Agent-facilitated Trust Building in the SEEM Infrastructure

Z. Ren, T.M. Hassan, C.D. Carter & C. J. Anumba
Department of Civil and Building Engineering, Loughborough University, Loughborough, UK

ABSTRACT: This paper presents an agent-based trust building approach developed for the Single Electronic European Market (SEEM). Intelligent agents, embedded in the distributed SEEM registry and repository nodes, SEEM Certification Authority (SCA), Trust Third Parties (TTPs) and external Certification Authorities (CAs) are adopted to collaboratively seek the trust related information of a potential partner such as user certificate and conformance information, as well as registry information.

1 INTRODUCTION

The EU sponsored SEEMseed project (Study, Evaluate, and Explore in the Domain of the Single Electronic European Market, IST-1-502515-STP, URL1) is undertaking policy orientated research within the field of the Single Electronic European Market (SEEM), with a focus on registries and repositories. A major objective of the project is to develop an experimental infrastructure for the SEEM that can be used throughout Europe (and beyond) and is compatible with other similar initiatives. The core infrastructure focus is an intelligent and distributed registry service that is able to provide all the necessary information to set up, run and terminate eBusiness interoperations along pan-European supply chains.

By definition, SEEM should offer a collaborative model to implement the exchange of information between its actors. Typical services of the SEEM Registry and Repository (RR) includes:

- company information support;
- person information support;
- product and service information support;
- business process monitoring support;
- business messages support;
- document specification support;
- business agreements support; and
- technical agreement support.

According to the SEEM user requirements report (D2.1), security and trust are two key aspects of the SEEM framework. The following three points illustrate these issues from the SEEMseed perspective, with further details available in D2.2.

- Firstly, in an open and dynamic environment, trust is a fundamental issue to enable companies to conduct commerce and collaboration. This requires various types of information that can be part of the trust profile of a company, and this information may vary depending on the type of relationship. Two kinds of information are essential: 1) basic user information: name, address (e.g. address types, country and region), company identifiers, contacts, means of contact, banking account and dealing, tax scheme information, legal registration information, currency information, categorisation of the company, description of the activities of the company, preferred language, relationships between companies. Such information is essential to identify an individual user; 2) user conformance information: attitude, expertise, quality of service, previous projects, client satisfaction, etc. Such information is used to address a user's service or professional performance for trust building.
- Secondly, the SEEM Registry and Repository Network (SRRN) should be able to store – in a secure and trustworthy way – all users' information; because it has to be digitally signed, users will consider it to be valid. The access policies of the SRRN will allow users to gain access to specific information, and can even specify the period of time that they are allowed to access it.
- Thirdly, to obtain more specific information about a company, it will sometimes be necessary for a trusted third party to evaluate the information and recommend or oppose the use of

services from a certain company. The SRRN will provide an algorithm to facilitate the information access from the SEEM registry to the trusted third party actors.

To adhere to the SEEM principles, the registry and repository possesses the following features and benefits:

- *No central control*: Users are left to their own devices, but have the support of trusted third parties when needed;
- *Open confidence*: The SRRN is secure and can be trusted, yet is open enough for all to participate in it freely at the layer they require;
- *Accountability*: The establishment of secured checksums, access control and authentication means that all parties are full accountable;
- *Privacy of Content*: The content, where required, continues to be private between relevant parties: and
- *Enhanced Reliability* – for example, the use of notification services on the registry allows participants to actively monitor the status of any process. If necessary the content can be replicated (whilst still secure and identified) to prevent any down time issues.

This paper presents a conceptual model in which multi-agent systems are used to facilitate trust building in the SRRN services.[1] Although these agents are designed to facilitate the complete trust-building lifecycle – from initial trust building, to monitoring of the collaboration process and finally reputation building and evaluation – this paper focuses on the agents' role in initial trust building through ensuring the credibility of the SEEM users in the distributed RR nodes, SEEM Credibility Authority (SCA) and TTPs.

