SECURE INTERACTIVE ELECTRONIC NEGOTIATIONS IN BUSINESS-TO-BUSINESS MARKETPLACES

Michael Rebstock

Fachhochschule Darmstadt University of Applied Sciences,
Haardtring 100, 64295 Darmstadt, Germany
Phone +49 6151 168392, Fax +49 6151 168399
E-mail rebstock@fh-darmstadt.de

Omid Amirhamzeh Tafreschi

Fraunhofer - Institute for Secure Telecooperation SIT,
Dolivostr. 15, 64293 Darmstadt, Germany
Phone +49 6151 869705, Fax: +49 6151 869704
E-mail tafresch@sit.fraunhofer.de

ABSTRACT

In this paper, we discuss security aspects of interactive bilateral multi-attribute negotiations. We introduce this type of electronic negotiations and maintain that it will be an important functional aspect of business-to-business electronic marketplaces. We discuss the general application architecture and the process flow for this type of negotiations. We introduce the relevant security issues and show how these issues can be dealt with, especially within a business relationship where a lower degree of trust prevails. To this purpose, we introduce and discuss a protocol for secure interactive electronic negotiations.

1. INTRODUCTION

Electronic negotiations have become quite popular. Their popularity today mainly is due to the fact that electronic markets gain more and more importance in business relations. In spite of this popularity, application functionality in business-to-business marketplaces only covers a small range of a company's overall procurement activities. Marketplaces offer electronic catalogs, auction and tender functionality. But by far not every product or service can be acquired using these three instruments. Additional services are necessary. It was proposed [Rebstock, 2001] that when it gets to decisions about (legally binding) contracts, many electronic negotiations will be *bilateral* and *interactive*. To cope with real world contract complexity, most of these negotiations have to be *multi-attribute* negotiations. To be able to process the negotiation results in in-house systems and thus achieve overall process efficiency, the transaction information exchanged will have to be *structured*, while accompanying messages may be *unstructured*. Some work has already been done on bilateral and multi-attribute negotiations, either conceptually [e.g., Jelassi and Foroughi, 1989; Wedekind 2000; de Paula et al., 2001], or in application design and development [Interneg, 2001; IBM, 2001; Menerva, 2001]. Some of the applications developed originate from workflow systems and contract management systems [Koetsier et al., 2000; DiCarta, 2001; SmartSettle, 2001]. Still, these works do not supply all the functionality necessary in business-to-business electronic marketplaces.

During the 1990s, electronic negotiations have already been a research topic. At that time, agent-based approaches [e.g., Jennings and Wooldridge, 1998] had gained much attention but did not meet all their ambitious objectives (e.g., the Tête-à-Tête project [Guttman et al., 2001]). The major objective of these projects was full automation of negotiation processes. Even though it has been expected since many years that this objective can be achieved, it is still a subject of controversial discussions [Davis and Smith, 1983; Guttman et al., 1998; Beam et al., 1999; Kersten and Noronha, 1999; Pradella and Colombetti, 2001]. Application developers still have to simplify negotiation scenarios to be able to fully automate processes. Against this background, we expect that agent-based applications in many cases will not handle complete negotiation processes, but will supply services like preparatory decision support or contract execution support. Although many well-known research projects – like Kasbah [Chavez and Maes, 1996], AuctionBot [Wurman et al., 1998] and others – focus on full automation, our approach focuses on *negotiation support* instead. A fully automated negotiation application is *result-oriented*: it aims to generate a negotiation result automatically. Our approach is *process-oriented*, because it primarily supports the process of the negotiation and leaves the final decision about a contract to human actors.

In this paper, we first explain the concept of electronic negotiations and, as their context, electronic markets. We introduce and discuss interactive, bilateral, semi-structured, multi-attribute electronic negotiations in business-to-business marketplaces. We discuss the application architecture and process flow for these kinds of negotiations. The main security aspects within this context are introduced and analyzed. Based on our analysis, we develop a protocol for secure electronic negotiations.

2. ELECTRONIC MARKETS AND NEGOTIATIONS

An electronic negotiation is a joint decision-making process of two or more parties within an electronic market [cf., among others, Davis and Smith, 1983]. The objective of this process commonly is to establish a contract between the parties involved. The parties issue offers to their market partners in order to reach an agreement. The number of parties involved in this process, its temporal and other conditions depend on the *negotiation protocol* chosen.

