Anonymous, Yet Trustworthy Auctions

Prasit Bikash Chanda[1], Vincent Naessens[2], and Bart De Decker[1]

[1] K.U.Leuven, Dept. of Computer Science, DistriNet-SecAnon
{Prasit.Chanda,Bart.DeDecker}@cs.kuleuven.be
[2] Katholieke Hogeschool Sint-Lieven, Dept. of Industrial Engineering, Mobility & Security
Vincent.Naessens@kahosl.be

Abstract. An auction is an inevitable market mechanism to setup prices of goods or services in a competitive and dynamic environment. Anonymity of bidders is required to conceal their business strategies from competitors. However, it is also essential to provide the seller guarantees that a bidder is trustworthy and competent enough to perform certain tasks (e.g transports). This paper proposes an auction protocol where bidders will participate anonymously, yet prove to be trustworthy and competent and can be held accountable towards auctioneers and sellers. Moreover, the protocol introduces promises, bonuses and compensations to ensure the best price for the sellers, extra profit for bidders and opportunities for newcomers in the business. It also handles ties, and copes with last minute bidding. Finally, the auction's fair proceedings and outcome can be verified by everyone.

Keywords: Auction, Credential, Anonymity, Trust, Distributed Systems

1 Introduction

The logistic management of a typical organization is an extension of the Supply Chain Management (SCM). SCM is the complete picture of planning, implementing and controlling of products or services across the business boundary to an extended environment composed of dealers, wholesalers, end-users and suppliers. It also includes management of transportation strategies (e.g. on-time delivery, reducing cost). Currently, organizations face numerous challenges regarding this issue. Hence, they are inclined towards outsourcing their transport activities to a fourth party organization 4PL[3]. These 4PL have short or long term contracts with third party organizations 3PL[4] and independent transport firms. The 4PL has to manage shipments within predefined time periods (e.g. 24 hours) through 3PL organizations or transport firms to meet the customers' demands. However, in a fast-paced dynamic and distributed setting, it is not sufficient to have short or long term contracts. The 4PL will also have to choose transport firms

[3] A Fourth Party Logistics provider (4PL) is a supply chain service provider that searches the best transport solutions for its clients, typically without using own assets or resources.

[4] Third Party Logistics (3PL) is the supply chain practice where one or more transport functions of a firm are outsourced to a 3PL provider.

from open markets to cope with the specified scenario. Hence, auctions are needed to hire freelance transport firms from these markets. In such a setting, the anonymity of the transport firm is important, both to ensure the best price for the 4PL and to hide its business strategies from its competitors (e.g. increase its market share, open up new routes, keep its workforce busy, . . .). However, anonymity may lead to abuse. For instance, an anonymous transport firm may win a deal to transport freights on a certain route in which it has no experience. Hence, the 4PL and the auction houses need guarantees from the transport firms that they are trustworthy and competent enough to perform a certain transport. Besides, these transport firms must be held accountable for carrying out such transports.

This paper is organized as follows. Sections 2 and 3 describe the requirements, assumptions and notations. Then, in section 4, an overview of the building blocks is given. Sections 5 and 6 deal with guarantees, bonuses and compensations. Section 7 gives a detailed design of the auction system. In section 8, the system is evaluated and section 9 describes related work. A conclusion and suggestions for future work can be found in section 10.

2 Requirements

The main goal of this paper is to design an efficient auction system, that allows bidders to remain anonymous, but offers sufficient guarantees to the sellers.

The auction should fulfill several requirements. These are divided into functional requirements and privacy, security and trust requirements.

Functional Requirements

- (F1) *Best price*: An auction should guarantee the seller the best price.
- (F2) *Efficiency*: The auction system should be simple and introduce no extra overhead or delays; therefore, multi-round auctions are not acceptable.
- (F3) *Fairness*: The auction system should be fair. Everybody should be able to verify the auction's proceedings and outcome.
- (F4) *Openness*: Every prospective bidder should be able to register for the auction system. Every registered bidder can participate in an auction if he fulfills the auction's prerequisites.
- (F5) *Generic*: The trust paradigms used by the system should be generic and extensible.

Privacy, Security and Trust Requirements

- (PST1) *Bidder's Anonymity*: Bidders will remain anonymous to hide their business strategies. Only the seller will eventually learn the true identity of the winning bidder.
- (PST2) *Guarantees for Seller and Auctioneer*: The seller or auctioneer should be ensured of the trustworthiness of the bidders. The seller should be able to define prerequisites that must be fulfilled by the bidders. The auctioneer will verify these guarantees when bids are collected.

- (PST3) *Accountability*: Each party within the system can be held liable for its actions.
- (PST4) *Selective Disclosure*: The bidder can decide which attributes (or properties thereof) of his credential will be disclosed during an auction.

3 Assumptions and Notations

In the sequel of this paper, the following **assumptions** are made:

RSA Key Pair and X.509 Certificates. The protocol assumes that each entity in the protocol holds one or more RSA key pairs [21]. RSA key pairs consist of a public key and a private key. The private key is kept secret and the public key will be certified in (X.509) certificates [19] issued by a trusted Certification Authority (CA).

Entity bound credentials. Each credential is bound to its owner. Sharing of credentials can be discouraged by including a valuable secret (e.g. credit card number) in the credential.

