

Legal aspects of agent technology

M. Apistola², F.M.T. Brazier¹, O. Kubbe¹, A.Oskamp², M.H.M. Schellekens³, M.B. Voulon²

¹ Intelligent Interactive Distributed Systems

Faculty of Sciences, Vrije Universiteit Amsterdam

De Boelelaan 1081A, 1081 HV Amsterdam, the Netherlands

² Computer and Law Institute

Faculty of Law, Vrije Universiteit Amsterdam

De Boelelaan 1105, 1081 HV Amsterdam, the Netherlands

³ The Center for Law, Public Administration and Informatization

Faculty of Law, Tilburg University

Warandelaan 2, 5000 LE Tilburg, the Netherlands

Email: frances@cs.vu.nl, kubbe@cs.vu.nl, a.oskamp@rechten.vu.nl;

m.h.m.schellekens@kub.nl; m.b.voulon@rechten.vu.nl, m.apistola@rechten.vu.nl

1 Introduction

Internet technology is changing society. The physical distribution of services, processes, and data, is no longer necessarily the same as the perceived location. Agent technology has made it possible for autonomous, pro-active digital entities to migrate, communicate, and interact within the digital world of the Internet. These digital entities, most often called software agents, are autonomous and pro-active. They learn from the knowledge they acquire in the course of their lives, and most often know "more" than their original designer or owner within a very limited amount of time. They build profiles of other agents (human and automated), find information, schedule activities, compare and negotiate offers, place orders, make payments, close contracts, et cetera. Although they often represent a specific user, they may also represent an organisation. They often initiate and perform legal transactions.

Legal rules do therefore indicate when technical protection of certain 'resources' is needed. Most rules ask for some form of technical protection. Sometimes, protection is an option open to the owner of the resources: the criminalisation of hacking does not prescribe that you have to protect your system. The system owner may choose to have no protection in place; the consequence is of course that a third party entering the system does not commit the criminal offence of 'hacking'.

The ALIAS project is an explorative project in which legal experts, computer scientists and AI experts aim to increase the understanding of the legal and technical implications of the use of software agents. To this purpose a number of intermediary concepts have been identified: concepts that are of importance to the use of agents within both fields. These concepts, however, have their own meaning within each of the two fields.

This paper consists of the following elements. Section 2 introduces the notion of open and closed systems. Section 3 describes a generic concept model consisting of intermediary concepts, legal concepts and technical concepts of agents. Section 4 analyses a chemical marketplace scenario is analysed, presenting legal and technical issues. The last part of this paper draws conclusions and sketches future work.

2 Open and closed systems

A distinction has been made between open and closed systems to indicate the level of regulation within a system. Within a closed system the data, procedures and actions are well-defined and can be verified. This implies a high level of integrity: it is clear who can do what when and with which information. Hospitals are examples of closed systems. Procedures define which patient data, for example, may be used for which purpose and how. Another clear distinction between open and closed systems is the distinction between the internet (open) and an intranet (closed). There are many examples of legal provisions in which legal consequences are dependent upon the openness and closedness of access to data, or (human or computer) actions or systems. The criminalisation of hacking protects e.g. systems and all data and processes within their perimeter against an attack by unauthorised parties (art. 138a Dutch Criminal Code, hereinafter: DCC). Telecommunications operators have to protect their systems against eavesdroppers (art. 11.3 Telecommunications Act). Other provisions are more closely tailored to the protection of data themselves (instead of protection of the system they reside in). The Dutch Data

Protection Act (hereinafter: DDPA) demands e.g. that personal data are suitably protected against loss or unlawful processing (art. 13 DDPA). Other legal rules do not mention the concept of data, but may nonetheless have far-reaching implications for data. E.g. a medical doctor has to abide to his professional confidentiality (art. 272 DCC). This implies that he may not orally disclose information about the medical status of a patient; it also means that he has to take sufficient security measures to ensure that patient data that are stored in his computer system remain confidential.

From a technical perspective, open and closed systems are based on three important ingredients: the data in the system, the procedures that can be attributed to the data, and the possible actions on these procedures and data, also called tasks. With these three basic ingredients, a closed system requires a model that enforces access control on the data, procedures, and actions that are used by an agent in an organisation. In other words, there are restrictions on the information flows implemented with and within such an organisation. The use of agents within, for example, closed systems for research purposes raises questions with respect to the legal implications. Is it possible that a software agent can access more patient files than, for example, a human agent because a software agent and its environment are closed and thus more controlled.