2 THE SEEM INFRASTRUCTURE

2.1 The SEEM RR Infrastructure

To fulfil the needs of the SEEMseed project, and the realisation of the registry and the interfaces, the infrastructure has been divided into five different layers: user layer, application layer, registry and repository (RR) service layer, core registry layer and core repository layer (Figure 1). Of these, the RR service, core registry and core repository layers are the critical focus of the SEEMseed project. These generic components are referred to as the SEEM Registry and Repository Network and their focus is to serve and be served by information content, which can be stored and indexed.

[1] This paper is a tentative research study based on the SEEMseed infrastructure rather than fully comply with the infrastructure.

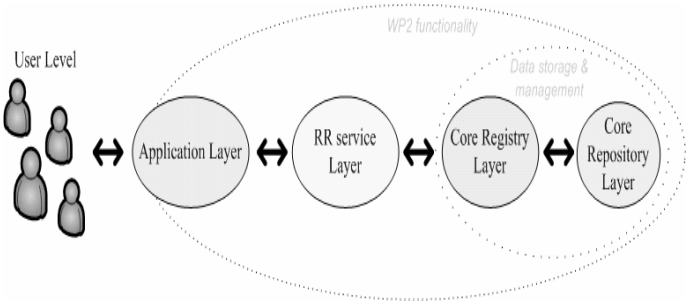

Figure 1. The layered structure of the SEEM (D2.1)

1) User and Application Layer

The user layer is a representation of all SEEMseed Users. The application layer contains applications and user interfaces to allow users to communication with the RR services layer. This can be an application running on a mobile device or a web site to enable access to the SEEM. From the RR service point of view, the high-level functions of this layer are:

- Formulate queries for company information and document retrieval;
- Receive and interpret information; and
- Formulate commands to store company information and documents.

2) Registry and Repository Service Layer

This layer is responsible for managing all kinds of registry logic, such as managing notifications and document types. It is an interface that allows the applications to access the information registered and stored in the registry in a homogeneous way. The scope of the functionality of the Registry Services Layer is constrained by the possibilities that the Core Registry Layer offers to it, and by the information model offered by the core itself. The functionality of the Services Layer has to be independent of any specific business framework specification. The RR services layer offers the external applications a high-level interface to access the contents of the registry and repository in order to:

- Query the SRRN for desired information;
- Manage information in a secure way, and make it available to authorised users;
- Allow users to specify 'alarms' that inform them when the information changes;
- Add, update, delete, and edit information on the registry;
- Categorise and associate the data in the registry so that users can find and use it; and
- Log the operations made at the registry.

3) Core Registry Layer

This layer is strongly connected to the Core Repository Layer. These layers are the key components of the SEEM's data storage and management system. The Core Registry Layer manages data distribution and access. It works as an access point to the global

registry network and offers functionalities to quickly find stored information, which can be located in different repositories distributed over the Internet. This layer therefore implements an indexing system and offers some basic queries to retrieve stored data by forwarding queries to repositories and other registries. This layer is content neutral. Once receiving a query from the RR Services Layer, the registry layer will forward it to the Repositories, connected to the Core Registry Layer, which will perform a search based on the query.

One of the main issues of the registry layer is the distribution of the registry. It takes care of the knowledge base for all repositories in the network and their suitability for specific kinds of information storage or retrieval. A core registry node needs to connect to other SEEM registry nodes and queries them as well. Those registry nodes might have more nodes that they are connected to. All core registry nodes are connected in a peer-to-peer arrangement. Each SEEM core registry layer instance (peer) has a list of other instances. Once a query is received, it is forwarded to all known peers, which will then forward the query to the peers that they are connected to. They then collects the search results (if there are any) and sends them back to the peer that originally sent out the query. If there are no results this information is also returned, thereby reducing the timeout effects.

