FROM CALL FOR TENDERS TO SEALED-BID AUCTION FOR MEDIATED ECOMMERCE*

Omid Amirhamzeh Tafreschi and Markus Schneider
Fraunhofer Institute for Secure Telecooperation (SIT)
D-64293 Darmstadt, Germany
{tafresch|markus.schneider}@sit.fraunhofer.de

Peter Fankhauser, Bendick Mahleko and Thomas Tesch
Fraunhofer Institute for Integrated Publication and Information Systems (IPSI)
D-64293 Darmstadt, Germany
{firstname.lastname}@ipsi.fraunhofer.de

Abstract With the emergence of business to business eCommerce conventional trading practices need to be adapted to the new electronic environment. One such trading practice is the call for tender (CFT) which is heavily used for trading perishable goods. A naive translation of the CFT to mediated eCommerce introduces new manipulation possibilities like identity masquerading, repudiation of messages etc. In a first step, we show how the basic CFT can be made robust against these security attacks. However, this approach does not eliminate fundamental economic design problems of the CFT itself. In a second step, we show how the CFT can be protected against attacks that damage the fairness and economic efficiency of a market by turning it into a secure sealed-bid auction protocol.

Keywords: Electronic Auctions, Mediated eCommerce, Security

Introduction

The basic IT ingredients for eCommerce—secure and robust network protocols, electronic authentication, payment and delivery chains, and scalable web servers for product offering and ordering—have matured. But current eCommerce solutions only scratch the potential of this infrastructure. New distribution channels and more direct consumer-provider relationships require more open and more flexible trading support which, at the same time, retains the stability of existing trading practices. The EU-funded eBroker project (IST

*This work was supported in part by the European Commission under contracts IST-1999-11060, project eBroker, and IST-1999-10288, project OPELIX.

The original version of this chapter was revised: The copyright line was incorrect. This has been corrected. The Erratum to this chapter is available at DOI: 10.1007/978-0-387-35658-7_21
R. Meersman et al. (eds.), *Semantic Issues in E-Commerce Systems*

1999/11060) tackles these challenges with a framework for mediated eCommerce solutions providing brokering services at two levels.

- Information brokering: Product information, trading preferences, as well as transaction-related information, such as shipping addresses can be and are modelled in a multitude of ways. To meaningfully couple these heterogeneous models, eBroker will employ a classic wrapper/mediator architecture, which uses as far as possible the results from the ongoing ebXML [18] initiative as a pivot model.
- Robust transaction brokering: In addition to heterogeneity of exchanged information, the autonomy of players participating in an open electronic market poses new challenges, because electronic markets tend to involve much less stable business relationships. The naive automation of existing trading practices gives rise to new forms of manipulations, such as spying out interests of business partners, fake offers and demands, or exaggerated negotiation practices. These manipulations can damage the fairness and efficiency of a market, and thus significantly impede the wide-spread acceptance of automated trading solutions.

In this paper we focus on robust transaction brokering. In Section 2 we formalize calls for tender (CFT) as a trading practice which is heavily used for trading perishable goods. In Section 3, we analyse the manipulation possibilities arising when deploying CFTs naively in an electronic market scenario, and derive general requirements for more robust trading models which avoid such manipulations. In Section 4, we show how CFTs can be made robust against classical security attacks, and in Section 5 we show how CFTs can be protected against manipulations that damage the fairness and economic efficiency of a market. We conclude with related and future work.

1. Sale by Call for Tenders

The fresh food industry exemplified by the eBroker application partners has been analyzed and three business models have been singled out. The first business model is a real time auction. A real time auction requires that auction participants be present at the site of the auction, as a lot takes about 6 seconds to sell. Since eBroker is an Internet-based system, it is not feasible to guarantee this time constraint. The other business model is the sale by catalog, which entails the use of fixed prices to different buyers based on their professional branch. Sellers make product offers through a catalog system, and buyers select the best offers. Finally, buyer and seller offers are matched. The third model is the sale by call for tender. The sale by call for tender (CFT) approach provides a negotiation framework where a seller instantiates a call for tender, and buyers make buy offers on a competitive basis. The winning buy offer is determined when the CFT is closed. The criterion for determining the winner

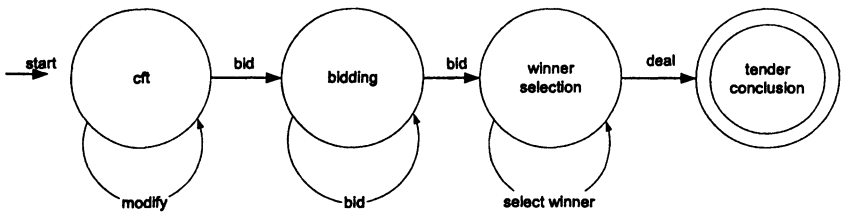

Figure 1. Sale by CFT

is not formalized. It can be simply selecting the highest offer, but may also be based among other considerations such as past business relationships with the seller or location.

