E-Commerce: Concepts And Protocols

Ashish Kashyap [96072]

April 24, 1999

Contents

1 Introduction **2**
- 1.1 Benefits of E-Commerce . . . 2
- 1.2 E-commerce Framework . . . 2

2 A Generic System for Process-Oriented Support of Business Transactions : No3rd **3**

3 IOTP **4**
- 3.1 Benefits of IOTP . . . 5
- 3.2 Protocol . . . 5
  - 3.2.1 Trading Roles . . . 5
  - 3.2.2 Trading Exchanges . . . 5
  - 3.2.3 Messages . . . 6
  - 3.2.4 Trading Blocks . . . 6
  - 3.2.5 Trading Components . . . 7
  - 3.2.6 Transactions . . . 8
- 3.3 Security Considerations . . . 8

4 Web-based Negotiation Support System **8**

5 Internet Auctions **9**
- 5.1 Requirements . . . 9
- 5.2 Real-time Auction System . . . 10
- 5.3 Multi-round Anonymous Auction Protocols . . . 11

6 Payment Methods **12**
- 6.1 Requirements for Payment Methods . . . 12
- 6.2 Ecash . . . 13
- 6.3 NetCheque . . . 13
- 6.4 NetCash . . . 14
- 6.5 PayMe . . . 14
- 6.6 SET(Secure Electronic Transactions) . . . 14
  - 6.6.1 Objectives . . . 14
  - 6.6.2 Features of the specification . . . 15
  - 6.6.3 Payment System Participants . . . 15
  - 6.6.4 Security Measures . . . 15
  - 6.6.5 Transactions . . . 16

7 Conclusion **16**

8 Bibliography **16**

1 Introduction

With the rapid growth of Internet, people all over the world are getting connected. E-commerce is an attempt to make use of this facility to conduct transactions electronically. E-commerce is defined as the process of sharing business information, maintaining business relationships and conducting business transactions by means of telecommunication networks.

E-commerce originates from EDI. EDI(Electronic Data Interchange) is computer-to-computer exchange of standardized electronic transaction documents. However, E-commerce is not restricted to EDI. While EDI involves only business-to-business transactions, E-commerce involves business-to-consumer transactions also. E-commerce involves support for interpersonal communications, transfer of money and sharing of common databases.

1.1 Benefits of E-Commerce

E-commerce has several benefits over the normal manual trade. As the reach of Internet is vast, the Merchant can sell goods to a larger number of people. Moreover, a merchant can reach a customer who is physically too far away. The customer, on the other hand, can buy something from a merchant who would otherwise not have been accessible to him. He has got a wider choice. Moreover, unnecessary delays that are involved in conducting a trade (like moving to the place where trade is conducted), can be cut short. This also reduces the overhead costs in certain cases. Take the case of a normal auction. You have to pay for the person conducting the auction and the place where where the auction is being held. However, if the auction is conducted on the Internet, you just have to pay for the the web application conducting the auction, which in general will be too cheap or might even come for free. The other advantage to the customer is round-the-clock availability of goods/services. The demands of customers can be met at awkward hours for there is no person needed to conduct the trade. The seller can have a web application selling his goods.

However, there are certain problems related to E-commerce that has greatly stalled the progress of E-commerce. The most obvious of these are those related to security and privacy. People won't like to give information over the internet related to finance unless they are very sure that the information cannot be accessed by someone not authorized to get the information. Money transaction has to be done securely. Moreover, some transactions demand anonymity of the customer. All these issues are very complicated and there has not yet been any universally accepted solution to it. The other reason for people being wary of E-commerce is that the legal framework for E-commerce is not properly defined.

A number of solutions are being proposed to take care of all these problems. Though none of them can be applied to every situation, E-commerce is surely catching up. Given the benefits it provides, the related problems must be solved (in a cheap and efficient manner) . There is no way out. However, till then this will remain restricted to the merchants who can afford to pay for installation of costly protocols that are made to solve their individual problem.