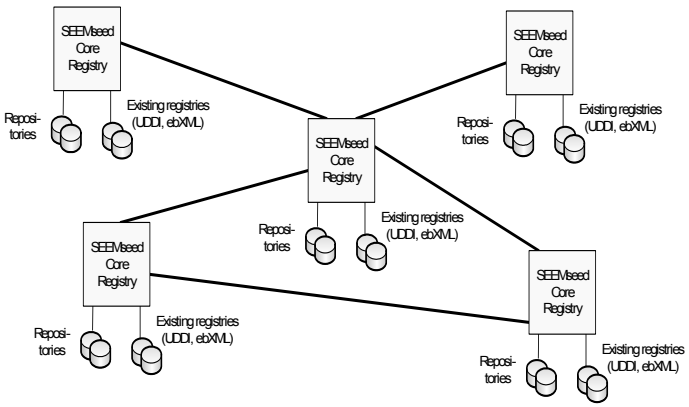

Figure 2. Connection of multiple SEEM core registries

4) *Core Repository Layer*

The core repository layer is responsible for storing documents and other entries and for retrieving them by performing queries received by the core registry layer. The primary goal of Repository Layer is to provide the storage functionality for the SEEM registry infrastructure. The high-level functionalities are:

- Store and serve all information used in the SEEM environment (e.g. schema, templates and instances of company information, business processes and documents, technical profiles, agreements, services, product information, etc.);
- Support different taxonomies and classifications;
- Store and serve metadata information;
- Support data versioning; and
- Security – providing access control and information privacy.

By implication, the layered structure implies a sequential flow of information from the user to the core repository layer. Each layer will thus receive requests, process them, possibly issue and wait for requests to be processed from the next layer, and ultimately return information to the calling layer.

2.2 Distributed Registry and Repository Nodes

Each SEEM implementation is a series of single components that are joined together in a serial manner. However, the reality is that there will be many instances realised of each layer, and each layers may use or know about only certain other layers. In other words, each layer should not be perceived as a single application, which can be implemented as many nodes with similar functionality. These nodes could be hosted by different service providers. The nodes can be linked and work together.

In addition, nodes in the same layer could be content or service specific. For example:

- There may be core repositories A,B,C…, of which A and B are generic (hosting any kind of information), whilst C only hosts company information,
- A core registry instance X may only know about A and B directly, but may be linked to another core registry instance Y, which may know about A and C, but not B;
- A RR Service instance P is implemented such that it only 'cares' about company related searches. It interfaces to registry X and another registry Z, which also knows about A and C but not B.

The distributed registry and repository nodes create a very flexible and comprehensive system in terms of how users are registered and how information is accessed and stored. However, with flexibility comes complexity. How to obtain users' information for trust building efficiently is a major technical problem.

3 TRUST FRAMEWORK IN THE SEEM

3.1 Theoretical Background

Trust building in the SEEM involves many different aspects. Although the SEEM trust building should consider the overall lifecycle of eBusiness conducted in the e-market, the SEEMseed project mainly focuses on the initial trust building. A trust building framework has been developed (Figure 3).

McKnight and Chervany (1996) identified three major trust types: dispositional, institutional and trusting beliefs. Trusting beliefs means that 'one believes that the other party has one or more characteristics beneficial to oneself'. It reflects the idea that interactions between people, and cognitive-emotional reactions to such interactions, determine behaviour.