The legal implications of the use of software agents for such purposes are not fully understood. Notions such as anonymity and privacy acquire new meanings in the digital world. New concepts such as pseudo-anonymity emerge. It is often unclear if existing legislation is applicable, and when. More general legislation with respect to the use of software is available, but there is little tradition, and few accepted procedures, with respect to the use of software agents. An additional complication is the cross-border activities in which agents engage. It is often unclear which legal system is applicable in specific situations. Nevertheless software developers would appreciate knowledge of the implications of their design choices (if only to decrease liability of the user and/or designer of agent systems).

Six very different scenarios have been devised to study both the distinction between open and closed systems, and the factors that need to be considered in a conceptual model such as the one presented in Section 3. The scenarios studied are: a) A grocery scenario in which customers of a grocery shop are assisted by an agent in the collection and payment of goods. b) An email scenario in which agents are used to perform the basic actions of sending and receiving email, but also to enhance this process with additional functionality such as certified mail and encrypted mail. c) A chemical marketplace scenario as described in section 4 of this paper. d) A traffic routing scenario, in which agents are defined on the basis of their specific tasks, e.g. road-based agents, car based agents and highway pricing agents. e) A hospital scenario in which a dossier management agent protects hospital data about patients, a planning agent, and a knowledge management agent that takes care of the distribution of data. f) A civil government scenario that uses agents to organise an ever-increasing body of diverse knowledge with regard to the environment in which citizens live, e.g. a counter assistant agent and labour resource assistants agents.

The traffic routing (d), the hospital (e) and the government (f) scenarios are closed systems. E.g. a doctor assistant agent has, because of the restrictions on information flow in a hospital, a different set of data, procedures and actions that it can perform than, for example, an insurance company agent. In contrast, the grocery (a), the email (b), and chemical marketplace (c) scenarios, have the property that one or more of the ingredients: data, or procedures on data, or actions can be freely accessed. If an agent can freely use one of these aforementioned ingredients, then it is part of an open system. In the chemical marketplace scenario, for example, customers can freely carry out the task of reseller or seller. The chemical marketplace is therefore considered to be an open system.

3 A conceptual model for Law and Computer Science

The intermediary concepts considered in this paper are: autonomy, identity, traceability, integrity, and trust. These concepts are meaningful to both lawyers and computer scientists and are defined as follows:

- **Autonomy**

Autonomy is the ability to act without direct interventions of agents (e.g. humans, software agents, etc.), or processes, and to have control over ones own actions and internal state.

- **Identifiability**

Identifiability is the ability to know a name or other (usual) denominator of an entity.

- Traceability

Traceability is the ability to recover the actions of processes or man.

- Integrity

Integrity encompasses authenticity and originality. Authenticity is the ability to conform to the original, not stained by man or material made causes. In the digital world conforming to the original is rather difficult.

Authenticity for agents should be interpreted to mean that the state of the agent not will be changed by other without agents consent. A method available to ensure this for an agent is to use redundancy in processes that constitute the agent. The processes can then vote on their results and have a guarantee that they are authentic. E.g. triple modular redundancy ([1] A. S. Tanenbaum, M. Steen, van. 2002 , [12] Schneier B 1997) Unfortunately this is best guaranteed when only one of the hosts that run these processes is under the control or influence of the targeted host, otherwise all processes could be changed by this host without the agents detecting this. Another method that is available is that logs are made of the states of the agent. A mathematical function is used to link the successive states in the log in such a way that an external change to the state can be detected or traced back because of a break in the chain of states. E.g. in the Ajanta agent platform such a method is used. ([6] N. Karnik, A. Tripathi 2001).

Originality is the ability to distinguish between original and copy. This also is difficult because in the digital world it is very easy to make copies. With agents, original can be interpreted as being agents under the control of the originator. Detecting a copy is then finding an unauthorised running agent not created by the originator. This means that the originator has to keep an administration of the agents that exist (logging).