1.2 E-commerce Framework

E-commerce framework is an established way to analyze the issues related to E-commerce and to develop a complicated E-commerce system. This is a hierarchical structure comprised of several levels, with the lower levels providing functional support to the higher levels.

This is illustrated below.

Level	Functions	Examples
7	Products and Structures Electronic marketplaces	auctions,brokerages, dealerships, supply chains
6	Products and systems	on-line marketing, supplier-consumer linkages
5	Services Enabling Services	smart agents,e-money, traffic auditing, digital libraries
4	Secure messaging	EDI, e-mail
3	Infrastructure Object management	WWW with Java
2	Communication utilities	Internet, VANs
1	WAN	Guided and wireless media networks

The three meta-levels are:

- Technological Infrastructure: This involves the software, hardware and telecommunication facilities that provide the backbone for all sorts of electronic transactions.
- Services: This involves such services as messaging, finding information and delivering information, negotiations, transactions and settlements.
- Products and Structures: This level is responsible for the direct provision of commercial services to consumers and business partners, interorganisation information sharing and collaboration, and organization of electronic markets and supply chains.

Most of the present work being done in this field is targeted at building services on the top of the existing technological infrastructure and then later combining these services to provide electronic market structures where a person can find a large number of goods supplied by different merchants.

2 A Generic System for Process-Oriented Support of Business Transactions : No3rd

No3rd is a generic system that supports business transactions.

This satisfies the following business requirements :

- It supports the the different phases of an electronic transaction in a process-oriented way. Transaction phases can very easily be added or replaced.
- It supports a wide range of applications and can be applied to different settings like business to business, business to consumer and intra-plant cost allocation.
- It can act as an Information system.
- It is cheap and as such well-suited for small merchants.

A typical transaction process in this system consists of eleven steps. They are :

1. Customer searches electronic catalogues
2. Customer registers at supplier's side
3. Checking and confirming authentication
4. Customer selects services and sends order
5. Supplier checks for availability of services and confirms order
6. Customer confirms order
7. Supplier sends encrypted data

8. Customer confirms receipt of encrypted data
9. Supplier charges customer's account and sends key for data decryption
10. Customer decrypts data and confirms receipt
11. Supplier sends purchase information

No3rd has the following modules :

1. Electronic product catalogue to support information phase (step 1)
2. Communication system between recipient and supplier to support agreement phase (steps 2-6)
3. Payment system and cryptography module to support settlement phase (steps 7-11)

The client software along with the web-based product-catalogue forms the recipient's side. The client software provides log-in procedure, communication facility through the Internet, display of current status of accounts, facility to confirm receipts and initiate and close processes and sessions. The server side has an internal interface, business components and technical components. The interface manages the data transfer between the server and the client as well as that between the business and the technical components. The business components provide external interfaces to enterprise information systems. It constitutes a complex database system. The technical components constitute file servers (to store electronic services), random number generators (for encryption purposes), key manager (to create and store keys), off-line and online cryptography tools and client file servers (to store encrypted electronic services). The communication process between recipient and supplier is realized by exchanging messages over Internet. The message consist of a header and a body. The header gives information on the kind of task and the body gives details of the task. Each module is implemented in an object-oriented manner using Java as the programming language. So, the software is platform-independent and flexible.

The current implementation of this system assumes a closed marketplace that is independent of any third party but it can easily be extended to cover open marketplaces.

3 IOTP

E-commerce is expanding at an enormous rate these days. A number of different protocols and standards are being proposed. Generally, these protocols target a particular section of E-commerce and vary widely from other protocols built for similar purposes. Hence, there is a need to integrate the whole process of trade using a simple messaging protocol that is independent of the means of transport, the payment instruments being used, the mode of delivery, the vendor providing the services and the type of services provided. Nevertheless, the protocol should be able to integrate the security and other features that a particular vendor wants to provide for its own implementation. This need led to the proposal of IOTP(Internet Open Trading Protocol) by IETF.