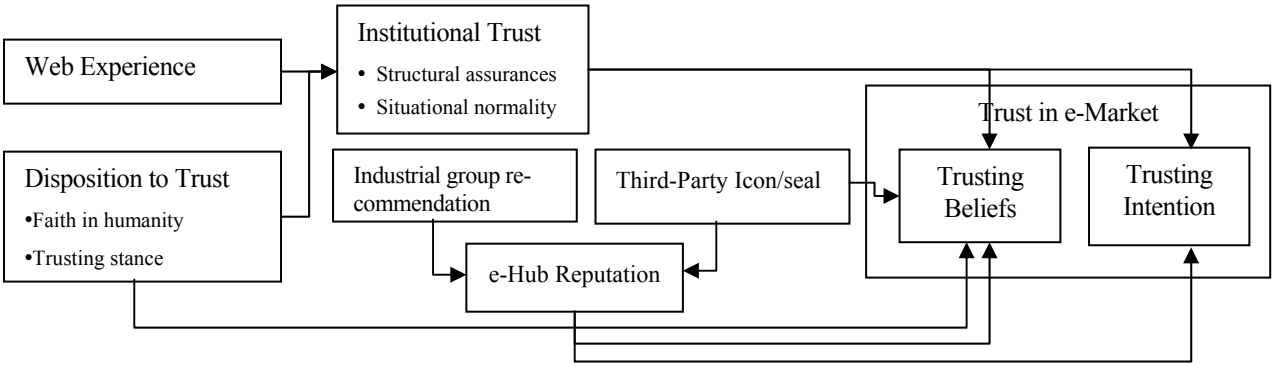

Figure 3. Conceptual trust building model for exploration stage (adapted from McKnight *et al*., 1998)

There are four types of trusting beliefs:

- *Competence* means that one believes that the other party has the ability or power to do for one what one needs done.
- *Benevolence* means that one believes that the other party cares about one and is motivated to act in one's interest.
- *Integrity* means that one believes that the other party makes good-faith agreements, tells the truth, acts ethically and fulfils promises.
- *Predictability* means that one believes the other party's actions are consistent enough that one can forecast them in a given situation.

These four aspects are essential for initial trust building. Ren *et al*. (2005) discuss the SEEM trust building in terms of technological, business and social infrastructure. This paper focuses on the users' trust relevant information during the registration process.

3.2 Trust Information in SEEM Registry

In any environment where a degree of conformance is required, and especially for those that are based on trust mechanisms, there are a series of requirements placed upon the parties and a series of expectations if these requirements are not fulfilled. SEEM works as an 'open club' or a 'community', where there are no onerous membership conditions, but users are expected to know and fulfil the rules and statues; otherwise it impacts the benefits of the club for the other members. Two kinds of information essential for trust building in the SEEM registry process are:

- *Identification of parties*: Identity can be proven through PKI techniques, but these still rely on the correct identification of a party in the first place. A digital certificate is required for each SEEM user to identify each participant. A digital certificate is an electronic piece of information proving the ownership of a public key by the entity. This identification will allow access control at every level. Additional registry information allows service personalisation and thus more efficient configuration and adaptation of services.

  The SEEM Certification Authority (SCA) could issue, revoke and manage certificates to be used by SEEM users. It also issues web server certificates and publishes Certificate Revocation Lists. Since many users also have non-SEEM identification, it is particularly important for the SEEM infrastructure to cope with this. In the case of accepting certificates from other TTPs or CAs, in order to be identified by the SEEM infrastructure, the attributes of the certificate should satisfy the requirements of the SEEM. TTPs or CAs can issue certificates if they follow the rules identified and authorised by SEEM authorities. Those certificates include the SEEM Identification Number (SID), which is used to authorise users and is directly connected to the security profile of each user. Each registry and repository must keep a list of all the certificate authorities it recognises.

  The SEEM infrastructure treats the certificates issued by the SCA, external CAs and TTPs differently. They are classified in different trust levels. Normally, a user with a certificate issued by a TTP is normally regarded as more trustworthy, because TTPs may specifically evaluate the various aspects/capability/behaviour of a company, whilst the users with certificates issued by the SCA and external CAs are regarded as being of 'normal trust level' (for details, see the SEEM trust infrastructure[2]).
- *High Level Conformance*: During the establishment of electronic trading relationships, it is often considered essential to perform high-level conformance checking. This includes a check on

[2] To be published in May, 2005.

system conformance – to ensure the integrity of the system and processes – and users' business behaviour – to ensure that participants are trustworthy in terms of their capabilities and good will. The conformance could be tested directly, or proven by reputation and comments left by partners, or through certificates issued by the SCA. In some cases, the issue of certificates could be undertaken by third parties that test conformance. This functionality therefore has to be supported within SEEM.