In the sequel of this paper, the following **notations** are used:

- $X \rightarrow Y$: *data* (resp. $X \leftarrow Y$: *data*) denotes that X sends *data* to Y (resp. X receives *data* from Y).
- $X \rightleftharpoons Y$: $(res_X; res_Y) \leftarrow \mathsf{protocol}(Common; Input_X; Input_Y)$ is used throughout the paper and represents a generic protocol where $Input_X$ and $Input_Y$ are inputs from X resp. Y. *Common* is known to both X and Y. The protocol produces the results res_X for X and res_Y for Y.
- $\mathsf{Sig}_X(Data)$ represents the signature on *Data* with X's private signature key Pr^s_X.
- $\lceil\overline{X}\rceil$ (cloaked X) denotes that entity X is anonymous in a particular interaction.

4 Building Blocks

In this section, the major building blocks used in the auction system will be briefly described. We discuss *TLS/SSL connections*, *anonymous channels* and *anonymous credentials*.

TLS/SSL Connections. The protocol specifies that TLS connections [15] should be set up prior to any interaction between business entities. The following protocol is relevant:

- $X \rightleftharpoons Y$: $(id_Y; id_X) \leftarrow \mathsf{setupTLS}(Cert^a_X, Cert^a_Y; Pr^a_X; Pr^a_Y)$ represents the establishment of a TLS connection between X and Y. Here, id_X and id_Y are the identities of X and Y respectively, which are embedded in the certificates $Cert^a_X$ and $Cert^a_Y$. During the set-up, X and Y mutually authenticate. The TLS connection protects the confidentiality, integrity and authenticity of the exchanged information.

Anonymous Channels. The protocol also uses anonymous channels (e.g. through MIX networks or Onion Routing networks) during some interactions. Anonymous channels [16] basically hide the traffic patterns (*'Who sends to Whom'*). Such channels will ensure confidentiality and integrity as well. The following protocol is relevant:

- $\lceil\overline{X}\rceil \rightleftharpoons Y\text{: } (id_Y; \emptyset) \leftarrow \mathsf{setupAnonChannel}(Cert^a_Y; \emptyset; Pr^a_Y)$ represents the establishment of anonymous channel between X and Y. During the setup, Y authenticates towards X, while X remains anonymous. The Anonymous channel also protects the confidentiality and integrity of the exchanged information.

Anonymous Credentials. Anonymous credential systems [10, 11] allow for anonymous yet accountable transactions between users and organizations and allow for selective disclosure by showing only part of the credential attributes or properties thereof (e.g. when the credential contains an attribute `numberOfTransactions`, it is possible to prove that this number is greater than 70 while hiding its actual value and the values of all the other attributes). In the Idemix system [10], different usages of the same credential are unlinkable, except when unique attribute values are revealed. Credentials can have features such as an expiry date, the allowed number of times it can be shown or the possibility to be revoked. Note that an anonymous channel is required for every credential show to provide anonymity at the network layer. The following protocols are relevant:

- $X \rightleftharpoons I\text{: } (Cred_X; \emptyset) \leftarrow \mathsf{issueCred}(\textit{trust values}, id_X, Cert^c_I; \emptyset; Pr^c_I)$ represents the protocol where a trusted credential issuer I issues a credential $Cred_X$ to a entity X. The anonymous credential $Cred_X$ contains an expiry date, the identity (id_X) of the holder and possibly other attributes (*trust values*) and is signed with I's private key Pr^c_I.

- $\lceil\overline{X}\rceil \rightleftharpoons Y\text{: } (trans_X;\ trans_Y) \leftarrow \mathsf{showCred}(props, Cert^c_I; Cred_X; \emptyset)\{data\}$ represents the protocol where an anonymous entity X proves to the entity Y the possession of a valid credential $Cred_X$, issued by I. X will selectively disclose attributes (or properties thereof) of $Cred_X$ described in *props* (see also section 6). During the credential show, X can sign *data* with its $Cred_X$ creating a provable link between the proof and *data*. The protocol returns the transcripts $trans_X$ and $trans_Y$.

  Additionally, transcripts resulting from showCred can be deanonymized by a predetermined trusted third party D. In this case, the credential owner (the prover, X) sends during the credential show its identity (verifiably encrypted [14] with the public key of D) to the verifier Y. Since the identity is also embedded in the credential, the owner can prove that the correct value has been encrypted, without actually disclosing the identity to the verifier. Deanonymization is used to determine the identity of the winner of an auction. Also, in case of abuse or disputes, the identity of the credential holder can be recovered.

5 Guarantees

Sellers want some guarantees from bidders: e.g. the seller may want that the bidder is specialized in transporting fragile goods, that the bidder has experience in delivering goods in a particular foreign country, that he is in business for more than 10 years, or that he has carried out already more than 500 transports.

These characteristics of the bidder are embedded in a credential and are proven during the bidding. The values are certified by a trusted third party (TTP) (the credential issuer). We use a simple but realistic trust model: most likely, the TTP will be a transportation association. We do not impose the existence of just one TTP. In fact, there may be several associations, and sellers can specify which TTPs they trust. Depending on the certification procedures used by these TTPs, sellers may have less or more trust in these TTPs and require weaker or stronger guarantees. For simplicity reasons, however, we assume in this paper that only one TTP exists. Extending the protocols to more TTPs is just straightforward.

In this paper, we use characteristics which can be easily verified by the TTP: years in business, total number of transactions, average value of transported goods, total value of transported goods, specialties in handling particular goods, experience in routes, etc. These can be derived from the charter of foundation of the company and from signed contracts. The TTP can use an *aging* mechanism to make sure that some accumulating values remain accurate: $\textit{new} = \alpha \times \textit{old} + \textit{evidence}$, with $\alpha < 1$.