Electronic negotiation applications today are often conceived as being part of an electronic market. An electronic market is an application that is based on electronic communication services and that supports the market coordination of economic activities [cf. Schmid, 1993; Schmid, 1999]. On this markets, electronic transactions are performed by market partners. The legal and economic core of an electronic market transaction is the contract between the market partners involved. In this paper, we focus on business-to business marketplaces, where partners both on the supply and on the demand side are companies or organizations.

Electronic market transactions can be conceptualized as having five phases (Figure 1) [Schmid, 1993; Schmid 1999; Rebstock, 2000]:

- Knowledge phase (where the relevant information concerning products, market partners etc. is gathered)
- Intention phase (where offers concerning supply and demand are specified by the market partners)
- Agreement phase (where the terms and conditions of the transaction are defined and the contract is closed)
- Execution phase (where the agreed-upon contract is executed and payment is made)
- Post-sales phase (where contract related services, support, maintenance etc. are delivered)

Electronic negotiation thus is an optional activity within the *agreement phase*. The agreement phase also includes other steps like matching and scoring. In this paper, we focus on the negotiation itself and will not deal with matching and scoring functions.

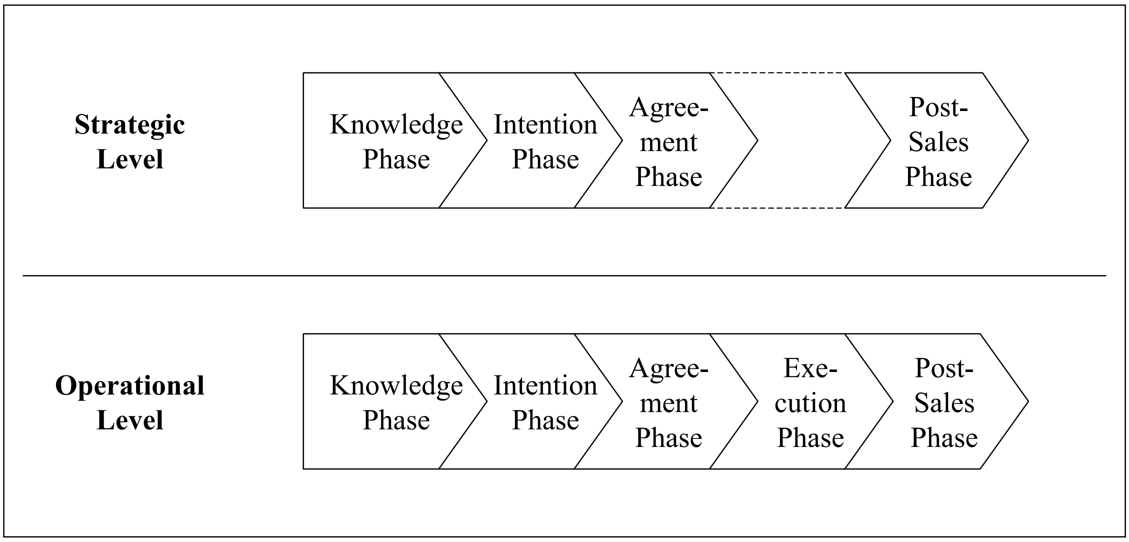

Figure 1. Electronic Market Transaction Phases.

In theory and in business practice we distinguish strategic and operational procurement (or purchasing). While the strategic goal is 'finding the right source', the operational objective is 'closing the right deal'. Except for the execution phase – which always refers to specific transactions – the five phases exist on a strategic as well as on an operational level. On the strategic level, long-term contracts are closed. These create a more or less flexible framework for specific transactions on the operational level.

3. NEGOTIATION APPLICATION ARCHITECTURE

3.1. Interactive bilateral multi-attribute electronic negotiations

Within the *MultiNeg* project [MultiNeg, 2001], an electronic negotiation application is being analyzed and developed. Like the project as a whole, the application focuses on bilateral, multi-attribute electronic negotiations. The main component of the application is the 'Negotiation Engine'. Other components include basic communication routines and management of negotiation semantics. This paper focuses on the Negotiation Engine. This component can be used as an add-on for an electronic marketplace or it can be used stand-alone. Either way, it is conceptualized as a large-grained electronic commerce component and as such exposes standard interfaces that are based on XML messages to communicate with other components or services locally as well as anywhere on the Web. General electronic market functionalities like service directories, catalog services or settlement services are supplied by other electronic market components and are not part of the electronic negotiation component.

