completeness theorems for non-cryptographic fault-tolerant distributed computation; Proc. of 20th Symposium on Theory of Computing (STOC) (pp. 1-10)

Bonifacio, M., Bouquet, P. and R. Cuel (2002); Knowledge nodes: the building blocks of a distributed approach to knowledge management; Journal of Universal Computer Science, Vol. 8, No. 6 (pp. 652-661)

Calmet, J., Maret, P. and R. Endsuleit (2004); Agent-oriented abstraction; Revista Real Academia de Ciencias, special volume on Symbolic Computing and Artificial Intelligence, Vol. 98, No. 1 (pp. 77-83)

Castro, M. and B. Liskov (2002); Knowledge nodes: the building blocks of a distributed approach to knowledge management; Journal of Universal Computer Science; Vol. 8, No. 6 (652-661)

Edwards, W.K. (1999); Core Jini; Prentice Hall

Ekeland, I. (1998); La modélisation mathématique en économie; SMF, Gazette des Mathématiciens, Vol.78 (pp. 51-62)

Endsuleit, R. and T. Mie (2003); Secure multi-agent computations; Proc. of Int. Conf. on Security and Management, Vol. 1 (pp. 149-155)

Gordon, M., Fan, W., Rafaeli, S., Wu, H. and N. Farag (2003); The architecture of common knowledge: combining link structure and user actions to support an online community; Int. Journal Electronic Business, Vol. 1, No. 1 (pp.69-82)

Hirt, M. and U. Maurer (2001); Robustness for free in unconditional multi-party computation; Proc. of Advances in Cryptography - CRYPTO 2001, Lecture Notes in Computer Science, Vol. 2139 (pp. 101-118)

Huhn, M.N. and L.M. Stephens (1999); Multiagent systems and societies of agents; Multi-Agent Systems (ed. G. Weiss), MIT Press (pp. 79-120)

Jiang, G. and G. Cybenko (2004); Functional validation in grid computing; Autonomous Agents and Multi-Agent Systems, Vol. 8, No. 2 (pp. 119-130)

Maret, P. and J. Calmet (2005); Corporate Knowledge in Cyberworld; IEICE Trans. Inf. & Syst., vol. E88-D (pp. 880-887)

Maret, P., Hammond, M. and J. Calmet (2004); Virtual knowledge communities for corporate knowledge issues; Proceedings of ESAW 04, LNAI 3451 (pp. 33-44)

RETSINA homepage (2004); <http://www-2.cs.cmu.edu/softagents>

Shamir, A. (1979); How to share a secret; Communications of the ACM, Vol. 22 (pp. 612-613)

Weber, M. (1986); Economy and Society; University of California Press (first edition in 1915).