It is also possible to add characteristics that are related to the transporter's *reputation*, such as: reliability (e.g. expressed as the percentage of timely and undamaged deliveries out of the total number of transports) or satisfaction of the seller (e.g. a rating from 0 to 10). However, such values require a feedback system that is foolproof, and may involve trusted arbiters in case of disputes. For instance, the transportation association may play the role of mediator, and if the dispute cannot be solved, a judge may return the final verdict. In this paper, we ignore such disputes and refer to future research.

To boostrap the system, bidders (transporters) have to register themselves with a TTP, the credential issuer R (see also section 7) and receive in return an anonymous credential in which the transporter's characteristics (trust values) are embedded. The relevant simplified functions that apply to guarantees are as follows; both are exclusively used by the registrar R:

- *trust values* ← calcTrustValues*(evidence, certificates, guarantees)* is a function that calculates the trust values based on information provided by a prospective bidder, such as: verifiable evidence, certificates issued by trusted CAs and other guarantees signed by an external trusted party (e.g. Government Institute or a non-governmental organization).
- *new trust values* ← updateTrustValues*(old trust values, new transactions)* is a function that calculates the *new trust values* when $\textit{Cred}_B$ expires and needs to be re-issued. The function calculates the *new trust values* according to the record(s) received. The records contain information about B's previous transactions signed *anonymously* by the sellers. Hence, the TTP does not learn anything about business relations between the bidders and the sellers.

6 Bonuses and Compensations

Winning bidders can get a **bonus** if they are prepared to prove more than is required (e.g. proving more guarantees than the auction prerequisites) or if they promise additional services (e.g. late night delivery). The seller determines before the auction starts which bonuses can be earned.

If the seller agrees, bidders that do not fulfill the prerequisites may nevertheless be allowed to participate in an auction if they fulfill less stringent requirements. However, they can only participate in exchange for a **compensation**. When the contract is signed the bid will be decreased with that compensation. This way, new participants with low or no guarantee values can participate but at a lower price. For instance, a particular auction prerequisite states that a bidder should have completed at least 50 transports during its business lifetime. However, the seller may allow bidders with only 20 transports to participate but they will have to compensate their lack of experience with a penalty of say 1000 EUR. The latter can be used by the seller to take an extra insurance.

Only the bids are taken into account for determining the winner of the auction. However, when the contract is signed, the bid_B is increased with the bonuses and decremented with the compensations. The relevant simplified functions are as follows:

- *(bid, promises, props)* $\leftarrow$ determineBidProps*(description, best bid)* represents the User Interface (UI) where a bidder B prepares a scheme (e.g. bid to offer, promises to bear and properties to prove) based on the auction description (i.e. prerequisites, bonuses, and compensations) and the best bid so far.
- *(bonus, compensation)* $\leftarrow$ calcBonusCompensation*(description, props, promises)* is a function (used by the seller) to determine the bonus and compensation based on the description of the auction, the properties (*props*) proved by the bidder and promises made by the bidder.

7 Design of an Anonymous, Yet Trustworthy Auction System

Initially, bidders have to register (once) with the registrar R, a trusted credential issuer. During the registration, bidders have to provide R with certificates and other evidence of experience signed by external trusted parties. Upon verification, the issuer delivers an anonymous credential to the bidders. With these anonymous credentials, bidders can anonymously participate in auctions and prove that they are trustworthy and competent enough to carry out certain transports. The seller defines the auction prerequisites, the bonuses and compensations and forwards this auction description to the auctioneer. The auctioneer publishes the description in the public domain. Bidders may make promises to earn bonuses and/or agree to compensate (when they do not satisfy the auction prerequisites and when this is allowed by the seller). Bidders can bid as many times as they want as long as the auction is not closed. Each bid is signed with the credential. The auctioneer publishes every bid transcript in the public domain so that everyone can verify the fair proceedings of the auction.

After a predefined deadline, the auction is closed and the winner is selected based on the **lowest bid**. The auctioneer requests the trusted deanonymizer to identify the winner (i.e. deanonymize the winning transcript). Note that, the winner's identity is only revealed to the seller. Later, the seller and winner will sign the transport contract.

After completing a transport, the seller will confirm the transport[5], which will be used for updating the trust values in the credential.

7.1 Initial Certification

The auction protocol involves several parties: Bidder(s) denoted by **B** (e.g. Skippers, Charter Truck Companies, 3PL), a Registrar (**R**) (e.g. a transport association), an Auctioneer (**A**) (e.g. an independent auction house), a Seller (**S**) (e.g. 4PL), a Bulletin Board (**BB**) and a deanonymizer (**D**). **R**, **A** and **D** are trusted third parties. The winner, which is the bidder with the lowest bid is denoted by **W**. We assume that each entity E has one or more key pairs (Pk_E,Pr_E) of which the public key (Pk_E) is certified in a certificate ($Cert_E$) by a trusted certification authority (**CA**). (A superscript refers to its usage: e for encryption, a for authentication, s for signing and c for issuing credentials.)

7.2 Registration and Trust Calculation

A prospective bidder B must first register with the registrar R. The bidder presents certificates and other evidence of experience that will be used by the R to calculate guarantees (trust and business parameters). R will issue a credential that includes as attributes these guarantees (*trust values*) and the identity information (id_B). See Table 1 for details.

B	$\rightleftharpoons$ R :	(id_R; id_B) $\leftarrow$ setupTLS($Cert^a_B$,$Cert^a_R$; Pr^a_B; Pr^a_R)
B	$\rightarrow$ R :	guarantees, certificates, evidence, ...
	R :	*trust values* $\leftarrow$ calcTrustValues(evidence, certificates, guarantees)
B	$\rightleftharpoons$ R :	($Cred_B$;$\emptyset$) $\leftarrow$ issueCred(*trust values*, id_B, $Cert^c_R$; $\emptyset$; Pr^c_R)

Table 1. Registration and Trust Calculation

Similarly, a prospective seller S has to register with R and receives as a result an anonymous credential $Cred_S$ with which S can confirm anonymously a transport.