The Negotiation Engine is depicted here as being used decentrally (Figure 2). Decentral instances (using trusted Java Applets) are necessary if local security functions are to be implemented. As it is realized in Java, the component as a whole or some of its modules can be implemented centrally, i.e. server-based (using Java Servlets) as well. Indeed, both alternatives are conceptualized and already have been partly realized and tested in the project.

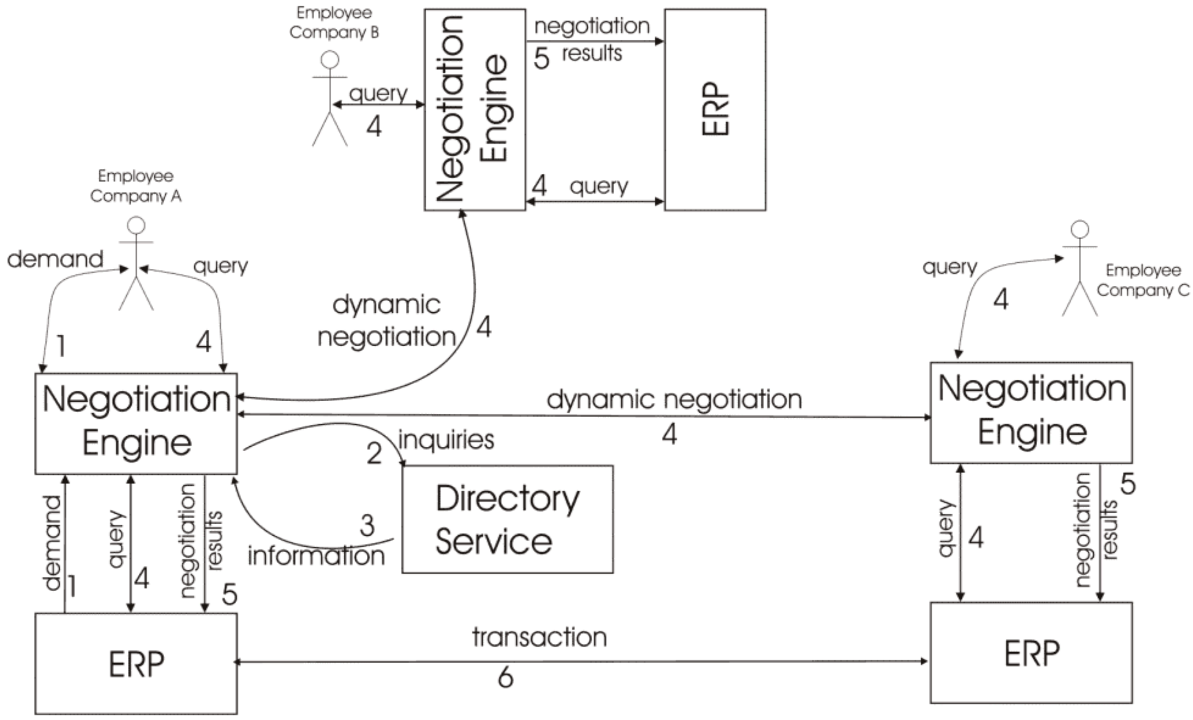

Figure 2. Application Architecture and Process Flow

3.2. Application architecture and negotiation process

Within our application scenario, demand is created in the system by either entering it online or by a message created by an ERP system (1). If the negotiation partner is not already chosen (relying on existing business relations, framework contracts, preferred supplier arrangements or similar sources), a directory service can be used to find a supplier (2). Note that the directory service is not part of the Negotiation Engine, but is an external application. Information from the directory service can be transferred to the Negotiation Engine (3). Once the negotiation partner is chosen, the actual negotiation is started. For this purpose, an initial offer has to be issued by one of the market partners. On the seller side, an offer can be a specific sales offer or can be based on general catalog data. Within our generic scenario, each of the market partners can post offers, buyers or sellers. In this sense, universal or specific requests for quotation issued by a potential buyer are also conceived as being offers (i.e., offers to buy). The initial offer data can be entered manually (1) or can be imported into the electronic negotiation component via XML messages out of the directory service (or another electronic market component, e.g., a catalog) (3) or out of an in-house system (ERP system) (1). Once an initial offer is created, a market partner can issue a counter-offer within the electronic negotiation component. Thus, a dynamic negotiation is initiated (4). Multiple bilateral negotiations at the same time may be necessary to determine the best supplier (4). The exchange of offers and counter-offers can be practiced as often as necessary. During the negotiation, it may be necessary to check the feasibility of certain attributes of the negotiation (qualities, delivery dates, prices etc.) personally or with an ERP system (4). For communicating with an ERP system, standardized messages are used. Finally, if both parties express their agreement on the attributes of the transaction, a contract is closed. The Negotiation Engine then provides the negotiation results for further processing to the in-house ERP systems (5). Thus, frictionless integration of the information chain is enabled. Follow-up processing of the contract may include direct information exchange between the ERP systems for, e.g., dispatch advices or financial settlement information (6).