- Trust

Trust encompasses reliability, confidentiality, availability, non-excessiveness and safety. Reliability of an agent process means that the process is able to meet its expectations for the total duration of its functional cycle. E.g. reliable communication. Confidentiality (also known as exclusiveness) denotes the ability to limit the availability of private or exclusive content to known authorised parties.

Availability is the ability to have data and processes at ones disposal in such a way that they can be used. Non-excessiveness means that the means are limited to just that that is necessary to meet ones goals. Safety (also known as security) is an encompassing concept for the CIA interests (CIA is an abbreviation for Confidentiality, Integrity and Availability).

3.1 The legal dimension in the conceptual model

The demands that are placed upon agents in the fields of autonomy, identity, traceability, integrity and trust (fig. 1.) are described with two dimensions: legal and technical.

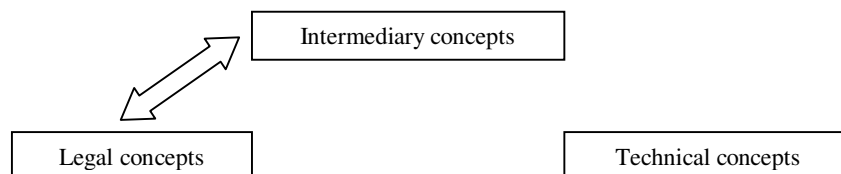


Fig. 1. The relation between the legal concepts and the intermediary concepts

3.2 Relation between intermediary concepts and legal dimension

The legal dimension has the function of making the meaning of the intermediary concepts more precise from a legal perspective. To this purpose a number of important legal fields and legal key concepts have been identified: liability, formation of contract/agreement and evidence. These concepts are not the only concepts that are of importance: 'privacy', for instance, is missing. This set, although limited, illustrates how such general legal concepts play a role in relation to almost all of the intermediate concepts, although at a detailed level their application may differ. The above mentioned scenarios were introduced for this reason: to study how and why these legal concepts relate to specific circumstances

and to understand the links between legal concepts and technical concepts as well as their interaction. Liability, formation of contract/agreement and evidence suffice for the example described in section 4.

Liability plays a prominent role in all phases of a software agent's lifecycle (from design to the end of its active life). Liability considerations may particularly influence design decisions. Liability relates to all of the intermediary concepts. The autonomy of an agent may constitute a liability risk, as it amounts to less control over an agent's behaviour. Identifiability and traceability have a less direct link with liability, unless the provision of identity or traceability is required by some contractual obligation or legal duty. Integrity on the other hand, does have a direct link with liability, since a compromise of the integrity of data or software may directly lead to accidents from which liability flows. Finally, liability may flow from the misuse of trust, unless the trust was light-heartedly placed.

Contract formation is of importance to software agents that closes contracts or agreements. It also has a considerable bordering surface with the intermediary concepts. The autonomy of agents may be of influence to the existence of a contract or agreement. Identifiability and traceability have to a lesser extent, a bearing on the formation of agreements. The integrity is an important consideration since an agreement comes about by an exchange of messages. Any inaccuracy in message exchange may directly influence the contents of the agreement that is to be formed. Trust is also an important dimension, since the willingness to close agreements with the help of agents depends to a high degree on the trust that one places/dares to place in software agents.

Evidence is of importance, because in law, rules about how to materialise ones claims is of equal importance to the rules determining what is materially the position of the parties involved. Autonomy hides the actions of a software agent potentially from the eye of the human beholder/user of the software agent. This may have implications for possibilities to prove afterwards what happened. Identifiability and traceability are prerequisites for proof in law. Integrity and trust have a narrow link with the persuasiveness of evidence.

3.3 The technical dimension in the conceptual model

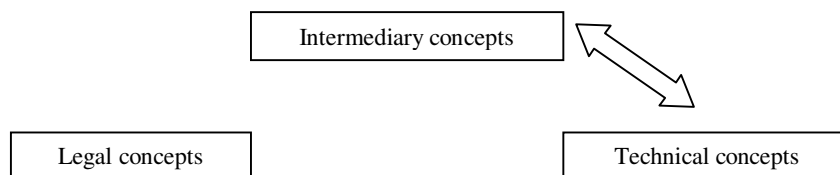


Fig. 2. The relation between the legal concepts and the intermediary concepts

The technical dimension has the function of making the meaning of the intermediary concepts more precise from a technical perspective (fig. 2). A number of technical key concepts are identified: names, protocols, procedures, communication, interaction with the external world, locality, authorisation/permissions, access control, authentication, logs, mobility and thread of control.