7.3 Auctions

Figure 1 gives an example of a description of an auction, including the prerequisites, bonuses and compensations. The prerequisites specify that the bidder's credential needs to be issued by `TrucAssoc`, and that the bidder should be in business for at least 5 years and be specialized in transporting fragile goods. A bonus of 1000 EUR is awarded if the goods can be delivered within 2 days and an extra bonus of 500 EUR for early delivery (before 6am). A compensation of 2000 EUR is requested for newcomers (between 2 and 5 years in business) or if the bidder not specialized in this kind of transport.

[5] If the credentials contain reputation-based values, the seller may also evaluate the transport. However, in case of disputes, a trusted arbiter may be involved.

auction: transport 10 pallets of crystalware from Leuven to Rome
prerequisites: `certifier` = TrucAssoc, `specialty` = fragile goods AND `YearsInBusiness` > 5
bonus: 1000 EUR **if** `delivery` <= **today** + 2 **days**
bonus: 500 EUR **if** `delivery` < 6 **am**
compensation: 1000 EUR **if** (2 < `YearsInBusiness` < 5) OR **no** `specialty`

Fig. 1. Description, prerequisites, bonus and compensation of an Auction

Creation of a new Auction. A seller S submits a description of a new auction and a certificate[6] Cert_S^e to the auctioneer A. The description of the auction, together with the auction policy and deadline, is posted on the bulletin board BB. See Table 2 for details.

S	: $\mathit{descr}_{auc} \leftarrow (\mathit{transport\ description}, \mathit{prerequisites}, \mathit{bonuses}, \mathit{compensations})$
S $\rightleftharpoons$ A	: $(\mathit{id}_A; \mathit{id}_S) \leftarrow \mathsf{setupTLS}(\mathit{Cert}_S^a, \mathit{Cert}_A^a; \mathit{Pr}_S^a; \mathit{Pr}_A^a)$
S $\rightarrow$ A	: $\mathsf{Sig}_S(\mathit{descr}_{auc}, \mathit{Cert}_S^e), \mathit{Cert}_S^s$
BB $\leftarrow$ A	: $\mathsf{Sig}_A(\mathsf{Sig}_S(\mathit{descr}_{auc}, \mathit{Cert}_S^e), \mathit{policy}, \mathit{deadline}_{auc}), \mathit{Cert}_S^s, \mathit{Cert}_A^s$
BB	: publish $\mathsf{Sig}_A(\mathsf{Sig}_S(\mathit{descr}_{auc}, \mathit{Cert}_S^e), \mathit{policy}, \mathit{deadline}_{auc}), \mathit{Cert}_S^s, \mathit{Cert}_A^s$

Table 2. Creation of a new Auction

Anonymous Bidding. A potential bidder B retrieves the description of an open auction from BB and bids anonymously to the auctioneer A. The bidding consists of a credential-show of an anonymous credential (Cred_B). During the show, the prerequisites are proven and possibly other properties which give right to bonuses. Besides the bid itself, the bidder can also sign extra promises, with which extra bonuses can be earned. The auctioneer A posts the transcript of the bid on BB and returns a receipt to B. See Table 3 for details. Note that trans_A contains a verifiable encryption of the identity of B with the public key of the deanonymizer D ($\mathsf{VEnc}_D(\mathit{id}_B)$).

Since the auction is multithreaded, simultaneous bids are possible. Therefore, as soon as a new thread is created to handle a new bid, a unique timestamp (t_s) is assigned to that thread. The bidder will sign both t_s and bid_B with his credential. Note that the bid_B, *promises*, *props* and t_s can be recovered from the transcripts.

The auctioneer will check whether the bid is better than any bid posted on the BB prior to time t_s. In order to avoid that some bidders start a bid, but only finish the bidding at the end of the auction period, each bid must be finished within a predefined time limit. If that time limit expires, the bidding is aborted. In order to avoid that some bidders do a final bid at the end of the auction period which is only marginally better than the best bid, the auction policy should define minimum deltas to be used in the different time frames.

[6] The certificate will be used later (by the deanonymizer) to encrypt the winner's identity.

$\lceil\overline{\text{B}}\rceil$	$\rightarrow$ BB	: request type of transports
$\lceil\overline{\text{B}}\rceil$	$\leftarrow$ BB	: $\mathsf{Sig}_A(\mathsf{Sig}_S(descr_{auc}, Cert^e_S), policy, deadline_{auc})$, $Cert^s_S$, $Cert^s_A$
For every bid:		
$\lceil\overline{\text{B}}\rceil$	$\rightleftharpoons$ A	: $(id_A; \emptyset) \leftarrow \mathsf{setupAnonChannel}(Cert^a_A; \emptyset; Pr^a_A)$
$\lceil\overline{\text{B}}\rceil$	$\leftarrow$ A	: "Hello anonymous bidder", t_s, $descr_{auc}$, Best Bid, $deadline_{auc}$
$\lceil\overline{\text{B}}\rceil$		: $(bid_B, props, promises) \leftarrow \mathsf{determineBidProps}(descr_{auc},$ Best Bid$)$
$\lceil\overline{\text{B}}\rceil$	$\rightleftharpoons$ A	: $(trans_B; trans_A) \leftarrow \mathsf{showCred}(props, Cert^c_R; Cred_B; \emptyset)\{bid_B, promises, t_s\}$
$\lceil\overline{\text{B}}\rceil$	$\leftarrow$ A	: $\mathsf{Sig}_A(trans_A)$
A	$\rightarrow$ BB	: $\mathsf{Sig}_A(trans_A)$
	BB	: publish $\mathsf{Sig}_A(trans_A)$

Table 3. Anonymous Bidding

`Example`: [00:00–01:00], -5%; [01:00–01:45], -10%; [01:45–End], -15%. This policy specifies that during the first hour of the auction, each bid should be at least 5% better than the previous best bid. Then, during the next 45 minutes, each bid should be at least 10% better than the previous best bid. After that, bids should be 15% better than the last best bid.