In this paper we focus on the sale by call for tender model. On the one hand it is more flexible than a fixed price sales model, especially in a highly dynamic food market. But on the other hand, as we will detail in Section 3, it entails particular manipulation possibilities when naively applied in mediated eCommerce with more unstable business relationships.

The sale by call for tender process can be broken down into four phases. The phases are described below:

1 *Seller calls for tender.* Registered sellers initiate a tender process by submitting lots for sale by way of CFT. More precisely, the seller announces his intention to sell goods, and invites buyers to make buy offers based on their valuation of the goods. Each lot is described by the following information: lot number, seller reference, branch, sale site organization, product species, product family, product description, unit, quantity, date of availability, place of availability, delivery conditions, and lot price. A seller can modify or delete a sale offer provided no buy offer has been made on it.

2 *Bid submission.* Once a CFT process has started, buyers submit buy offers on the lots available based on their valuation. This is a simple process where buyers select lots they want to buy and the price for which they are willing to pay for each lot. A bid carries the following pieces of information as a minimum: tender Id, buyer reference, quantity, price offered, currency and date and time of bid submission. A buyer can delete or modify an offer provided the closing date has not been reached.

3 *Winner Determination.* The selection of winners is done either manually or automatically. For bids to be considered, they must be at least equal to the set reserve price. The reserve price is set by the seller and is known only to him. The criterion for determining the winner is based among other considerations on the bid amount where highest bids stand a greater chance of winning. Once winners have been selected, the seller contacts them and the tender process is concluded.

4 *Tender Conclusion.* This is the last phase of the sale by CFT. After winners have been determined, the following statements are distributed:
   - o *confirmation statement* - this statement is sent by the seller to the winners to confirm their orders.
   - o *transaction statement* - this statement describes details of the transaction and the service charges.

The transaction is processed, and payment and delivery executed in line with prior arrangements by the various parties. The actual transfer of good and money is done outside the system. The process is depicted as a finite state automata diagram as shown in Figure 1.

2. Requirements for Secure CFT

The sale by call for tender process introduced above works well in a closed environment with stable business relationships. This is currently the scenario provided by the application partners in the eBroker project. Buyers and sellers trust each other. In addition, the number of buyers and sellers is small. In Internet-based mediated eCommerce all these assumptions do not hold usually. Business relationships 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 adoption of the CFT to mediated eCommerce is subject to manipulation. We can distinguish four main sources of attacks:

- *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 on transmission.
- *Repudiation of messages*: a party sending a message within a CFT process may later claim it has not originated it or it may dispute the exact contents of the message. authentication and non-repudiation of digital messages.

From the above attacks we derive requirements for a CFT applied in a mediated eCommerce setting.

- *Data confidentiality (privacy)*: the messages exchanged during the CFT process between seller and bidders should be private. Thus, 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*: an unauthorized party should not be able to modify or corrupt message contents without being detected in order to guard against message manipulation.
- *Transaction authentication*: each message exchanged should be unique such that it cannot be intercepted and replayed by an unauthorized third party without being detected.

- *Non-repudiation*: to prevent the subsequent denial of a CFT, all messages exchanged among sellers and bidders need to be legally binding and non-repudiable. Thus, the sender of a message cannot later deny ownership of the message if it was sent with his/her digital signature.

We discuss in Section 3 how the basic CFT can be supplemented with non-repudiable communications including authentication of origin, message integrity, and transaction authentication. This approach ensures that no new manipulation possibilities are introduced by the realization of CFT with computer support. However, this approach does not eliminate fundamental design problems of the CFT process itself. Further drawbacks of the CFT protocol surface in the economic design of the protocol. The main source of manipulation caused by the design of the CFT are:

- *Asymmetry of knowledge*: in the bidding phase of a CFT the state of knowledge on the current bidding status is unevenly distributed between the bidders and the seller. During this phase a seller can open the present offers and exploit this knowledge. For example, the seller can inform other market players on the current bidding status and motivate them to outperform the current bids.
- *Asymmetry of control*: the manual winner selection is solely controlled by the seller. In contrast to auction protocols the CFT thus can not give any guarantees w.r.t. the winner selection. In practice, the winner determination is based on criteria beyond the price like a bidder's identity and the trust already established in the business relationship between the bidder and seller.

In addition, the CFT protocol can result in a sub-optimal allocation of goods. The manual winner selection cannot guarantee that the bidder selection is the most efficient solution, i.e., the solution that maximizes the surplus of the economy. Furthermore, the protocol motivates bidders to speculate on the bids of their opponents. To overcome the manipulation possibilities caused by the asymmetry of knowledge and the asymmetry of control an extended CFT protocol demands the following requirements:

- *bid confidentiality*: to avoid the manipulation possibilities caused by the asymmetry of knowledge, we demand that bids can only be opened when the CFT expires. Additionally, it should be ensured that invalid bids cannot violate the integrity of the CFT process.
- *fairness*: to avoid asymmetry of control the winner determination needs more transparency for the bidders. For a fair winner determination, it is required that the rules for the winner determination are stated a priori by the seller in the CFT, e.g., only best price like in auctions or a combination of price and delivery time etc. One prerequisite for fairness is that rules allow to rank the bids in a total order where the highest ranked bid is the winning bid.