IOTP provides an interoperable framework for Internet Commerce. The developers of IOTP seek to provide a virtual capability that safely replicates the real world, the paper based, traditional, understood, accepted methods of trading, buying, selling, value, exchanging that has existed for many hundreds of years.. The negotiation of who will be the parties to the trade, how it will be conducted, the presentments of an offer, the method of payment, the provision of a payment receipt, the delivery of goods and the receipt of goods. These are events that are taken for granted in the course of real world trade. IOTP has been produced to provide the same for the virtual world, and to prepare and provide for the introduction of new models of trading made possible by the expanding presence of the virtual world. IOTP seeks to produce a definition of trading events in such a way that no matter where produced, two unfamiliar parties, using electronic commerce capabilities to buy and sell, that conform to the IOTP specifications will be able to complete the business safely and successfully.

In summary, IOTP supports familiar trading models and new trading models as and when developed and global interoperability.

3.1 Benefits of IOTP

The E-commerce software vendors benefit by getting the ability to develop interoperable products by developing the products using IOTP as the basic protocol.

The payment brands get more widely distributed and will be available on a wider variety of platforms.

The merchants will be able to offer wider variety of payment brands. As such, there reach will increase.

The financial institutions get new opportunities for IOTP related merchants and new merchants.

The customers benefit by having a choice of a larger section of merchants and more consistent interface.

All theses benefits are a result of the fact that IOTP is independent of payment brands and delivery services. The additional benefits result from the fact that any vendor can add his own features (payment protocols, security,etc.).

3.2 Protocol

IOTP identifies some Trading Roles. Messages are exchanged between these Trading Roles. A Message is an XML document that consists of a number of Trading Blocks. The Trading Blocks consist of a predefined set of Trading Components. A number of Messages result in an Exchange. A Transaction is a sequential collection of Exchanges.

3.2.1 Trading Roles

Trading Roles are the parts played by an organization involved in an IOTP transaction during a particular message transfer. The same organization can take different trading roles at different times of transactions.

The various Trading Roles identified by IOTP are:

1. Consumer receives goods and services and pays for them.
2. Merchant publishises his goods and negotiates with the consumer to sell his goods.
3. Payment Handler physically receives the payment from th Consumer on behalf of the Merchant.
4. Delivery handler physically delivers the goods on behalf of the Merchant.
5. Merchant Customer Care Provider negotiates and resolves disputes between a Merchant and a Customer.
6. Payment Customer Care Provider resolves the problems with a particular payment instrument.