Only the best bid published before t_s is taken into account, so it is possible that simultaneous bids do not differ that much (in that case, a later higher bid will be ignored).

Selection of the Winner and Contract Signing. Once the deadline of the auction has expired, the auctioneer A selects the first lowest bid and sends the transcript of the bid to the deanonymizer D. D recovers the identity of W, and returns that identity (encrypted with the public key of the seller S) to the auctioneer who forwards it to S. The seller will calculate the bonus and compensation and contact W to sign a contract. R is also kept informed by D about a W's transport engagement (i.e. anonymized[7] details of the task (such as the route, type of goods, the total transaction value, etc.). The transport has to be confirmed (e.g. done or canceled) before the deadline expires (see Table 4). Note that *reportID* is a unique number used to match a transport report with a transport engagement.

End of Contract. When a transaction between S and W has been completed, S will confirm the transport (e.g. done or canceled). If the bidder's credential also contains reputation-based values, then S and W should also agree on the outcome (late/timely delivery, damaged/undamaged goods, etc.). However, if they cannot agree a trusted arbiter will have to step in.

The result (confirmation and possibly assessment) is signed by W and this signature together with the reportID (provided by D when the winner was announced to S) is signed anonymously by S during a credential show to R, which will –after some checks: signatures, outcome and reportID are valid– add it to the list of reported transports of W. Finally, a receipt (i.e. the signed transcript of the credential show) is sent to W via S. See Table 5 for details.

[7] The details are generalized so that they cannot identify a specific auction.

A			: $\mathit{trans}_W \leftarrow \mathsf{selectFirstLowestBid}(\text{all bids})$
A	$\rightarrow$	BB	: $\mathsf{Sig}_A(\mathit{trans}_W, \text{"}winner\text{"})$
		BB	: post $\mathsf{Sig}_A(\mathit{trans}_W, \text{"}winner\text{"})$
A	$\rightleftharpoons$	D	: $(\mathit{id}_D; \mathit{id}_A) \leftarrow \mathsf{setupTLS}(\mathit{Cert}^a_A, \mathit{Cert}^a_D; \mathit{Pr}^a_A; \mathit{Pr}^a_D)$
A	$\rightarrow$	D	: $\mathsf{Sig}_A(\mathit{trans}_W, \mathsf{Sig}_S(\mathit{descr}_{auc}, \mathit{Cert}^e_S), \text{"}winner\text{"}), \mathit{Cert}^s_S, \mathit{Cert}^s_A$
		D	: $\mathit{id}_W \leftarrow \mathsf{Deanonymize}(\mathit{Pr}^e_D, \mathit{trans}_W)$
		D	: $(\mathit{reportID}, \mathit{summary}) \leftarrow \mathsf{genUniqueReportID}(\mathit{descr}_{auc})$
A	$\leftarrow$	D	: $\mathsf{Enc}_S(\mathsf{Sig}_D(\mathit{trans}_W, \mathit{id}_W, \text{"}winner\text{"}, \mathit{reportID})), \mathit{Cert}^s_D$
A	$\rightleftharpoons$	S	: $(\mathit{id}_S; \mathit{id}_A) \leftarrow \mathsf{setupTLS}(\mathit{Cert}^a_A, \mathit{Cert}^a_S; \mathit{Pr}^a_A; \mathit{Pr}^a_S)$
A	$\rightarrow$	S	: $\mathit{trans}_W, \mathsf{Enc}_S(\mathsf{Sig}_D(\mathit{trans}_W, \mathit{id}_W, \text{"}winner\text{"}, \mathit{reportID})), \mathit{Cert}^s_D$
S	$\rightleftharpoons$	W	: $(\mathit{id}_W; \mathit{id}_S) \leftarrow \mathsf{setupTLS}(\mathit{Cert}^a_S, \mathit{Cert}^a_W; \mathit{Pr}^a_S; \mathit{Pr}^a_W)$
S			: $\mathit{bid}_W \leftarrow \mathit{trans}_W.\mathit{bid}$
S			: $(\mathit{bonus}, \mathit{compensation}) \leftarrow \mathsf{calcBonusCompensation}(\mathit{descr}_{auc},$
			: $\mathit{trans}_W.\mathit{props}, \mathit{trans}_W.\mathit{promises})$
S	$\rightarrow$	W	: $\mathsf{Sig}_S(\mathit{contract}, \mathit{bid}_W + \mathit{bonus} - \mathit{compensation})$
S	$\leftarrow$	W	: $\mathsf{Sig}_W(\mathit{contract}, \mathit{bid}_W + \mathit{bonus} - \mathit{compensation})$
D	$\rightleftharpoons$	R	: $(\mathit{id}_R; \mathit{id}_D) \leftarrow \mathsf{setupTLS}(\mathit{Cert}^a_D, \mathit{Cert}^a_R; \mathit{Pr}^a_D; \mathit{Pr}^a_R)$
D	$\rightarrow$	R	: $\mathsf{Sig}_D(W, \mathit{reportID}, \mathit{summary}, \mathit{deadline}_{transport})$
		R	: append $\mathsf{Sig}_D(W, \mathit{reportID}, \mathit{summary}, \mathit{deadline}_{transport})$ to record$[W]$