In addition, a fair CFT requires that the bidders can restrict the amount of information revealed to the seller. That is, only the information required to determine the winner should be accessible by the seller. Thus, information like identity, location, business profile etc. should only be accessible if required by the seller for the winner determination.
The existence of comprehensible winner determination rules also allows bidders to verify the correctness of the selection process carried out by the seller.

3. CFT with Non-Repudiation

In the following we will present an electronic version for a reliable call for tender model that allows the involved parties to detect a variety of attacks performed by malicious parties and provides legal bindingness by using techniques for non-repudiation. The goal of our approach is to cope with problems that result from

- eavesdropping messages,
- message integrity,
- masquerading of identities,
- replaying messages,
- repudiation of messages.

The first problem in this list can be solved by encrypting the transmitted data. The encryption of data at the transport level can be achieved via SSL [6]. In the following, we assume that all data are transmitted in an encrypted way. In order to tackle the remaining vulnerabilities, there are basically 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 [4], and meanwhile, there exists several standards for signing digitally, e.g., [19]. An extensive overview on digital signatures can be found in [16]. 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. Therefore, this person uses a secret —a secret cryptographic key— to calculate the digital signature. Since no other party knows this secret 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 —e.g., a judge— of its creator. Beside the means for signature creation, the concept of digital signature involves also means for signature verification. In order to do this, 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., see [9].

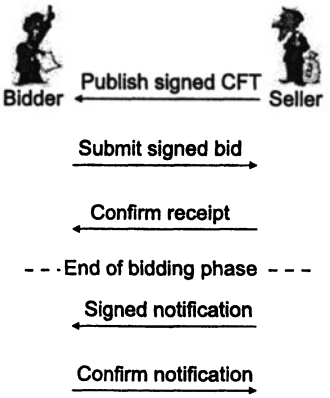

Figure 2. The CFT protocol

The combination of digital signatures and the 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 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. The non-repudiation follows by the property that no other party is able to calculate the digital signature since the secret key is exclusively known to the owner.

The security of the electronic call for tender is achieved by designing a protocol that basically applies digital signatures relying on a infrastructure that guarantees the authenticity of public keys. Therefore, it is necessary to find a suitable sequence of messages that have to be exchanged between the seller and the bidders in order to meet the previously described requirements. In the following, we will explain the protocol steps and give reasons for them.

1 In the first step, the seller issues a digitally signed CFT. It has to be emphasized that the signed message should include the seller's identity, a description of the goods to be sold, and all further relevant conditions of the CFT such as the time in which the seller will accept the submission of bids. Because of the digital signature a bidder can verify the integrity and the validity of the CFT. Since the signature also depends on some time constraints replay attacks can be avoided. Thus, a malicious party can not take a copy of an old CFT and publish it elsewhere in order to make a buyer submit his bid. Since the origin of the CFT can be verified the bidder can be sure that this CFT does not come from a faked seller. In case there is one very famous seller in the market that attracts a lot of bidders, other sellers could claim his identity and thereby draw the attention of some customers to themselves. A further motivation for masquerade could be the damage of reputation of an honest seller. All these

attacks can be avoided if the seller signs all the information that he publishes to make the authenticity verifiable.

2 The second step deals with the submission of bids. Here, one assumes that the bidder takes a form that is provided by the seller and fills in all the relevant data such as his identity and his bid amount and finally signs all this information before submitting it to the seller. With this signed bid the bidder declares that he is willing to buy the offered goods for the price proposed by himself while respecting the seller's conditions. The form provided by the seller should contain the corresponding signed CFT or a reference to it. The application of a digital signature helps the seller to verify the integrity of the bid and to identify the bidder. Furthermore, replay attacks are not possible since there exists a unique relation between the CFT and each specific bid. Thus, if the seller receives a signed message twice this would have no effect as long as the offered goods are only sold to one bidder as a whole. In another context, if bidders are allowed to ask for some smaller portions of the offered goods, and if more than one winner are allowed, then some further bid identification information should be included. If not, then a malicious party is able to send copies of one signed bid in a replay attack and thereby bidding for multiple portions of the offered good while masquerading the bidder. The signature on the bid can be used as an evidence by the seller in case of a dispute in which the bidder denies his bid. Such an evidence can be used to convince any other party that the bidder behaves in a malicious way.

3 In the third step, the seller sends a signed confirmation of receipt to the bidder. Such a confirmation includes a unique reference to the received bid. This confirmation ensures the bidder that his bid will be considered in the determination of the winner. But this confirmation is also of use for the seller regarding his interests. Without the existence of such a confirmation, a malicious bidder that is powerful enough could try to intercept all concurrent bids. This would be advantageous for him since in the winner determination other bids would be out of the game. By such an attack, the seller does not become aware of better bids. But since in the here considered protocol the bidders expect a confirmation of their bids such an attack would become obvious.