4. SECURITY MECHANISMS

Electronic negotiation services today are generally offered using the Internet as a platform for telecommunication. Two main characteristics of the Internet are its openness and the anonymity of involved parties. As we described above, a contract is closed when the market partners agree on all aspects of a transaction. Closing the contract electronically has to include all activities and functionality necessary to install a complete, consistent, and legally binding contract on this platform. At this point, security mechanisms become relevant. For successful electronic negotiations, non-repudiation after closing a contract is crucial. Besides the need for non-repudiation, we also discuss further security issues.

4.1 Security issues

The amount and complexity of the security mechanisms necessary is directly linked to the amount of trust already established through other sources, such as framework contracts, long-term business relations or trusted third parties involved in the transaction. If such business relationships or contracts do already exist, a framework generating trust is given. The requirements for security within the electronic negotiation application itself then are comparatively low.

In more anonymous electronic markets these preconditions often are not given. Business relationships then are much less stable, buyers and sellers can more flexibly join and leave a market, and there are virtually no limits to the number of market participants. A naive negotiation then may be subject to manipulation. Security issues gain importance with the number of risks to which electronic market transactions are exposed. Generally, we can distinguish four main issues:

- Eavesdropping of messages: messages may be spied out and the observed information can be misused by unauthorized third parties.
- Masquerading of identity: parties can act under wrong identity.
- Message manipulation: a message can be modified during its transmission.
- Repudiation of messages: a party sending a message within a negotiation process may later claim it has not originated it or it may dispute the contents of the message.

From the above risks we derive requirements for a negotiation application in more anonymous electronic markets:

- Data confidentiality (privacy): the messages exchanged during the negotiation process between parties should be private. I.e., it should not be possible for an unauthorized third party to eavesdrop the message contents.
- Message origin authentication: the receiver of a message should be assured of the identity of the sender to avoid masquerading of identity.
- Message integrity: to guard against message manipulation, an unauthorized party should not be able to modify or corrupt message contents without being detected.
- Transaction authentication: each message exchanged should be unique so that it cannot be intercepted and replayed by an unauthorized third party without being detected.
- Non-repudiation: the sender should not be able to deny the ownership of a message at a later point in time. To prevent the subsequent denial of a negotiation result, all messages exchanged among sellers and buyers need to be legally binding and non-repudiable.

We will now discuss how an interactive bilateral negotiation on an anonymous market can be supplemented with non-repudiable communications including authentication of origin, message integrity, and transaction authentication. Our approach ensures that electronic negotiations are at least as secure as negotiations via other media.

4.2 Reliable Negotiations

In the following, we present a reliable electronic negotiation model that allows the involved market partners to detect a variety of attacks performed by malicious parties and provides legally binding contracts by using techniques for non-repudiation. As a whole, the goal of our approach is to cope with problems that result from:

- Eavesdropping of messages,
- Message integrity,
- Masquerading of identities,
- Replaying messages,
- Repudiation of messages.

Encrypting the transmitted data can solve the first problem in this list. The encryption of data at the transport level can be achieved via SSL [Freier et al., 1996]. In the following, we assume that all data are transmitted in an encrypted way. In order to tackle the remaining vulnerabilities, there are two security concepts that will be applied: digital signatures and availability of authentic public keys. Loosely spoken, digital signatures can be understood as the electronic equivalent of handwritten signatures. They were first sketched in [Diffie and Hellman, 1976]. Meanwhile, there exist several standards for signing digitally [e.g., NIST, 2001]. An extensive overview on digital signatures can be found in [Menezes et al., 1997]. In the electronic world, digital signatures bind pieces of information to identities. Thereby, no other party should be able to create a digital signature binding a statement to the person's identity instead of the person itself. For this purpose, a secret cryptographic key is used to calculate the digital signature. Since no other party knows this secret key, and by the assumption that the underlying signature algorithm prevents forging, a digital signature can be used as a proof to convince any other party of its creator. Therefore, in the European Union as well as in other countries, digital signatures are becoming legally equivalent to handwritten signatures [European parliament and council, 2000].