Names are important because an agent needs a label in order to exist and interact with its environment. How names are given and where in the system is design dependent.

Protocols are needed to provide the formats for agent communication (e.g. TCP/IP) and object interaction.

Procedures prescribe what an agent needs to do in a specific context to perform a specific task.

Communication refers to the interaction between agents: message passing.

Interaction with the external world refers to the interaction between an agent and its environment: observations and actions., e.g. by means of method invocations of objects.

Locality indicates to the locations of an agent (e.g. on which machine).

Access control, authentication, and authorisation/permissions are three interacting concepts. Access control is the reflection of a policy, authentication refers to the mechanisms that provide access and authorisation, permissions describe the meta-data that determine access rights.

Authorisation and permissions are needed to protect data.

Authentication is needed for an autonomous agent to be able to enter a trusted environment.

In the digital world *logs* are the only means to trace who has done what.

Mobility refers to the concept of migration: an agent decides to migrate to another location (a so-called autonomous mobile agent), its code is “shipped” to another location and reactivated.

The final technical concept identified is *thread of control*: the ability of an agent to have control over its own actions in its environment. Fig. 3 provides an overview of the relations that exist between the intermediary, the legal and technical concepts distinguished.

| Legal Concepts | Intermediary Concepts | Technical concepts |
|----------------------------------|-------------------------------|--|
| Evidence Concluding contracts | Autonomy | Names Protocols Procedures Authorisation/Permissions Thread of control Mobility Authentication Communication Interaction with external world |
| Liability Evidence | Integrity | Names Protocols Procedures Authorisation/permission Access control Logs |
| Liability Evidence | Traceability/ Identifiability | Names Protocols Procedures Authorisation/Permissions Access control Logs Locality Authentication |
| Liability Evidence | Trust | Names Protocols Procedures Access control Authorisation/Permissions Authentication Communication Locality Mobility Logs |

Fig. 3. An overview of the relations that exist between intermediary, legal and technical concepts.

4 Illustration of conceptual model

To illustrate the implications of the conceptual model of one of the open systems described in section 2 is analysed: the chemical auction.

In the chemical commodities market there are no central marketplaces. Vendors of supplies cannot be found easily or have busy agendas and are difficult to contact. Using the Internet, electronic, on-line marketplaces can be constructed. ([13] Sanders, R. 2000¹) An electronic marketplace offers at least a central communication channel through which supply and demand can be matched. This matching can take place in several forms: a ‘blackboard’ ([4] L. Erman, et al. 1980), whereby interested parties match their needs based on advertisements on a publicly available meeting place; a marketplace with (automated) matchmaking through a third party; an auction; and finally through (automated) negotiation.

Chemicality.com is an electronic, on-line auction, in which agents play an important role. The auction is a platform through which buyers and sellers can trade in basic chemical commodities like caustic

¹ <http://www.computable.nl/artikels/archief0/d36ag001.htm>

soda, solvents and acids. Chemicality.com uses a number of ways to facilitate trading in chemical commodities. First, all variables (such as grade, concentration, specs, delivery details) concerning the commodities are standardised. Secondly, both buyers and sellers are screened before they are allowed access to the marketplace. To ensure payment of the seller, credit insurance is offered. Thirdly, all communication is encrypted. In this situation, the auctioneer agent uses a Dutch auction to sell the chemicals to the buyer agents. The mechanism of a Dutch auction works like this: a chemical is up for auction with a maximum price in 'front' of the auction hall filled with buyers (agents). The prices start to drop with a predetermined rate and time interval. A buyer agent who represents the company does a bid when the price is to its liking. The first agent to do this bid acquires the goods, and only has to tell the auctioneer how much it needs. When an agent participates in an auction, it is possible that collectives of buyer agents are formed to bargain for lower prices or for reseller-agents to match the demand of a customer.

In this chemical auction it is necessary to know the user, to be able to close contracts. Since users of agents are bound to the contracts agents close, they will want to have insight into, and control over, the activities of their agents in this field. They will need to know which levels of autonomy are possible and which level of autonomy of his agent (for example which actions can be taken without the owner's explicit consent). The user can, and has to, be able to determine the level of autonomy.