4 After the declared time interval of the bidding phase the seller selects the winner(s) and performs the fourth step in the protocol. This step focuses on the notification of the winner(s). For the sake of simplicity and without constraining generality assume that there is one winner. This notification should be signed by the seller for several reasons. Furthermore, the notification should be uniquely related to the bid. The winner can ensure that the message is not faked since he can verify its origin and integrity. Replaying the notification message would make no sense since the receipt of copies will not mislead or confuse the winner. Even a malicious winner can not gain any

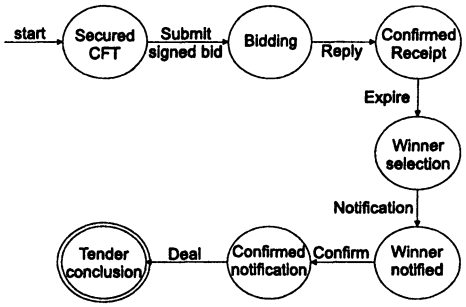

Figure 3. Transitions for secure CFT

profit from copying the notification and requesting the goods for each copy since each acceptable notification is unique and copies will not be accepted. On the other hand, the signature of the notification provides an evidence that can be used in the case of a dispute that arises when the seller changes his decision after the notification. In such a case, the evidence will entitle the winner to claim for the goods.

5 In the fifth step, the winner confirms the receipt of the notification message exchanged in the previous step. In order to make this confirmation undeniable, the winner has to sign it. If such a confirmation is not included in the protocol a malicious seller could leave out the notification in the previous step and claim afterwards that he has sent this notification. Thereby, he would be able to request the amount of money included in the undeniable bid of the second step without informing the winner. In order to have an evidence that he correctly followed the rules of the game the seller has to collect the winner's confirmation. But on the other hand, this confirmation also protects the seller against a malicious winner that refuses of having received the notification. If a malicious winner refuses to send the confirmation then the seller could force him to do so by using an official delivery service. Thus, the seller has the guarantee that he will always have the required confirmation.

After the execution of these five steps the delivery of the sold goods and the payment can be performed. Here, both activities are contained in the term *deal*. The transition diagram in figure 2 depicts the sequence of all the states and actions included in the secure CFT protocol.

The CFT protocol as previously described is more or less an adaptation of the real world CFT scenario to the electronic world using security techniques to avoid the described attacks. Thereby, it is the intention of the seller to have a rather unbalanced model. In the CFT protocol it is requested that the winner determination is done manually and also the rules for that process are not obvious for the bidders. Furthermore, the whole CFT process is controlled exclusively by the seller and he gets a complete insight in all the strategies of

the bidders. Thus, beside all the security that was introduced by the previous protocol, there are still various possibilities for unfairness. These problems can be solved by using sealed-bid auction models.

4. Sealed-bid Auction with Trusted Third Party

Auctions provide another approach for price discovery mechanisms and for the selection of suitable partners for business relations. In this section, we present a secured solution for electronic sealed-bid auctions. The auction approach provides an interesting alternative for a call for tender model since it overcomes some shortcomings of the secure electronic call for tender model, e.g., concerning fairness. In the CFT model, the seller was free to determine the winner in whatever way he decided. The rules for this process were not public —if any fixed rules ever existed. In contrast, we assume that the rules for the winner determination in auctions are publicly known [12, 13, 15]. Furthermore, all bidders have the possibility to check whether the seller —who is called *auctioneer* in the auction context— really follows these rules. Thereby, we achieve another quality in this kind of business model for mediated eCommerce dealing with bid collection and selection out of various offers.

The focus of this section is on the sealed-bid auction type. In general, in sealed-bid auctions submitted bids are not visible for all other bidders. A sealed-bid auction basically consists of two phases: the bid collection phase and the winner determination phase. Here, during the bid collection phase, the bids are submitted in a way that their contents remain hidden not only to competitive bidders but also to the auctioneer. This prevents an unfair auctioneer from colluding with an other bidder by notifying him about the best bid. Before the bids are revealed, the auctioneer commits to the sealed bids. In the winner determination phase, the bids are revealed and the winner is singled out. Thereby, our solution ensures that all involved parties are able to verify that the auctioneer really follows the auction rules without possibilities to cheat. Furthermore, there is a need for means that prevent bidders to deny or to withdraw their bids once they have submitted them.

Further properties of our approach for sealed-bid auctions are non-repudiation, anonymity of the bidder, and prevention of message manipulation and masquerading attacks. The auction model approach involves the role of a trusted third party (TTP). The reason for the introduction of a TTP is mainly motivated by the goal of anonymity to be combined with the prevention of bid withdrawals. Anonymity is necessary since the auctioneers could draw conclusions from the knowledge of bidder's identity concerning his concealed bid. Other work in the context of anonymity can be found, e.g., in [3, 2, 7, 20].

In our concept, the TTP has to be trusted only by the bidder, the auctioneer's trust is not necessary. Thus, there arises no difficulty in finding a TTP which is trusted by both parties in common. Each bidder can choose any desired TTP.

