

# An Agent Framework for Legal Validation of E-Transactions

Jacques Calmet and Regine Endsuleit

University of Karlsruhe, Germany  
{calmet@ira.uka.de, endsuleit@ira.uka.de}

## 1 Introduction

E-business requires trust in business partners and in technologies. The former belongs to the domain of law, the latter to information technology. We propose a methodology based on a high level abstraction of what a multi-agent system is. This methodology and some of its consequences are enumerated in the following sections.

## 2 Methodology of Multiagent Systems

1. Agent-Oriented Abstraction:  
This recently proposed methodology is motivated by a fully abstract view of what an agent system is [2]. It requires to view an agent as made of a knowledge component on which a decision making system can make decisions. This implies a society of agents in agreement with the original work of Weber in sociology [6].
2. A consequence is to be able to organize the knowledge available for a given task into specific knowledge communities [5].
3. To abstract further some concepts, it is possible to filter the knowledge such as to define ontologies. This is achieved by defining a concept of distance based upon entropy [1].

## 3 Security Mechanisms

We propose a three-level security to increase the reliability of a system. On the one hand this is motivated by different classes of possible attacks and on the other hand it allows the system to degrade gracefully.

1. External security:  
This level deals with the protection of a system against outside attacks. The availability of the system, authorization mechanisms and encrypted communication are faced at this level. The first is mainly endangered by Denial-of-Service (DoS) attacks. We are currently investigating a fully new approach to defend against such attacks. For authorization and encryption we rely on existing tools like firewalls and PGP that are satisfactory.

2. Internal security:

Once the external security barrier has been broken, the internal security mechanisms allow identification and elimination of intruders by monitoring the system. At this level also so-called *malicious players* which come from inside the system can be detected. External security does not handle this (internal) problem. Both, intruders as well as malicious players may be active adversaries by influencing the system's behavior (e.g. by disturbing computations) or passive ones that just spy on data to gather information. The latter is hard to find and to fight against. Techniques are emerging in [3] that build an alliance of agents which share their computational state using a protocol for secure multi-party computation. Such an alliance has one common task -like monitoring the system- that is fulfilled in a robust and private way as long as less than one third of them has been corrupted. Powerful capabilities like authentication and authorization mechanisms are not allowed to be concentrated in one single agent. Indeed, one such agent is a bottle neck and leads to inefficiency. Furthermore, it is a visible target to various attacks.

3. Data security:

Even when data is encrypted and software is protected by firewalls, privacy and integrity is not assured. It is possible to investigate encryption mechanisms that are time dependent or better annotated with time to build a system internal security barrier for the protection of data. In addition all data should be signed to guarantee its integrity. Software protection needs more sophisticated methods since it should always be executable. Exemplarily, we mention catchwords like *trusted hardware* which is a topic that caused lots of discussions in the past, and *code obfuscation*.

## 4 An Open Society

The methodologies outlined above lead to an open society. This is the legal requirement of any validation methodology. It is concerned for instance with privacy or property rights. However, there are many practical issues that are not obvious to interconnect with such a generic approach. For instance, the management of Peer-to-Peer systems like [4]. There, protection of privacy rights and free speech could simplify illegal activities that hurt property rights.

## References

1. Jacques Calmet and Anusch Daemi. Identification of ontologies. Submitted.
2. Jacques Calmet, Pierre Maret, and Regine Endsuleit. Agent-oriented abstraction. Submitted.
3. Regine Endsuleit and Thilo Mie. Secure multi-agent computations. In *Proc. of the 2003 Int. Conf. on Security and Management (SAM'03)*, volume 1, pages 149–155. CSREA, 2003.
4. Regine Endsuleit and Arno Wagner. Increasing peer-to-peer file-sharing resistance against legal attacks. submitted.

5. Pierre Maret, Marc Hammond, and Jacques Calmet. Multi agent based virtual knowledge communities for distributed knowledge management. Submitted.
6. Max Weber. *Economy and Society*. University of California Press, 1986.