Who the user is, is also relevant with respect to evidence. To recover what happened in the past, logs can be inspected. This raises several questions: What events are logged? Who logs them? Who has access to those logs? How accessible are the logs in the sense that relevant information is easily identifiable? In fig. 3 the party capable of logging is the auction. Transparency and control of the actions of the software agent are thus important. In the following sections, the intermediary concepts as defined in section 3 are applied to the chemical marketplace and the legal and technical implications of each of the intermediary concepts in the chemical marketplace are described.

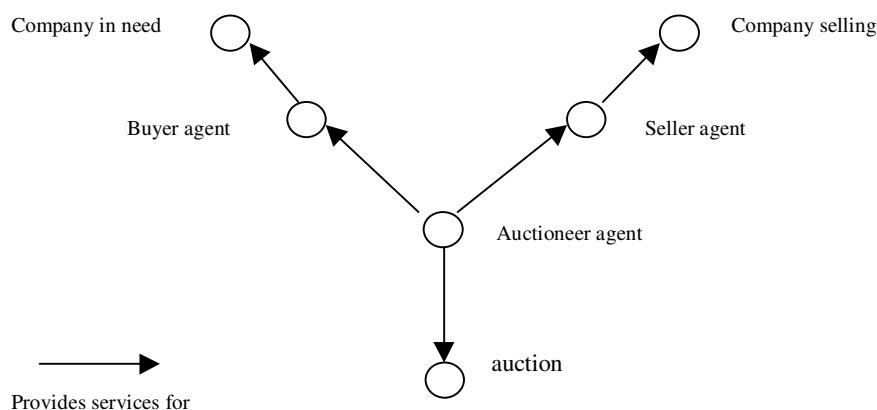


Fig. 4. The relations that parties have to each other in the marketplace.

4.1 Autonomy

- The legal dimension

Close contracts

Contract formation by intelligent agent is subject to debate. ([8] I.R. Kerr 1999,[10]J.F. Lerouge, 1999, and [11]J.E.J Prins, S.J.H. Gijrath, 2000², [9] I.R. Kerr 2001.) A bidder uses a software agent in order to *close contracts*. A bid constitutes legally the acceptance of an offer to close a purchase agreement. Because a bidding agent acts autonomously, i.e. without human intervention, one could ask whether the actions of the bidding agent are suitable to legally bind its user. According to art. 9. Directive on Electronic Commerce³, one may use electronic means to close a contract. From this, may very well be concluded that a software agent can be used to bid and thus bind their users. The fact that a software

² <http://rechten.kub.nl/keybase/>.

³ http://europa.eu.int/eur-lex/en/lif/dat/2000/en_300L0031.html

agent can bind its user, does not mean that there cannot be circumstances in which the user is not bound to the declarations/actions of the agent. Generally, a user will be bound to actions that the agent performs while it stays within the constraints that were given by its user. In Dutch law, the actions of the agent may then namely be considered an expression of the will of the user (compare art. 3:33 Dutch Civil Code)([6] Asser-Hartkamp 4-II 2002). If an agents acts beyond its constraints the user may still be bound to the contract. This effect may be construed in one of two ways. 1. the act is still an expression of the will of the user (which may not very often be the case) or 2. the auctioneer could perceive the act of the agent, conform the meaning that the auction under the circumstances at hand could reasonably attribute to it, as a bid directed by the user to him (art. 3:35 DCC). E.g.: if the auctioneer sees that the bidding agent malfunctions, the auctioneer can no longer trust that a bid by the agent really is a bid and as a consequence, can not make the 'bid' stick to the user.

Evidence

The autonomy of an agent may entail that even the user for whom the agent is active does not know what the agent does or has done. It is therefore wise that an autonomous agent logs its activities, in order to report them (afterwards) to its user. The user of a bidding agent will e.g. want to know to what agreements he is bound. There is, however, no general legal requirement to log, store or write down the agreements one accedes to (which does of course not take away that it very wise to do so). Specifically with respect to providers of information society services art. 11 Directive on Electronic Commerce³ states that a service provider who receives an order through technological means has to acknowledge the receipt of the order without undue delay and by electronic means. This rule, however, does not hold if a contract is concluded exclusively by exchange of electronic mail or by equivalent individual communications. The order and the acknowledgement of receipt are deemed to be received when the parties to whom they are addressed are able to access them.⁴