Besides the means for signature creation, the concept of digital signatures also involves means for signature verification. To do so, the verifier requires a public key corresponding to the signer's secret key. Since a malicious party is able to create a public key and claim for it to belong to a faked identity, this concept requires a method to support the authenticity of public keys. This is achieved by the certification of public keys [e.g., ISO, 1995].

The combination of digital signatures and availability of public keys ensures that any modification of signed documents can be easily detected since this would cause the invalidity of the signature. Additionally, the identity of the signer can be obtained by using the certified public key assigned to a specific identity. Replay of old statements can be detected if the signed documents are unique. Such attacks can be avoided by the usage of sequence numbers or time stamps and a receiver that will never accept an identical message twice. Non-repudiation follows because no other party is able to calculate the digital signature – since the owner exclusively knows the secret key.

4.3 A Secure Interactive Bilateral Negotiation Protocol

The security of the interactive bilateral negotiations is achieved by designing a protocol that applies digital signatures and relies on an infrastructure that guarantees the authenticity of public keys. It is necessary to find a suitable sequence of messages that have to be exchanged between the parties in order to meet all security relevant requirements. In the following, we will explain the protocol steps and give reasons for them.

The transition diagram (Figure 3) depicts the sequence of all the states and actions included in the secure negotiation protocol. All in all, this negotiation protocol is more or less an adaptation of the real world negotiation scenario to the electronic world using security techniques to avoid the risks described above:

- In the first step, the seller issues a digitally signed initial offer (in our generic scenario, it could be the buyer to start the negotiation as well). The message should include his identity, a description of the goods to be sold, and all further relevant conditions of the negotiation such as the time in which he will accept the submission of acceptance or counter-offers. Because of the digital signature a potential market partner can verify the integrity and the validity of the offer. Since the origin of the negotiation can be verified, a market partner can be sure that this offer does not come from a faked source. For instance, if there were a very famous seller in the market attracting many buyers, other parties could claim his identity and thereby draw the attention of some customers to themselves. A further reason for masquerade could be the attempt to damage the reputation of an honest party. These attacks can be avoided if the party signs all the information that they publish to make its authenticity verifiable.
- The second step deals with the (optional) submission of counter-offers. It is assumed that the second party uses the negotiation application to specify her counter-offer and signs this information before submitting it back to the first. The counter-offer references the initial offer. With the signed counter-offer, the buyer declares that she is willing to buy the offered goods for the conditions stated. Again, the use of a digital signature helps the seller to verify the integrity of the offer and to identify his market partner. Furthermore, replay attacks are not possible for there exists a unique relation between the initial offer and the counter-offer. The seller can use the signature on the offer as evidence in case the buyer denies her counter-offer. Such evidence can be used to convince a third party – e.g., a court – that the market partner behaves in a malicious way.
- In the third step, the seller sends a signed confirmation of receipt to the buyer. Such a confirmation includes a unique reference to the received counter-offer. This confirmation ensures the buyer that the seller will consider her counter-offer.
- In step 4 to step n, the process of submitting a counter-offer can be performed by the parties involved once again. Now the seller can specify a counter-offer to the buyer's previous counter-offer, sign it, and send it. The buyer then issues a signed confirmation. The exchange of counter-offers and confirmations can be practiced as often as necessary.
- If one of the parties agrees with the other party's last offer, he sends a signed notification of acceptance. It is also uniquely related to the specific offer accepted. The other party can ensure that the message is not faked since she can verify its origin and integrity. Also, the signature of the notification provides evidence that can be used in case one of the parties changes their decision after notification. In such a case, the evidence will entitle the other party to claim the agreed upon conditions.
- In the next step, the party that received the other party's notification confirms the deal by sending her own notification of acceptance. In order to make this confirmation also undeniable, the party has to sign it as well. Still, the other party could not agree and submit another counter-offer instead. Only if both parties have exchanged their notifications of acceptance, the contract is closed. Both parties have a proof of this acceptance that could not be forged or repudiated.
- In the last step, the transaction data is sent to the respective internal (ERP) applications of the parties involved. As both parties have already signed the contract information, the information cannot be forged at this point without being detected.