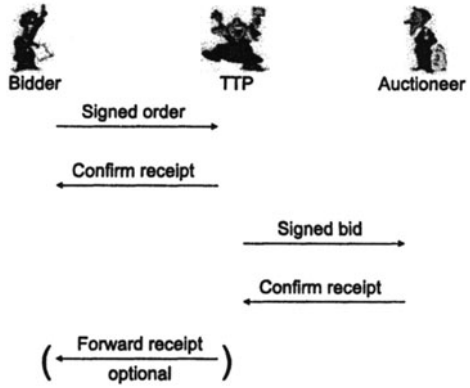

Figure 4. Protocol for the bidding phase

Thus, the auctioneer can be in contact with several TTPs executing the protocol. Beside the reason of anonymity, the existence of a TTP offers a higher level of comfortability for the bidders. By using a TTP's service they do not have to care about sending messages in time according to the time conditions defined in the auction rules.

In contrast to the traditional sealed-bid auction [15], in our model the auctioneer gets insight into all bids during the winner determination phase. This decision is motivated by the fact that under certain circumstances it is of high interest for the auctioneer to find out about the demand for specific goods. This knowledge can be used in the organization of following auctions. A further property of our approach is using efficient primitives that results in feasibility.

For the sake of simplicity, we assume in the following that the winner determination rules concentrate exclusively on the bid amount. In a more general approach, there could also be further variables beside the bid amount that could affect the winner determination provided that they can be put in a total ranking. However, by our restriction we do not constrain the generality of our approach.

Assume that the bidder has received all the relevant information about the auction, e.g., the goods that can be purchased in the auction, and the auction rules like auction start time and deadline. For reasons of authentication, all this information is signed by the auctioneer A. Before a bidder B_i participates in the auction he selects one of the available TTPs to use its services. Another bidder B_j also interested in the auction can select either the same or a different TTP. During the bid collection phase, B_i starts the following protocol:

1 In the first step of the protocol, B_i prepares an order $order$ that consists of the following parts to be sent to the TTP:

$$order_i = order\_details_i,\ encr_{K_i}(amount_i),\ E_{pk_A}(K_i),\\ Sig_{B_i}(order\_details_i,\ encr_{K_i}(amount_i),\ E_{pk_A}(K_i)).$$

In this context, these variables have the following definitions. The variable $order\_details_i$ describes all necessary information that is needed later by TTP in order to participate in the auction on behalf of B_i such as identity of B_i, the auction B_i is interested in, the auctioneer A, and auction details (e.g., rules, time constraints). The term $encr_{K_i}(amount_i)$ describes the ciphertext obtained by symmetric encryption of $amount_i$ —the amount of money B_i is willing to pay in the auction— using key K_i which is randomly chosen by B_i. There exist several algorithms that can be applied for symmetric encryption, e.g., *AES*, *IDEA*, *3DES*. This ciphertext will be used later as a part in the sealed bid to be forwarded to A. As long as A does not possess K_i he is not able to reveal the amount. The term $E_{pk_A}(K_i)$ specifies the ciphertext obtained by asymmetric encryption of K_i using the auctioneer's public key pk_A. Using asymmetric encryption, a secure channel from B_i to the auctioneer via TTP for later exchange of K_i is established. A well-known algorithm for asymmetric encryption is *RSA* [21]. B_i's digital signature on a document *doc* is described by $Sig_{B_i}(doc)$. This part fulfills the requirements concerning message integrity, data origin authentication and non-repudiation.

2 In the second step, TTP confirms the receipt of the message obtained in the previous step. In order to do this, TTP replies a digital signature on the received message.

3 In the next step, TTP extracts some parts of the message obtained in the first step and creates a bid to be forwarded to A. This bid contains the following elements:

$$bid_i = auction\_details,\ encr_{K_i}(amount_i), bidID_i, \\ Sig_{TTP}(auction\_details,\ encr_{K_i}(amount_i), bidID_i).$$

With bid_i, the auctioneer A possesses a commitment concerning the amount of money B_i is willing to pay without knowing the amount. This means that neither B_i nor TTP are able to change this amount afterwards. Furthermore, signing the bid by TTP meets the requirement of non-repudiation. In addition, B_i's identity remains unknown to the auctioneer. Thereby, the requirement of anonymity remains fulfilled. The $bidID_i$ is selected by the TTP and will be used afterwards for easy re-identification of bid_i. Thus, the $bidID_i$ has to be unique.

4 In this step, the auctioneer informs TTP that he has included the received bid in the actual auction by replying a signed declaration. Thereby, TTP is ensured that bid_i was received and will also be considered in the auction. Furthermore, TTP —and therewith B_i— has an evidence in a possible case of dispute that bid_i has to be considered in the winner determination phase.

5 TTP passes the received confirmation to B_i after having signed it again. Thereby, the latter knows that TTP has executed his order properly. This step is not mandatory. Since B_i trusts TTP this message serves more the purpose of notification than that of evidence.