4 AGENT-FACILITATED TRUST BUILDING FRAMEWORK

Previous studies (Zacharia *et al*., 2000; Maarof & Krishna, 1999; Moukas *et al*., 2000) demonstrate that the personalised, autonomous, adaptive and proactive nature of agents provides for the high level of interactivity and expressiveness needed for an effective and fulfilling customer experience, leading to a trusting relationship with the business. Recently, Chihiro *et al*. (URL2) and Hu (2002) have attempted to use agents as facilitators to build trust in eBusiness.

4.1 The Role of Trust Building Agents

Unlike previous studies, this project embeds multi-agent systems within the distributed SRRN and credibility authorities to facilitate the search for, and storage of, trust relevant information in the user registry process.

In this framework, there is an agent in each of the registry and repository nodes, as well as within the SCA and TTPs/CAs. These agents collaborate with each other to help a registered user find a trusted partner, based on its certificate and conformance information. To do that, agents work in three aspects:

1) Firstly, a registry agent contacts other registry nodes (agents) to check whether a potential partner (either customer or supplier) has registered with these registry nodes. The registry agent also contacts repository nodes (agents) to check whether a node contains the specific information about the potential supplier/customer.

2) Secondly, the registry agent searches for the potential supplier/customer's certificate. In such a case, the agent will first contact the SCA agent. If it cannot find the certificate, the SCA agent will then contact its neighbouring TTPs to see whether they have the certificate of the partner. If not, the related TTP agents will further contact their nearby TTPs or CAs. Since each TTP can only link to a number of neighbouring TTPs, an algorithm has been developed for agents to seek and negotiate the certificate.

3) Similar to the process for seeking the certificate, the registry agent also needs to contact different registry nodes (agents) or repository nodes (agents) and SCA agents to explore the possible conformance information.

4.2 Attribute Definition

Accordingly, a number of attributes have been designed for the agents to specify a SEEM user such as:

– Certificate: The subject field identifies the entity associated with the public key stored in the subject public key field. The entity is a combination of Relative Distinguished Names (RDN), which comprise several attributes.

Table 1. Essential attributes of user certificate

Attribute	**Object Identifier**	**Description**
Country-Name	{ 2 5 4 6 }	Abbreviation for country
Common-Name	{ 2 5 4 3 }	Combination of subject's surname and given Name.
OrganisationName	{ 2 5 4 10 }	An informative unique name of the subject's organisation
OrganisationalUnit-Name	{ 2 5 4 11 }	An informative unique department name of the subject's organisation
SerialNumber	{2 5 4 5}	The SEEM Identification Number (SID)

In addition, there is extended information in the certificate such as the communication approach, bank account, business scope, decipherment, signature, certificate signing, etc.

– Conformance: This field specifies a user's performance related information. For example, for a customer, the following information needs to be addressed: rank by the SEEM ranking system, initial information provision, requirement description, payment, communication capability, response to change management, etc.; for a service provider, rank by the SEEM ranking system, the information to be addressed includes: expertise, product, resources, quality of service, communication effectiveness, response to change management, etc.

4.3 Scenario

The developed conceptual model will be implemented in the SEEMseed waste disposal scenario (WP3). In this scenario, a waste disposer (i.e. the customer) tries to find a specialist transportation company (i.e. the service provider) to dispose of the waste. The cus-

tomer registers at a registry node, the registry agent receives the user request through the application layer and RR service layer (for details, see the SEEM trust framework). Following the request from the user, the agent starts to seek potential waste transportation companies (WTC) that are qualified to offer the service through the SEEM network.