- After performing these steps the deal can be executed, i.e. goods or services can be delivered and payment can be made.

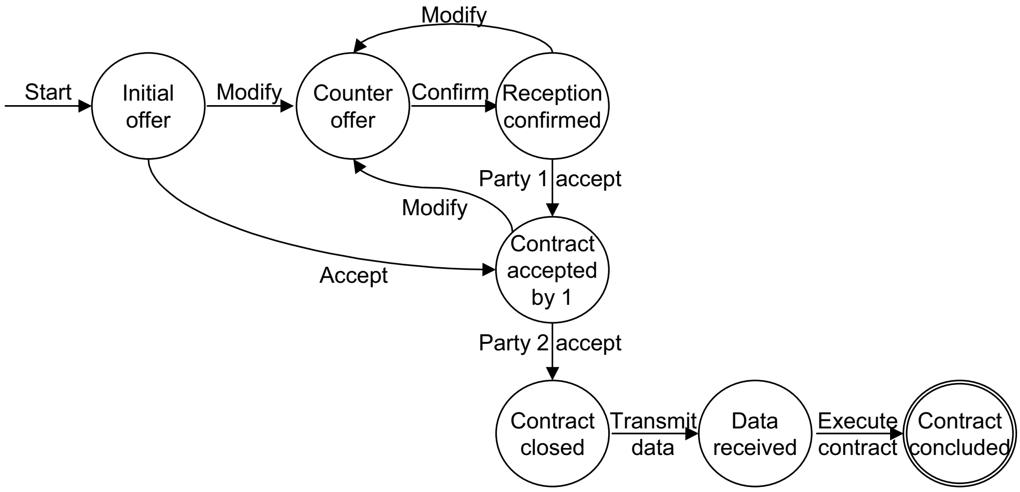

Figure 3. Secure Interactive Negotiation Protocol.

5. CONCLUSION

We have maintained that *interactive, bilateral, multi-attribute electronic negotiations* will be an important part of business-to-business marketplaces. We have discussed the general application architecture and the flow of the negotiation process for this type of negotiation. We have shown how security concerns can be dealt with that will arise within a business relationship where a lower degree of trust prevails. To this purpose, we have introduced and discussed a protocol for secure interactive electronic negotiations.

Compatible with our general philosophy, we have developed a first prototype that covers real-world complexity of business-to-business transactions. For the determination of the negotiation results, we rely on human actors instead of software agents. Still, we see a large potential for partly automating the negotiation process, especially in the areas of information management and semantics management.

Many other questions are open to future research. Establishing efficient interfaces between electronic negotiation applications and in-house systems to our mind is crucial for a wide acceptance and universal usability of electronic negotiation systems. The same holds true for the ability to flexibly deal with diverse business object frameworks. Both aspects will be a major part of our future research.

REFERENCES

BEAM, C., SEGEV, A. and BICHLER, M. et al. (1999). On Negotiations and Deal Making in Electronic Markets. *Information Systems Frontier*, 1 (3), 241-258.

CHAVEZ, A. and MAES, P. (1996). Kasbah: An Agent Marketplace for Buying and Selling Goods. *Proceedings of the First International Conference on the Practical Application of Intelligent Agents and Multi-Agent Technology* (CRABTREE, B. and JENNINGS, N., Eds.), 75-90. The Practical Application Company Ltd, Blackpool.

DAVIS, R. and SMITH, R.G. (1983). Negotiation as a Metaphor for Distributed Problem Solving. In: *Artificial Intelligence,* 20 (1), 63-109.

DE PAULA, G.E., RAMOS, F.P. and RAMALHO, G.L. (2001). Bilateral Negotiation Model for Agent-Mediated Electronic Commerce. In: *Agent-Mediated Electronic Commerce III. Current Issues in Agent-Based Electronic Commerce Systems* (DIGNUM, F. et al., Eds.), 1-14. Springer, Berlin.

DICARTA. http://www.dicarta.com, 2001-05-23.

DIFFIE, W. and HELLMAN, M. (1976). New directions in cryptography. *IEEE Transactions on Information Theory*, IT-22 (6), 644-654.

EUROPEAN PARLIAMENT and COUNCIL (2000). Directive 1999/93/EC of the European Parliament and of the Council on a Community framework for electronic signatures of 13 December 1999. *Official Journal of the European Communities L 13/12, 19.1.2000.* http://europa.eu.int/comm/internal_market/en/media/sign/Dir99-93-ecEN.pdf, 2001-05-23.