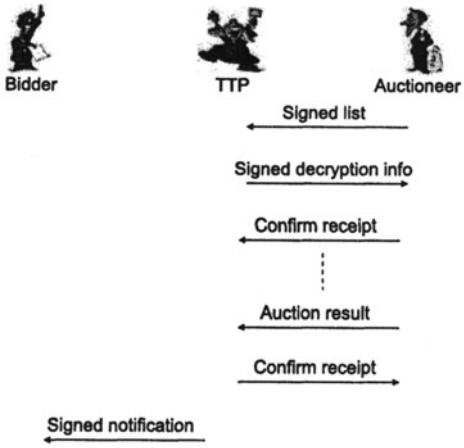

Figure 5. Protocol for the winner determination phase

Let us assume that the auctioneer receives n bids via m TTPs with $1 \leq m \leq n$ during the bid collection phase. After the end of the bid collection phase, the winner determination phase starts. In this phase, the involved parties continue with the following protocol:

6 After having collected n bids via m TTPs, the auctioneer composes a new message $list$ containing the $auction\_details$ referencing to the corresponding auction, all the received ciphertexts of the bid amounts $amount_1, \ldots, amount_n$, the bid identifications $bidID_1, \ldots, bidID_n$, and his signature on all these variables.

$$\begin{aligned} list \;=\; & auction\_details, \\ & encr_{K_1}(amount_1), bidID_1, \ldots, encr_{K_n}(amount_n), bidID_n, \\ & Sig_A\,(auction\_details, \\ & encr_{K_1}(amount_1), bidID_1, \ldots, encr_{K_n}(amount_n), bidID_n)\,. \end{aligned}$$

By this message, the auctioneer creates a commitment on all the encrypted bids he received. After the generation of this message, he distributes it to all the TTPs involved in the auction. Thereby, each TTP is able to verify whether all the bids submitted by himself are taken into account in the auction. If not all the bids are contained in $list$ the TTP can complain using the evidence that he received in protocol step 4. The same evidence can also be used in the case if one TTP does not receive $list$ in time. The time constraints are known to all participants by the auction rules.

7 Upon receipt and positive verification of $list$, all involved TTP_i for $i = 1, \ldots, m$ generate a new message $resolve\_info$ containing —beside others— the secured decryption keys for all the encrypted bids with identities $bidID_1$,

$\ldots, bidID_{i_l}$ sent by the same TTP_i where $\{i_1, \ldots, i_l\} \subset \{1, \ldots, n\}$. Furthermore, the message contains the TTP's signature on this content.

$$\begin{aligned} resolve\_info \;=\; & auction\_details, \\ & E_{pk_A}(K_{i_1}), bidID_{i_1}, \ldots, E_{pk_A}(K_{i_l}), bidID_{i_l}, \\ & Sig_{TTP_i}\,(auction\_details, \\ & E_{pk_A}(K_{i_1}), bidID_{i_1}, \ldots, E_{pk_A}(K_{i_l}), bidID_{i_l})\,. \end{aligned}$$

In the case in which a TTP does not send his message in time the auctioneer can request the corresponding $resolve\_info$ using the evidence of step 3.

8 Upon receipt of the message $resolve\_info$, the auctioneer confirms the receipt by replying a signature on this. This message assures the TTP that the auctioneer has really received the correct information.

After the auctioneer has collected all the messages $resolve\_info$ from the m different TTPs he can start the auction resolution in order to determine the winner, i.e., to find the highest amount. In the case of two or more coinciding bid amounts, there can be some further rules to be applied for the auction resolution. For the sake of simplicity and without restricting generality, we assume that there is a unique highest bid amount. In order to execute the winner determination, the auctioneer applies the key K_i to $encr_{K_i}(amount_i)$ for $i = 1, \ldots, n$. K_i is obtained by decryption of $E_{pk_A}(K_i)$ with his secret key sk_A. With this information, the auctioneer is able to compare the amounts which leads to the determination of the winner in the auction without the possibility to manipulate the result of the auction. He composes a message $result$ in which the winning bid —say bid_i— with $amount_{max} = amount_i$ is published beside the remaining $n - 1$ bids. With revealing this information, all further parties involved in the auction are able to verify that the auctioneer executed the auction correctly. Since the auctioneer has given a commitment on the encrypted bids in step 6 there is no way to introduce later new bids of other bidders or to manipulate the amount of existing bids. This reasoning is based on the assumption that it is not possible for an auctioneer with a colluding bidder B_j to find a key $\tilde{K}$ that decrypts the committed value $encr_{K_j}(amount_j)$ to the decryption result $amount$ that is greater than $amount_{max}$. In general, this can be achieved by the introduction of some redundancy in the representation of $amount_i$ for $i = 1, \ldots, n$.