3.2.2 Trading Exchanges

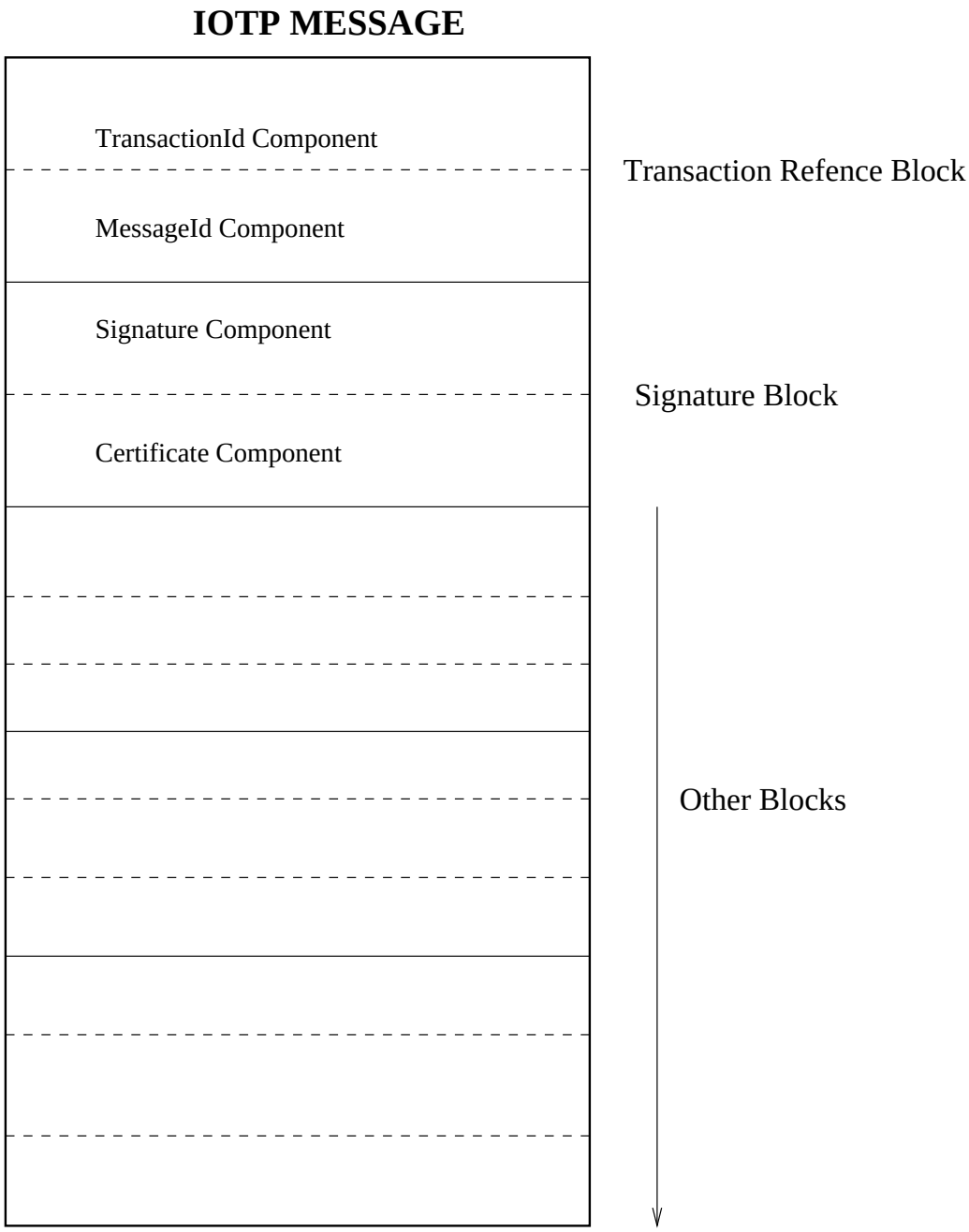
Trading Exchanges are exchange of data between trading roles resulting in a complete disjoint part of a transaction. This consists of message exchanges between two Trading roles who don't change during the process of trading exchange.

The different Trading Exchanges identified by IOTP are:

1. Offer is a Trading Exchange between the Consumer and the Merchant. This results in the Merchant providing the Consumer with the reason for trade. This is the first step in any transaction. This may be something like a seller giving information about the good that is to be bought to the buyer, or a vendor requesting a bank for refund of money.
2. Payment results in payment of some kind between Consumer and Payment Handler. The payment can either be made by the Consumer or the Payment Handler. There is a provision to allow for payment receipt to certify the completion of payment.
3. Delivery is the actual process of delivery of on-line goods or services or providing delivery information about the physical goods. This Trading Exchange takes place between a Delivery Handler and a Consumer.
4. Authentication exchange can take place between any two trading roles to authenticate the Trading Roles.

3.2.3 Messages

These are the actual documents physically sent between Trading Roles. These are made using XML constructs. Messages are composed of Trading Blocks. A typical Message is as shown below.



3.2.4 Trading Blocks

Trading Blocks consist of a predefined set of Trading Components.
Some of the Trading Blocks are:

1. Transaction Reference Block contains information which describes the transaction and the message. This uniquely identifies the message. This contains a globally unique identifier TransactionId Component that

uniquely identifies the Transaction and a MessageId Component that uniquely identifies the message within that transaction.

2. Signature Block contains one or more Signature Components and their associated Certificates. The Signature Components contain digital signatures. This is to ensure the integrity of the data transferred.

3. Trading Protocol Options Block contains options which apply to the transaction. These options relate to how the transactions are to be carried out (whether there will be any security feature, whether there will be any authentication or not) and have nothing to do with the actual trade.