FREIER, A. O., KARLTON, P., and KOCHER, P. C. (1996). The SSL Protocol: Version 3.0. Internet draft, ftp://ietf.cnri.reston.va.us/internet-drafts/draft-freier-ssl-version3-01.txt, 1999-10-10.

GUTTMAN, R.H., MOUKAS, A.G. and MAES, P. (1998). Agents as Mediators in Electronic Commerce. *International Journal of Electronic Markets*, 8 (1).

GUTTMAN, R.H., VIEGAS, F. and KLEINER, A.F. (2001). Tête-à-Tête. http://guttman.www.media.mit.edu/people/guttman/research/tete/tete.html, 2001-05-23.

IBM RESEARCH (2001). SilkRoad. http://www.zurich.ibm.com/csc/ebizz/silkroad.html, 2001-05-23.

INTERNEG (2001). http://interneg.org, 2001-05-23.

ISO/IEC (1995). Information Technology - Open Systems Interconnection - The Directory: Authentication Framework. 9594-8: 1995.

JELASSI, T. and FOROUGHI, A. (1989). Negotiation support systems: an overview of design issues and existing software. *Decision Support Systems,* 5 (2), 167-181.

JENNINGS, N.R. and WOOLDRIDGE, M. Eds. (1998). *Agent Technology: Foundations, Applications, and Markets*. Springer, Berlin.

KERSTEN, G.E. and NORONHA, S.J. (1999). Negotiations in Electronic Commerce: Methodological Misconceptions and a Resolution. Interneg-Report INR02/99. http://interneg.org/interneg/research/papers/1999/02.pdf, 2001-05-23.

KOETSIER, M., GREFEN, P. and VONK, J. (2000). Contracts for Cross-Organizational Workflow Management. *Electronic Commerce and Web Technologies* (BAUKNECHT, K. et al., Eds.), 110-121. Springer, Berlin.

MENERVA (2001). http://www.menerva.com, 2001-05-23.

MENEZES, A.J., VAN OORSCHOT, P.C. and VANSTONE, S.A. (1996). *Handbook of applied cryptography*. CRC Press.

MULTINEG (2001). http//www.fbw.fh-darmstadt.de/multineg, 2001-10-23.

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (2001). Digital signature standard DSS. FIPS 186-2, http://csrc.nist.gov/publications/fips/fips186-2/fips186-2-change1.pdf, 2001-05-23.

PRADELLA, M. and COLOMBETTI, M. (2001). A Formal Description of a Practical Agent for E-Commerce. In: *Agent-Mediated Electronic Commerce III. Current Issues in Agent-Based Electronic Commerce Systems*. LNCS Vol. 2003 (DIGNUM, F. et al., Eds.), 84-95. Springer, Berlin.

REBSTOCK, M. (2000). Elektronische Geschäftsabwicklung, Märkte und Transaktionen - eine methodische Analyse. *HMD Praxis der Wirtschaftsinformatik,* 37 (215), 5-15.

REBSTOCK, M. (2001). Towards Interactive Electronic Negotiations in Business-to-Business Marketplaces. Extended CD-ROM version. *CD-ROM Proceedings of the 46. International Scientific Colloquium - Multimedia, The Challenge for Science* (KERN, H., Ed.). Ilmenau Technical University, Ilmenau.

SCHMID, B. (1993). Elektronische Märkte. *Wirtschaftsinformatik*, 35 (5), 465-480.

SCHMID, B. (1999). Elektronische Märkte - Merkmale, Organisation und Potentiale. *Management-Handbuch Electronic Commerce* (HERMANNS, A. and SAUTER, M., Eds.), 31-48. Vahlen, München.

SMARTSETTLE (2001). http://www.smartsettle.com/, 2001-05-26.

WEDEKIND, H. (2000). On Specifying Contract Negotiations. *Proceedings of the 8th European Conference on Information Systems, Volume 1* (HANSEN, H.-R. et al., Eds.), 23-30. Vienna University of Economics and Business Administration, Vienna.

WURMAN, P.R., WELLMAN, M.P. and WALSH, W.E. (1998). The Michigan Internet AuctionBot: A Configurable Auction Server for Human and Software Agents. *Proceedings of the 2nd International Conference on Autonomous Agents* (SYCARA, K.P. and WOOLDRIDGE, M., Eds.), 301-308. ACM Press, New York.