The registry agent searches for three kinds of trust relevant information with other peer agents: the possible registry information of waste transportation companies, the certificate information of the companies and the conformance information if available. Figure 4 illustrates the simple process described below:

1) The registry node A agent first sends an enquiry to registry node agents B and C. The enquiry form is based on the SEEM generic partner requirement template;
2) Neither B nor C finds any registered waste transportation company in their records;
3) Agent B then forwards the enquiry to registry Agent D, E, F, whilst Agent C forwards the enquiry to Agent G and H;
4) After the search through the SEEM registry nodes, no agent finds any waste transportation company registered (for the case that there are registered transportation companies, please see the SEEMseed trust infrastructure report);
5) The search result then feeds back to Agent A;
6) Agent A then sends the enquiry and information to the SCA. The SCA agent sends the enquiry to TTP2 agent;
7) TTP2 agent has not found any required company, then forwards the enquiry to TTP1 and TTP3;
8) This process continues until TTPn finds a waste transportation company, which has a valid certificate; and
9) The relevant certificate and conformance information (if any) is then fed back to Agent A from TTPn agent through the peer agents.

5 CONCLUSION

As a Europe-wide electronic market, the SEEM should provide a mechanism to foster the trust building between customers and suppliers, particularly when dealing with complex engineering services. Current studies in trust building mainly focus on the online security, business perspectives (e.g. initial trust building, trust building and distrust building factors, reputation system and disputes resolution) and social legal framework. The SEEMseed project not only considers these aspects, but also develops a trust building agent-based system for the SEEM infrastructure.

An important characteristics of the SEEM is the distributed registry and repository systems, as well as the TTPs/CAs. Therefore, tracing the information related to user registration and credibility is important for trust building. Multi-agent systems provide an effective approach to tracing this information, and will help users to find trustworthy partners.

As this model is still immature, much work still needs to be done, and several specific issues need to be addressed, including:

- The principles of agent behaviour in each node, particularly those related to security. In fact, trust among agents themselves is an issue. When agent systems are used to facilitate trust building, particularly when dealing with confidential information, careful system design is required.
- There are many problems affecting the implementation of agent systems in the SEEM infrastructure. This is mainly because agent-building toolkits are not yet mature. Therefore, additional work is required.
- It is expected that agents could also facilitate the lifecycle trust building. The mechanism of how agents could be involved in monitoring and evaluating users' behaviour in the SEEM will be another interesting area of investigation.