9 The auctioneer composes a message $result$ to be sent to all TTPs participating in the auction. By this message, all TTPs can verify the correctness of the winner determination process.

$$\begin{aligned} result \;=\; & auction\_details, \\ & K_1, amount_1, bidID_1, \end{aligned}$$

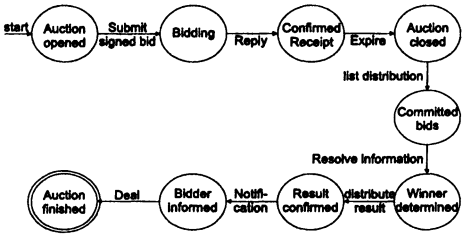

Figure 6. Transitions for sealed-bid auction

$$\vdots$$
$$K_i, amount_i, bidID_i, \quad \longleftarrow \text{ winner}$$
$$\vdots$$
$$K_n, amount_n, bidID_n,$$
$$Sig_{Auc}(auction\_details, K_1, amount_1, bidID_1, \ldots,$$
$$K_n, amount_n, bidID_n)$$

In the verification, a TTP checks if all the parameter values sent by his own are properly contained in the message *result*. Additionally, they can apply the keys K_i to their corresponding ciphertexts $encr_{K_i}(amount_i)$ for $i = 1, \ldots, n$ to obtain the values of $amount_i$. By the $bidID_i$, the verifiers are able to identify the bids sent by their own. Furthermore, all TTPs are able to reconstruct the winner determination. If the auctioneer tried to manipulate the winner determination, this can be detected.

10 In this step, the TTP confirms that he received the message *result* and that he accepts the result of the auction by sending a signed reply.

11 In the last step of the protocol, the TTP informs the bidder about the result of the auction. The message to be exchanged depends on the fact whether the receiving bidder won the auction or not.

Figure 5 depicts the transitions of the here presented sealed-bid auction. In all the steps that were performed during the auction the identities of the bidders remain hidden to the auctioneer. Thereby, we have fulfilled the requirement of anonymity at the same level at which this is also fulfilled in real world auctions. Therein, agents can operate on behalf of their clients. The subsequent steps such as shipment and payment are outside the auction itself. But even there, dependent on the services offered by the TTP these steps can be performed via the TTP. Thus, the winner can remain anonymous to the auctioneer also after the auction finished.

The protocol was designed to keep the overhead for computation, communication, and the number of required components, e.g., servers, small. Further-

more, the presented auction approach that focuses on a single-round sealed-bid auction can easily be adapted to the need of multi-round auctions.

5. Related Work

In general, the World Wide Web provides a ubiquitous platform for the execution of electronic auctions. In [11], a framework of constituting elements of auctions is presented and the impact of the Web on the proliferation of auctions is discussed. A short discussion on auctions' benefits and a description of the goods and services traded in auctions is given in [25].

Franklin and *Reiter* present a solution in [5] which is based on a distributed system approach in which the security requirements are fulfilled as long as not too many out of the set of auction servers operate maliciously and do not collude. In our context, the requirement for multiple servers is not suitable for small companies intending the role of an auctioneer. Furthermore in order to prevent collusions between these servers they have to be offered and maintained by different parties.

In [8], an adaption of the first price and second price sealed-bid auctions to computational environments is presented. Like in [5], the privacy of submitted bids is preserved by using a form of secure distributed computation. The mechanism ensures that the auctioneers and participants (except for the winner) will be completely unaware of the non-winning bids. The solution of [10] considers multiple auctioneer servers and multi-round auctions. In [14], *Kumar* and *Feldman* describe a variety of commonly used auction mechanisms and present a software architecture for electronic auctions. Other work in the area of electronic auctions with focus on security aspects was done in [17, 1, 24, 23]. In [28], a method to earn strategies for multilateral negotiations such as auctions is presented.

The economic design of auction protocols has been widely discussed in auction literature. The objective is to design auctions on solid economic principles and to ensure that participants have incentives to bid as they truly value the item. An overview and analysis of the underlying economic principles is given in [15]. In [27] Vickrey has designed a sealed-bid second price auction that is incentive compatible, and maximizes consumer surplus. The analysis and investigation of the economic properties of auctions usually assumes a trustworthy auctioneer or auction house. With the application of auctions to the Internet this assumption can no longer be maintained. The application of auctions to computational environments and its implications are discussed in [13, 26]. In [22], problems and limitations of automated Vickrey auctions are discussed and means to circumvent them are developed.

6. Conclusion

We have introduced two solutions how the CFT protocol can be used in mediated eCommerce environments. It has been shown that a naive adoption of the CFT to mediated eCommerce is subject to security attacks like eavesdropping of messages, masquerading of identity, message manipulation, and repudiation of messages. The new secure CFT protocol introduced in Section 3 shows how the basic CFT can be supplemented with non-repudiable communications including authentication of origin, message integrity, and transaction authentication. This approach ensures that no new manipulation possibilities are introduced by the realization of the CFT protocol with computer support.

Our analysis has also revealed that further drawbacks of the CFT protocol surface in the economic design of the protocol. The main source of manipulation is caused by the unequal distribution of knowledge and of control between buyers and sellers within the CFT process. The secure sealed-bid auction protocol introduced in Section 4 provides an interesting alternative to a CFT because it overcomes these limitations. It provides means for a bidder to verify the result of the auction process, and thus, introduces trust among the participants because a correct application of the winner determination rules is guaranteed.