- The technical dimension

As can be seen in the in fig.4. the auctioneer agent, buyer agent and seller interact with each other. They have a certain degree of autonomy that must be programmed into the agent. This autonomy is constrained by the auctioneer with the actual implementation of the auction room, and the companies sending their mobile agents to attend the auction. To efficiently let the attending agents function the auctioneer most likely will make available a list of requirements/constraints that it uses in the auction. With regard to *names* the auctioneer can, for example, state that it constraints the naming of the agents by giving aliases to all agents in the auction room. The attending companies can conclude that it is not possible for their agents to know up front who the contenders are, and that procedures such that the attending agents autonomously can seek to collaborate before entering the auction is not easily accomplished. With regard to *protocols*, or formats for communication, these will most likely be based on standards such as for example stated by the FIPA organisation and additional custom made protocols created by the auctioneer. E.g. the auctioneer can create ontologies (knowledge modelling concepts), and knowledge representation languages. E.g. XML ([4] E.L Harold 2001), DAML⁵, OIL⁶ ([2] D. Fensel, I. Horrocks, F. Van Harmelen et al. 2000), such that agents can communicate in the setting of chemicals and auctions. On the part of the customers it will be necessary to incorporate these protocols in their agents.

Authorisation and permissions, are determined by the auctioneer who provides the environment. To operate autonomously customers have to acquire these authorisation/permissions and incorporate the appropriate mechanisms to enable their agents to operate autonomously in this respect.

4.1.1 Identifiability and traceability

- The legal dimension

Liability

It can be important to a bidder at an auction other bidders do not know his identity. The auctioneer will probably know the identity of the participants at the auction (he has had them screened). If through a cause attributable to the auctioneer, the identity of a bidder becomes (prematurely) known to other bidders, a liability may exist. If the auctioneer is subject to the contractual obligation not to make the

⁴ Parties who are not consumers may agree otherwise on the topic of acknowledgement and the definition of receipt.

⁵ <http://www.daml.org>

⁶ <http://www.cs.vu.nl/~frankh/abstracts/EKAW00.html>

identities of the bidders known, the liability can be based on breach of contract.⁷ Alternately the liability could be based on the general duty to act with due care: the publication of identity may e.g. under circumstances constitute a breach of privacy.

Evidence

Traceability (in the sense of being able to find out how events unfolded) and identifiability (in the sense that the identity of persons or objects is known or can be found out) is generally an important evidentiary asset. If a dispute arises, one of the first questions that needs clarification is the question about the facts of the dispute: what statements have been made, by whom, to whom, who has done what and when did it occur? In the determination of the facts of a case, a judge or in fact any other arbitrator will use evidence. Of course, do computer data, logs, stored files etc. contain a wealth of information about the facts of an auction dispute. They would in principle make for an almost ideal means of evidence. But can they? In Dutch Law it is reassuring to know that in principle everything can act as a means of evidence (compare art. 179 Dutch Code of Civil Procedure). A judge does not have to decide on the admissibility of evidence.

- The technical dimension

In order for an agent to enter an auction, it is clear that all customer agents need to know the auctioneer agent. In this case the identity is static, the name will not change. However, as stated in the previous section, the names used for the customers are aliases assigned by the auctioneer. Agents can leave and enter when they like. This means that the aliases are dynamically assigned. To achieve identifiability in the marketplace, the auction needs a naming service, and the customer agents need a mechanism to recognise their assigned aliases, and probably be able to pro-actively identify themselves with these aliases.

Traceability is associated with the technical concepts: names, logs, protocols, procedures, locality, access control, authentication and authorisation/permissions. Names are an obvious needed in order to be able to address the agents in the auction. Logs are a needed to backtrack the actions of an agent and other processes. These logs should possibly be append-only, secure and include timestamps. In the chemical auction, it is likely that the communicative acts that are used in the bidding process are logged. Locality indicates where an agent and other processes are situated (e.g. which machine) If the auctioneer uses a single host for the auction this is clear. However, if the auction consists of multiple host, knowing where an agent is becomes more difficult to trace for the owner of an agent attending the auction. The routes that agents follow in the network and machines of the auction can be of interest.