4. Trading Protocol Options Selection Block is a result of selections made for the options contained in the Trading Protocol Options Block.

5. Offer Response Block contains an offer request. It contains details of goods or services or amount information or delivery instructions.

6. Authentication Request Block contains data which describes what additional authentication the consumer must provide.

7. Authentication Response Block contains response to the Authentication Request Block.

8. Payment Request Block contains information requesting to start a Payment.

9. Payment Exchange Block contains payment scheme specific data. (the details of the scheme that is to be used).

10. Payment Response Block contains information about Payment status, receipt, etc. and is a response to the Payment Request Block.

11. Delivery Request Block contains details of goods which are to be delivered.

12. Delivery Response Block is a response to that request.

13. Payment Instrument Customer Care Request Block requests Payment Instrument Customer Care Transaction to be started.

14. Payment Instrument Customer Care Response is a response to this request.

15. Inquiry Request Block enquires on the state of the Transaction.

16. Inquiry Response Block is a response to Inquiry Request Block and contains details of the state of the Transaction.

17. Ping Request Block is a request to determine whether a remote server is up or not.

18. Ping Response Block is a response to the Ping Request Block. This identifies the sender of the message and thus informs the sender of the Payment Request Block that this server is up.

3.2.5 Trading Components

This is the basic building block for all Trading Blocks. All Tiding Blocks consist of one or more of these Components. Most of these correspond to the Trading Blocks (eg. Trading Protocol Options Component for the Trading protocol Options Block.). However, most of the Blocks consist of one or more of these clubbed together with a Signature Component to identify the Block. There is also an Error Component to inform about the errors in an IOTP Message.

3.2.6 Transactions

IOTP defines a set of basic Transactions that can be carried out using IOTP. However, these transactions are just the '*Baseline*' Transactions and we can always add a new Transaction to this list by carrying out a specific sequence of messaging. The basic Transactions are :

1. Purchase involves an offer for the goods/service, a payment made by the consumer and a delivery of the goods/service. The sequence of exchanges being followed is an Offer Exchange followed by a Payment Exchange and then a Delivery Exchange.

2. Refund of payment involves an Offer Exchange made by the Trading Role demanding refund, followed by a Payment exchange. There might be an optional Authentication Exchange.

3. Value Exchange consists of exchange of value between different currency or payment methods. This involves an Offer Exchange followed by two Payment Exchanges.

4. Authentication consists of remote Authentication of Consumer. This Consists of a sequence of two Authentication Exchanges.

5. Withdrawal of electronic cash from financial institutions consists of an optional Authentication Exchange followed by an Offer Exchange and then a Payment exchange.

6. Deposit of electronic cash at a financial institute consists of an Authentication Exchange, followed by an Offer Exchange and then a Payment Exchange.

7. Payment Instrument Customer Care supports provision of Payment Brand or Payment Method Specific customer care of a Payment Instrument initiated by the Consumer Payment Instrument software. This relies on the Consumer Payment Brand software to identify the net location of the Payment Instrument Care Provider. This transaction ends when Payment Scheme Specific Customer Care Service determines that the exchange of messages within the consumer is to stop. This transaction can be started in the middle of another transaction.

8. Inquiry provides the consumer information on the status of an IOTP transaction. Inquiry Request and Inquiry Response Trading Blocks are used for this purpose.

9. Ping enables one IOTP application to determine whether another IOTP application is working or not.

3.3 Security Considerations

IOTP does not enforce any Security Method. It has support for Digital Signatures , but it does not enforce the Merchant to use them. This allows the vendor to either choose the Security Method as specified in IOTP or implement an entirely different security protocol over IOTP or ignore the security issue at all. Digital signatures are treated as IOTP components. They hash one or more Components or Blocks and identify which organization should verify the signature and which organization signed the signature. This provides support for both public-key and private-key cryptography but is not mandatory. For the purpose of secure electronic communication of messages, IOTP suggests the use of SSL as the transaction medium.