Future work will be devoted to the specification of winner determination rules and a technical infrastructure detailing how bidders can monitor their application. This will result in a secure sealed-bid auction mechanism that allows for more flexible auctions compared to the existing mechanisms where the winner is solely determined via the best price.

References

[1] Christian Cachin. Efficient private bidding and auctions with an oblivious third party. In *5th ACM Conference on Computer and Communications Security*, November 1999.

[2] David Chaum. The dining cryptographers problem: Unconditional sender and recipient untraceability. *Journal of Cryptology*, I(1), 1988.

[3] David L. Chaum. Security without identification: transaction systems to make big brother obsolete. *Communications of the ACM*, 28(10):1030–1044, October 1985.

[4] Whitfield Diffie and Martin Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, IT-22(6):644–654, November 1976.

[5] Matthew K. Franklin and Michael K. Reiter. The design and implementation of a secure auction service. In *Proceedings of the IEEE Symposium on Research in Security and Privacy*. IEEE Computer Society Press, May 1995.

[6] Alan O. Freier, Philip Karlton, and Paul C. Kocher. The SSL protocol version 3.0. Internet Draft, November 1996.

[7] David Goldschlag, Michael Reed, and Paul Syverson. Hiding routing information. In *Information Hiding*, number 1174 in Lecture Notes in Computer Science. Springer-Verlag, Berlin Germany, 1996.

[8] M. Harkavy, H. Kikuchi, and J. D. Tygar. Auctions with private bids. In *Third USENIX Workshop on Electronic Commerce*, Boston, USA, September 1998.

[9] ISO/IEC. Information technology – Open Systems Interconnection – The directory: Authentication framework, 1995.

[10] Hiroaki Kikuchi, Michael Harkavy, and J.D. Tygar. Multi-round anonymous auction protocols. In *Proceedings of the first IEEE Workshop on Dependable and Real-Time E-Commerce Systems*, jun 1998.

[11] Stefan Klein. *The Emergence of Auctions on the World Wide Web*. Springer-Verlag, Berlin Germany, 2000.

[12] M. Kumar and S. I. Feldman. Business negotiations on the internet. Iac reports, IBM T.J. Watson Research Center, March 1998.

[13] M. Kumar and S. I. Feldman. Internet auctions. Iac reports, IBM T.J. Watson Research Center, November 1998.

[14] Manoj Kumar and Stuart I. Feldman. Internet auctions. In *Proceedings of the 3rd USENIX Workshop on Electronic Commerce*, aug 1998.

[15] R. P. McAfee and J. McMillan. Auctions and bidding. *Journal of Economic Literature*, XXV:699–738, 1987.

[16] Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone. *Handbook of applied cryptography*. CRC Press series on discrete mathematics and its applications. CRC Press, 1997. ISBN 0-8493-8523-7.

[17] Moni Naor, Benny Pinkas, and Reuben Sumner. Privacy preserving auctions and mechanism design. In *Proceedings of the first ACM Conference on Electronic Commerce*, nov 1999.

[18] Duane Nickull and Brian Eisenberg. ebxml technical architecture specification. Technical report, UN/CEFACT, October 2000.

[19] U.S. National Institute of Standards and Technology NIST. The digital signature standard DSS. FIPS PUB 186-2, January 2000.

[20] Michael Reed, Paul Syverson, and David Goldschlag. Anonymous connections and onion routing. *IEEE Journal on Selected Areas in Communications*, 16(4), 1998.

[21] Ron L. Rivest, Adi Shamir, and Leonard M. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, February 1978.

[22] T. W. Sandholm. Limitations of the Vickrey auction in computational multiagent systems. In Victor Lesser, editor, *Proc. of the first Int. Conference on Multi-Agent Systems*. The MIT Press, Cambridge, MA, 1995.

[23] Frank Stajano and Ross Anderson. The cocaine auction protocol: On the power of anonymous broadcast. In *Proceedings of Financial Cryptography 99*, number 1768 in Lecture Notes in Computer Science. Springer-Verlag, Berlin Germany, 1999.

[24] Stuart G. Stubblebine and Paul F. Syverson. Fair on-line auctions without special trusted parties. In *Proceedings of Financial Cryptography 99*, number 1648 in Lecture Notes in Computer Science. Springer-Verlag, Berlin Germany, 1999.

[25] Efraim Turban. Auctions and bidding on the internet: An assessment. *Electronic Markets*, 7(4), 1997.

[26] J. D. Tygar. Atomicity versus anonymity: Distributed transactions for electronic commerce. In *Proc. of the 24th Int. Conference on Very Large Databases*, pages 1–10, New York City, USA, 1998.

[27] W. Vickrey. Counter specification, auctions, and competitive sealed tenders. *The Journal of Finance*, pages 9–37, 1961.

[28] E. Wolff, M.T. Tu, and W. Lamersdorf. Using genetic algorithms to enable automated auctions. In *Electronic Commerce and Web Technologies*, number 1875 in Lecture Notes in Computer Science. Springer-Verlag, Berlin Germany, 2000.