4.1.2 Integrity

- The legal dimension

Liability

The integrity of software agents, the auction environment and the data they process is essential for the correct performance of the 'market'. The fairness of the bidding process, the determination of the securing bid, the determination of the modalities of the contract (who bought what quantity of what substance from whom against which price?) all are highly dependent on the technical integrity of systems, software and data.

Evidence

As stated by Dutch law everything (including electronic records) can act as a means of evidence. There is, however, a catch: a judge is free in his/her evaluation of the evidence. ([2] Dijksterhuis-Wieten 1998) It is up to him/her to decide, if, and to what extent, a piece of evidence 'convinces' him/her of the facts to be proved. In this respect computer data have a weakness: they can be easily manipulated, deleted, created etc. Therefore a judge will treat 'computer evidence' with some care. For the people who have to rely on computer-generated evidence (e.g. a party in an e-commerce dispute) the evidential consequences of the manipulatory nature of computer data is beyond their control. Many measures can be taken that increase the capacity of computer data in convincing third parties, such as

⁷ He might perhaps even be under a contractual obligation to have – according to customary standards - enough security in place to prevent third parties from accessing the information.

judges. A relying party may take care that it has a clear policy in place about the storage of information (what is stored by whom and for how long), it may take technical measures such as storage on a WORM (Write Once Read Many) medium, working with acknowledgements of receipt, using digital signatures, up-to-date protection against hackers etc. Integrity does not only mean that information that is available is correct, the information must also be complete. An uninterrupted trace of logs will enhance the trust that the logs are integer. The better the integrity of logs can be ensured, the larger the evidentiary value will be.

- The technical dimension

As is stated in section 3 integrity encompasses authenticity and originality. Now in the chemical marketplace these requirements are possible to meet, because of the transactional nature of the auction: there are at least two communicating parties needed to close a contract. A possible solution would be that the agent gives the auctioneer a challenge that is given by the owner. In order to start a transaction the auction should use this challenge with the owner of the agent in order to verify that this agent is an authorised copy. This challenge-response protocol should be well known, because these protocols are best tested with regard to the guarantee that impersonation is not possible while performing the challenge. As can be seen achieving real integrity requires a careful design of the auction, and can have major repercussion on performance and cost. In practice the trust and additional guarantees given (e.g. like used with credit cards) that parties have can possibly relax the requirements for the design of the auction place.

4.1.3 Trust

- The legal dimension

Liability

Users may lose trust in agents, if ‘accidents’ happen because of imperfections in the interoperability between software agents and the auction-environment. A possible liability following such accidents can be based on breach of contract, if there is a contract between the user and the auctioneer, the contract contains an obligation for the auctioneer concerning the interoperability and the auctioneer did not abide to this obligation, thus causing the damage. A tortious liability may also exist. This requires inter alia that negligence on the part of the auctioneer can be established. Non-adherence to agent standards or non-adherence to interoperability standards (if existent) may in itself not be enough to establish negligence. ([14]C. Stuurman 1995) It may, however, constitute a indication for negligence.

Evidence

Reliability of logging/storage of information with evidentiary value ensures that the information is available when needed. Especially, if the auctioneer provides the users with their bidding agents, the trust that the users have may increase if logs pertinent to the actions of their agents are available for them and not just for the auctioneer.

- The technical dimension

As said before in this example the names on the market are assigned by the auctioneer. The auctioneer has an instrument to protect the trust in the auction. On the one hand this guarantees that all agents in the market are only possible buyers or resellers, on the other had it guarantees the confidentiality of the agents. Because of the fact that the auctioneer agents have procedures to assign names to agents it also can enforce access control onto what an agent can do in the trusted environment. The authorisation/permissions that the auctioneer assigns to an agent regulates who can enter the trust relationships of the auction. The auctioneer thus has to provide a specification of the authentication methods the auction uses to enable agents to enter the auction. The bidding process (in this case the Dutch auction) has to be performed according to protocols and procedures, if the auctioneer does conform to well known protocols and procedures, it will also increase the trust that the customers have. Because the auction is closed the communications can be monitored and contained to the auction room by the auctioneer, thus being private with respect to the outside world. The auctioneer provides the communication facilities in the auction. By doing this the auctioneer can provide a reliable communications infrastructure, so it is sure that an agent receives the communication it was sent. The way the auction is organised means that the customer agents place a lot of trust in the correct workings of the auction. Therefore, the auction should store the communicative acts, and tasks the auction agent

can make. The auction should provide a public policy on how these logs are made, managed and stored. This provides insight into the decisions of the auctioneer onto how, what and why it logs. The customers can make their own decisions about how trustworthy the auction is and engage in the auctioning process.