Table 4. Selection of the winner

S	$\rightleftharpoons$	W	: $(\mathit{id}_W; \mathit{id}_S) \leftarrow \mathsf{setupTLS}(\mathit{Cert}^a_S, \mathit{Cert}^a_W; \mathit{Pr}^a_S; \mathit{Pr}^a_W)$
S	$\rightleftharpoons$	W	: $\mathit{result} \leftarrow \mathsf{agreeOutcome}()$
S	$\leftarrow$	W	: $\mathsf{Sig}_W(W, \mathit{result})$
$\lceil\overline{\mathrm{S}}\rceil$	$\rightleftharpoons$	R	: $(\mathit{id}_R; \emptyset) \leftarrow \mathsf{setupAnonChannel}(\mathit{Cert}^a_R; \emptyset; \mathit{Pr}^a_R)$
$\lceil\overline{\mathrm{S}}\rceil$	$\rightleftharpoons$	R	: $(\mathit{trans}_S; \mathit{trans}_R) \leftarrow \mathsf{showCred}(\mathit{Cert}^c_R; \mathit{Cred}_S; \emptyset)\{\mathsf{Sig}_W(W, \mathit{result}), \text{reportID}\}$
		R	: append trans_R to record$[W]$
$\lceil\overline{\mathrm{S}}\rceil$	$\leftarrow$	R	: $\mathsf{Sig}_R(\mathit{trans}_R, \text{"}OK\text{"}), \mathit{Cert}^s_R$
S	$\rightarrow$	W	: $\mathsf{Sig}_R(\mathit{trans}_R, \text{"}OK\text{"}), \mathit{Cert}^s_R$

Table 5. End of Contract

7.4 Updating Credentials

When a bidder's credential expires (typically, a credential will be valid for one or two months), the bidder will request a new credential from the registrar (R). The registrar will verify whether the outcome of all previous expired transactions (i.e. transactions for which the transport deadline has been exceeded) have been reported. If not, an investigation may be started. (See Table 6.)

8 Evaluation

The protocol is evaluated against the requirements of section 2.

B $\rightleftharpoons$ R	:	$(id_R; id_B) \leftarrow \mathsf{setupTLS}(Cert^a_B, Cert^a_R; Pr^a_B; Pr^a_R)$
R	:	*new trust values* $\leftarrow$ $\mathsf{updateTrustValues}$(old *trust values*,
	:	$\forall_i$ record[B].$result_i$)
R	:	$\forall_i$ delete record[B].$result_i$
B $\rightleftharpoons$ R	:	$(Cred_B;\emptyset) \leftarrow \mathsf{issueCred}$(*new trust values*, id_B; $\emptyset$; Pr^c_R)

Table 6. Updating Credential

(F1) Best price. Since bidders can bid anonymously, it is less likely that they restrain themselves when making a bid (they do not reveal their business strategies). Also, all bids are posted on a bulletin board. Hence, as long as the auction is open, a bidder can make a lower bid. The auction system has schemes for bonuses and compensations (see section 6). The bonus scheme increases the bidder's profits when the bidder is willing to provide extra services or prove extra guarantees. Similarly, the compensation scheme increases the seller's revenues (or reduces its risks) as it allows an unexperienced bidder (newcomer) to take part in an auction in exchange for a compensation. The winner is finally selected by sorting the bids according to their unique timestamp and considering the earliest lowest bid.

(F2) Efficiency. Sellers have to complete a particular task within a predefined time to satisfy their customers' needs. Repeat or round bid auctions are time consuming and are inappropriate in a distributed environment: distributed agents (auctioneer, bidders) have to exchange a lot of messages during auctions and the execution periods are lengthy. An example can be found in [5]. Similarly, a concurrent or distributed auctioning mechanism [4, 18] has the same time complexity and also has to aggregate information about other market demands.

(F3) Fairness. The auctioneer A posts the bids for a particular auction on a bulletin board BB. At the same time, A returns a receipt (the signed transcript) to the bidder. The transcript contains a verifiable encryption of the identity (id_B) of the bidder with the public key (Pk^e_D) of the deanonymizer D. Everyone can verify the transcripts on BB without learning anything meaningful about the identities of the bidders. In case of abuse, the identity of the culprit can be recovered. Also, the winner of an auction will be held accountable for his bids.

(F4) Openness. Every prospective bidder B can register in the system. A bidder can take part in an auction as long as his $Cred_B$ is valid and fulfills the auction prerequisites. The seller may allow bidders that fulfill only a less stringent version of the prerequisites in exchange for a compensation.

(F5) Generic. The guarantees embedded in $Cred_B$ help auctioneers to choose competent bidders based on their business and trust parameters. However, these guarantees are not a part of the auction mechanism itself. It is easy to adopt or extend the set of trust values.

(PST1) Bidder's Anonymity. $Cred_B$ contains the identity of the bidder but it is not revealed during the $\mathbf{showCred}()$ protocol. The id_B sent to the auctioneer is verifiably encrypted ($\mathsf{VEnc}_D(id_B)$) with the public key of a trusted deanonymizer (D). The identity of the winner will only be disclosed to the seller. Note also that business relations between bidders and sellers are not revealed to the registrar: the seller anonymously reports about a finished transport. Only the trusted deanonymizer D will temporarily learn this relationship. However, D is not required to keep logs or store evidence information.