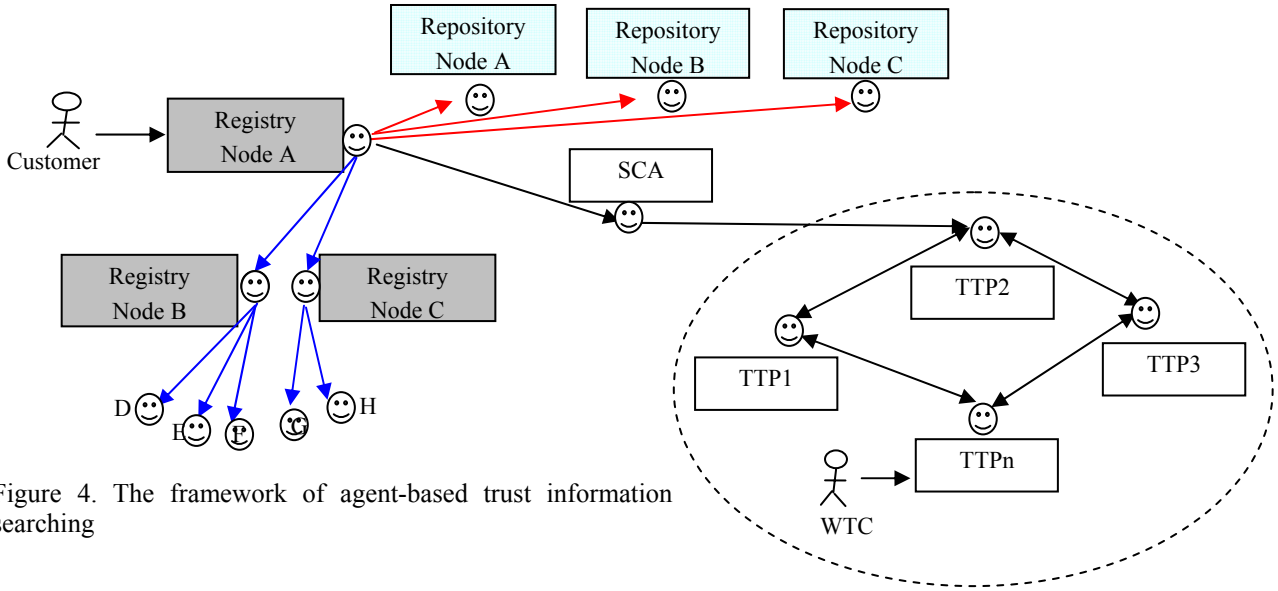

Figure 4. The framework of agent-based trust information searching

6 ACKNOWLEDGEMENT

This work has been partly funded by the European Commission through the IST Project SEEMseed: Study, Evaluate and Explore in the Domain of the Single Electronic European Market (IST-1-502515-STP). The authors wish to acknowledge the Commission for their support. We also wish to acknowledge our gratitude and appreciation to all the SEEMseed project partners for their contribution during the development of various ideas and concepts presented in this paper.

REFERENCES

D2.1 (2004). SEEM User Requirements. SEEMseed Project Deliverable.

D2.2 (2004). SEEM Infrastructure Specification. The SEEMseed Project Deliverable.

Hu, Y. J. (2002). Trusted Agent-Mediated E-Services via Semantic Web Rules Inference. *URL: http://www.cs.nccu.edu.tw/~jong/pub/web-trust-talk.pdf*.

Maarof M. A. and Krishna K. (1999). An Hybrid Trust Management Model For MAS Based Trading Society. *URL: http://www.old.netobjectdays.org/pdf/02/papers/malceb/0697.pdf.*

McKnight, D. H., and Chervany, N. L. (1996). The Meanings of Trust, University of Minnesota MIS Research Center Working Paper Series, WP96-04, Minneapolis.

McKnight, D. H., Cummings, L. L., and Chervany, N. L. (1998). Initial Trust Formation in New Organizational Relationships, Academy of Management Review, Vol. 23, pp. 473-490.

Moukas, A., Guttman, R., Zacharia, G., and Maes, P., (2000). Agent-mediated Electronic Commerce: An MIT Media Laboratory Perspective. *International Journal of Electronic Commerce, Vol. 4, No. 3*.

Ren, Z., Hassan, T.M., and Carter, C. D. (2005). Trust Building for SMEs in B2B e-Markets – A Case Study of the SEEMseed Project (in press). T*he 11th International Conference on Concurrent Enterprising (ICE2005)*, Munich, Germany.

URL1: http://www.seemseed.net/default.aspx

URL1: *http://www-cdr.stanford.edu/~petrie/ono-trust.pdf*. Chihiro, O, and Nishiyama, S., Kim, K., Paulson, B. C., Cutkosky, M. and Petrie, C. J., Trust-based Facilitator: Handling Word-of-mouth Trust for Agent-based E-Commerce.

Zacharia, G., Evgeniou, T., Moukas, A., Boufounos, P., Maes, P. (2000). Economics of Dynamic Pricing in a Reputation Brokered Agent Mediated Marketplace. *Electronic Commerce Research Journal, Special Issue on Intelligent Agents in Electronic Commerce*, Baltzer Science Publishers, Bussum, Netherlands; ISSN: 1389-5753.