5 Conclusions and future work

This paper presents a conceptual model with which a large number of technical and legal implications of the use of software agents can be analysed. An example scenario of an open system with closed elements, namely a chemical marketplace, has been used to illustrate its use. It is clear that the scope of the framework can be broadened to include more legal and technical concepts: this is currently subject of research. Current research questions include: does the framework provide insight in the fields involved? Will it provide enough support in the design of a “cookbook” for software designers in which the legal implications of design choices are made clear? Will it provide support in defining areas in which legislation is missing, and possibly needed? One of the platforms in which these questions will be addressed is the website <http://www.iids.nl/alias>. All input is valued.

References

- [1] A.S. Tanenbaum, M. Steen, van. (2002), *Distributed Systems principles and paradigms*. p. 367 Prentice Hall Inc. New Jersey. ISBN 0-13-088893-1.
- [2] H.L.G. Dijksterhuis-Wieten (1998), *Bewijsrecht in civiele procedures*, Deventer: Kluwer, p. 16 – 18.
- [3] D. Fensel. I. Horrocks, F. Van Harmelen et all. (2000) OIL in a nutshell, *Proceedings of the 12th European Workshop on Knowledge Acquisition, Modeling, and Management (EKAW'00)* editor R. Dieng, Lecture Notes in Artificial Intelligence p.1-16 Springer-Verlag, Berlin.
- [4] L. Erman., F. Hayes-Roth, V.R. Lesser et all. (1980), The HEARSAY II speech understanding system: Integrating knowledge to resolve uncertainty. *Computing Surveys* 12(2), p. 213-253.
- [5] E. R. Harold. (2001), *The XML Bible* 2nd edition Hungry Minds, Inc; ISBN: 0764547607.
- [6] A.S. Hartkamp, mr. C. Asser (2001), *Handleiding tot de beoefening van het burgerlijk recht, Verbintenissenrecht, Algemene leer der overeenkomsten*, Deventer: W.E.J. Tjeenk Willink, p. 92 – 126
- [7] N. Karnik, A. Tripathi (2001), Security in the Ajanta Mobile Agent System, *Software Practice & Experience* vol. 31, no. 4. p. 301-329, Apr. 2001.
- [8] I.R. Kerr (2001) Ensuring the success of contract formation in agent-mediated electronic commerce, in: *Electronic commerce Research*, 1: Kluwer Academic Publishers, p. 183 - 202.
- [9] I.R. Kerr (1999), Spirits in the Material World: Intelligent Agents as Intermediaries in Electronic Commerce, *Dalhousie Law Journal* 1999, p. 190-248.
- [10] J.F. Lerouge (1999), Uniform Computer Information Transaction Act: The Use of Electronic Agents Questioned under Contractual Law: Suggested Solutions on a European and American Level, *The John Marshall Journal of Computer & Information Law*, p. 403-432.
- [11] J.E.J Prins, S.J.H. Gijrath (2000), *Privaatrechtelijk aspecten van elektronische handel: Juridische aandachtspunten voor Internet Service Providers*. Studiepockets privaatrecht nr. 61. Deventer: Tjeenk Willink.
- [12] F. B. Schneider.(1997) Towards Fault-tolerant and Secure Agency. Invited paper, in *Proceedings 11th International Workshop on Distributed Algorithms*, Saarbrücken, Germany, Sept. 1997 Also available as TR94-1568, Computer Science Department, Cornell University, Ithaca, New York
- [13] R. Sanders (2000). *Goedkoop grossieren* Computable 8 september 2000, nr 36, p. 33.
- [14] C. Stuurman (1995), *Technische normen en het recht* (diss. VU), p. 267.
- [15] M. Wooldridge, N.R. Jennings, (eds.) (1995) *Intelligent Agents*, Lecture Notes in Artificial Intelligence, Vol. 890, Springer Verlag, Berlin.