(PST2) Guarantee for Seller and Auctioneer. It has been discussed earlier that the guarantees are derived from business parameters of the bidders (see section 5). Moreover, the guarantees are embedded in $Cred_B$. These guarantees create an essence of trustworthiness of the bidders among sellers and auctioneers. The trustworthiness implicitly describes whether the particular bidder is competent enough to carry out a specific transport. The seller defines the auction prerequisites at the start of an auction and bidders must prove such requirements when they make a bid. However, the seller and, hence, the auction protocol may allow newcomers in exchange for a compensation (see section 6). Furthermore, the protocol also rewards bidders who are willing to prove more attributes about themselves or promise to provide extra services.

(PST3) Accountability R's signature on $Cred_B$ makes R accountable for the trustworthiness of the embedded *trust values* in $Cred_B$. A bidder B is accountable for its bids and promises, since these are signed with $Cred_B$. The auctioneer returns a signed receipt to the bidder. All auction descriptions and transcripts on the bulletin board are signed by the appropriate parties. Finally, the outcome of a certain completed transport is signed by the seller to ensure authenticity and trustworthiness of the transport's feedback.

(PST4) Selective Disclosure It is not compulsory to show all attributes of the bidder's $Cred_B$ to participate in an auction. It is sufficient to prove that the attribute values fulfill the auction's prerequisites.

9 Related Work

Many practical electronic auction systems rely on one mediator to maintain the secrecy of bids and to hide the link between bidders and bids. However, bids clearly reveal strategic information about the bidder to the mediator (such as the bidder's economic position, its productivity, ...). Hence, a huge amount of trust in the mediator is typically required. In our solution, bids are anonymous and multiple bids cannot be linked to the same bidder by the auctioneer. Moreover, our system consists of a clear separation of duties and responsibilities. Trust is split among multiple entities, namely the registrar, the auctioneer and the deanonymizer.

Secure multi-party computation is another approach to distribute trust among multiple entities. A lot of research has been performed to solve efficiency problems for special types of applications such as e-voting and e-auctions. Multiple entities are required to reveal the results of the bidding process. Hence, trust is also split among multiple entities. Although a lot of research is invested in secure multi-party computation for auctions, only few practical implementations exist. One prototypical implementation is presented in [24]. The system is used to clear market prices for farmers that produce sugar beets in Denmark. Three servers are involved in the bidding and clearing process. Each server is administered by a different organization. However, that system presents multiple disadvantages compared to our approach. First, although trust is distributed between multiple entities, there is no clear separation of duties and responsibilities. Second, although the secrecy of bids is guaranteed, bidders are not anonymous. Hence, the auctioneer knows in which items bidders are interested (even if the bidder did not win the auction). The system presented in [24] also does not explicitly implement any security measures against cheating bidders.

eBay[8] is a prominent example of a centralized auction system. Bidders are pseudonymous to other bidders during an auction, but the winner of a specific auction can be discovered afterwards by analyzing the seller's profile. eBay allows sellers to restrict the set of prospective buyers by blocking specific buyers based on personal past experiences, by defining prerequisites (e.g. no buyers from certain countries, only buyers with PayPal,.....) and by canceling the winning bid if the seller cannot verify the true identity of the winner. Also, eBay has a reputation system that is based on feedback given by sellers and buyers. However, it is very difficult for a seller to judge a specific buyer with whom s/he has not dealt before as buyers always get positive feedback. In our paper, we describe a distributed system, in which prospective bidders are completely anonymous towards the auctioneer and the seller (during the auction). Moreover, the winner will remain anonymous towards the auctioneer and other bidders even after the auction has been completed.

Xiong and Liu [2] define a transaction based trust equation as a function of various parameters namely the feedback from peers, the total number of transactions, the credibility of the feedback, and the adaptive transaction context factor. Their trust system does not involve any TTP and lack the essence of accountability. In addition, the trust parameter mainly depend on the feedback instead of the business attributes.

Allen and Merril [6] conduct research by studying and analyzing different trust related aspects on on-line consumers' prospectives. The work includes research methodologies and contributions of such trust aspects. Moreover, they define an abstract trust framework on e-merchant trust beliefs but they do not precisely point out the building blocks of such a concept. It is more like a case study of trust construction where points like trust featured on business attributes and accountability of the attributes are ignored.

Rahman and Hailes [3] illustrate a high level approach of trust in a virtual community. They do not develop a protocol regarding their work and most of the research is based on theories and abstract metrics to calculate transitional trust. Moreover, they ignore how the individual's attributes can deploy trust in the environment.

Research on the usage of context and content based trust mechanisms within semantic web applications has been conducted by Bizer et al. [7]. In their paper they outline a trust architecture which allows the formulation of subjective and task-specific trust policies as a combination of reputation, context and content based trust mechanisms.

[8] eBay Policies: http://pages.ebay.com/help/policies/overview.html

However, their architecture does not calibrate transaction based trust associations in a SCM platform and it is not an attribute-based trust architecture.

Furthermore, none of these papers including [2, 4, 18] do address privacy, security, accountability, or anonymity issues.

10 Conclusion and Future Work

This paper presents an anonymous auction protocol, that nevertheless provides guarantees to sellers. These guarantees prove the competence of the bidder in performing a certain transport. The seller may award bonuses to bidders when they agree to provide extra services or prove additional guarantees. Similarly, newcomers may be allowed to take part in an auction if they compensate for their inexperience. The credentials (with embedded trust values) are regularly updated. Privacy policies and preferences should be used during peers' interactions. A *Privacy Policy* states what sort of information a party needs, what it will do with the information, how long it will keep the information, with whom it will share the information and so on. Similarly, a *Privacy Preference* states: what information can be forwarded, how long it can be kept, with whom the information can be shared and so on. For instance, in a bidder $\rightleftharpoons$ seller interaction scenario: the seller should send its privacy policy and bidders can check whether these policies match their privacy preferences. The protocol does not include such privacy features and elaborate research is required to determine what policies are required in this context. There is no doubt that the implementation of these features will increase the privacy level of all business parties.

Acknowledgements

This research is partially funded by the Interuniversity Attraction Poles Programme Belgian State, Belgian Science Policy, the Research Fund K.U.Leuven and the IWT-SBO Project (DiCoMAS) "Distributed Collaboration using Multi-Agent System Architectures".

References

1. Mohamed Layouni and Hans Vangheluwe, "Anonymous k -Show Credentials", In Proc. Public Key Infrastructure, Fourth European PKI Workshop: Theory and Practice, EuroPKI 2007, LNCS 4582, Springer 2007, pp. 181-192.
2. Li Xiong and Ling Liu, "A Reputation-Based Trust Model for Peer-to-Peer eCommerce Communities", In IEEE International Conference on E-Commerce Technology (CEC'03), 2003, pp. 275.
3. Alfarez Abdul Rahman and Stephen Hailes, "A Distributed Trust Model", In Proceedings of the 1997 Workshop on Security Paradigms, ACM Press, 1998, pp. 40-68.
4. H. Kikuchi, M. Harkavy, and J. D. Tygar, "Multi-round Anonymous Auction Protocol", Institute of Electronics, Information, and Communication Engineers Transactions on Information and Systems, 1999, pp. 769-777.

5. Frank Stajano and Ross Anderson, "The cocaine auction protocol: On the power of anonymous broadcast", Information Hiding Workshop, LNCS 1768, Springer, 1999, pp. 434-447.
6. Allen C. Johnston and Merrill Warkentin, "The Online Consumer Trust Construct: A Web Merchant Practitioner Perspective", 7th Annual Conference of the Southern Association for Information Systems, 2004.
7. Christian Bizer and Freie Universität, "Using Context- and Content-Based Trust Policies on the Semantic Web", ACM Press. 2004, pp. 228-229.
8. Ronald L. Rivest and Adi Shamir and Yael Tauman, "How to leak a secret", Proceedings of the 7th International Conference on the Theory and Application of Cryptology and Information Security: Advances in Cryptology, Springer, 2001, pp. 554–567.
9. Michel Abdalla and Bodo Möller, "Provably secure password-based authentication in TLS", Proceedings of the 1st ACM Symposium on InformAtion, Computer and Communications Security (ASIACCS 2006), ACM Press, 2006, pp. 35–45.
10. Jan Camenisch and Anna Lysyanskaya, "An efficient system for nontransferable anonymous credentials with optional anonymity revocation", Proceedings of the International Conference on the Theory and Application of Cryptographic Techniques, Springer, 2001, pp. 93–118.
11. David Chaum, "Security without identification: transaction systems to make big brother obsolete.", Commun. ACM, 28(10), 1985, ACM Press, 1983, pp. 1030–1044.
12. Joon S. Park and Ravi S, "Smart Certificates: Extending X.509 for Secure Attribute Services on the Web", Proceedings of 22nd National Information Systems Security Conference, 1999.
13. T. Pedersen, "Non-Interactive and Information-Theoretical Secure Verifiable Secret Sharing", Proceedings of 11th Annual International Cryptology Conference on Advances in Cryptology, Springer, 1992, pp. 129–140.
14. J. Camenisch and I. Damgard, "Verifiable encryption, group encryption, and their applications to group signature and signature sharing scheme"', LNCS Vol. 1976, ASIACRYPT '00, LNSC, 2000, pp. 331–345.
15. Simon Schütz and Lars Eggert and Stefan Schmid and Marcus Brunner, "Protocol enhancements for intermittently connected hosts", ACM Computer Communications Review, Volume 35, ACM Press, 2005, pp. 5–18.
16. Michael G. Reed and Paul F. Syverson and David M. Goldschlag, "Anonymous Connections and Onion Routing", 1998, IEEE Journal on Selected Areas in Communications, Volume 16, pp. 482–494.
17. Matt Hooks and Jadrian Miles, "Onion Routing and Online Anonymity", Final paper for CS182S, Department of Computer Science, Duke University, Durham, NC, USA, 2006.
18. Moshe Babaioff and Noam Nisan, "Concurrent Auction across Supply Chain", Journal of Artificial Intelligence Research, Volume 21, 2004, pp. 595-629.
19. Mary R. Thompson and Abdelilah Essiari, "Certificate-based Authorization Policy in a PKI Environment", ACM Transactions on Information and System Security, Volume 6, ACM Press, 2003, pp. 566–588.
20. Robert Nelson and Gruia Pitigoi Aron, "p2p Trust Infrastructure", Computer Science Division, University of California.
21. Alfred J. Menezes and Paul C. Van Oorschot and Scott A. Vanstone and R. L. Rivest, Handbook of Applied Cryptography, 1997.
22. S. Brands, "A technical overview of digital credentials", White Paper, 2002.
23. T. Pedersen and I. Damgard and B. Pfitzmann, "Statistical secrecy and multi-bit commitments", Information Theory, IEEE Transactions, Volume 44, 1996, pp. 1143–1151.
24. Peter Bogetoft, Dan Lund Christensen, Ivan Damgard, et al., "Secure Multiparty Computation Goes Live", in FC£09, Proc. Thirteenth International Conference on Financial Cryptography and Data Security, Cryptology ePrint Archive: Report 2008/068 (2009).