4 Web-based Negotiation Support System

This introduces a Web-based Negotiation Support System(NSS) CBSS. Most of the NSS that have been developed till date are solution-driven NSS. They suggest a list of possible solutions to the negotiating parties and the possible solutions are limited to that list. A process-support NSS, on the other hand, supports the actual process of negotiation.

A Web-based NSS INSS was developed at Carleton University, Canada. This was a solution-driven NSS that facilitated internal messaging, graphical displays and preferences specification. However, this could not handle complex negotiation processes that are generally desired. CBSS is a Web-based process-support NSS.

The main objectives of CBSS are :

1. Easy access through the Web
2. Real-time interaction
3. Structured and well-organized process
4. Automatic documentation
5. Security and Privacy

CBSS is written in Java in a Client/Server environment and installed on a Web server.Negotiating parties need to log on to the web page as clients. A dialogue window is automatically created to facilitate co-ordination and allow the negotiating parties to send and receive messages. It also has a monitoring window to notify other side of activities as opening an issue window, preparing a message, etc. This allows synchronisation of actions of two parties.

The main menu of CBSS consists of three parts: Pre-session, Session and Help. The Pre-session part supports preparation for negotiations. The Session part consists of the dialogue related to the negotiation. The Help provides on-line help.

The Session part consists of a General Discussion that includes agenda setting, time allocation to each issue and trade-offs and limits to each issue. The second part of Session is Issue Discussion where negotiating parties negotiate particular issues. The final bargaining and the ritual affirmation forms the Agreement part of Session.

All messages can be composed in a Comment Editor before it is displayed to the other party. All messages exchanged during the negotiation process are saved and can be viewed later on.

Performance evaluation of CBSS has shown that it may be a valid alternative to face-to-face negotiation, although the bargaining process is slower than face-to-face negotiation. CBSS can be further improved by adding voice communication to it. However, this is a good start in the field of on-line negotiation.

Infact, this leads to the development of Internet Auctions - a real-time negotiation process

5 Internet Auctions

The growth of the Internet has, among other things, led to the desire to bring auctioning to the rooms of the people. A number of attempts are being made to simulate different sorts of real-time auctions. Making auctions online does have a number of obvious advantages including reach to a larger group of people at lower cost and in less time. However, in comes the issue of fairness, security and real-time nature of the auctions.

5.1 Requirements

1. Support for different auctioning methods : A number of auctioning methods are used in the real-world auctions. The different auction methods are :
   - open-cry auctions : In this the bidders are all present at the same place and bids are made by shouting the prices. Everybody present gets to know about the bids being made at the same time. Anybody making the highest bid at the end of a bidding session is deemed to be the winner. However this is a problem in Internet auctions as Internet typically works on the best-effort delivery principle. There is no guarantee about the delay. So, the problem is that you cannot guarantee fairness of service.
   - sealed-bid auctions : In this the bids made by one person are not known to another bidder during the auction period. Implementing this leads to issues of data confidentiality.
   - dutch auctions : In this, the seller starts for bids at a high price initially and anybody accepting the bid gets the goods. The bids are gradually decreased till the seller sells all his goods.
2. Prevention of bidder collusion : A number of bidder may form a ring. Then they share information about the bids made by anyone of them. Any member of the ring does not outbid another person of the ring. After the auction is over and the a member of the ring buys the goods, he will auction the good in the ring. Later on, they share the profits. Arranging such a thing in real-life auctions is generally difficult and can be detected easily. However, once trade is taking place on the Internet and people are sharing informations at high speeds, this might become a major problem.

3. Security : Apart from the data integrity and confidentiality property that any electronic transaction requires, this additionally requires access control and anonymity. If access is free, denial of service attacks might become a large problem. Anonymity is desired to prevent the auctioneers from studying the bidding behavior of a consumer and adding artificial bids. Such things do exist in real life. Such a person acting as a bidder when he is not going to buy the good is called a "shill". However, the detection of shills is relatively easy in real-life. This is because, electronic communications are still not as secure as physical communications.

No standard has yet been proposed that takes care of all these requirements. However, some progress has been made in providing fairness to some extent in real-time open outcry auctions and in providing anonymity to some degree.

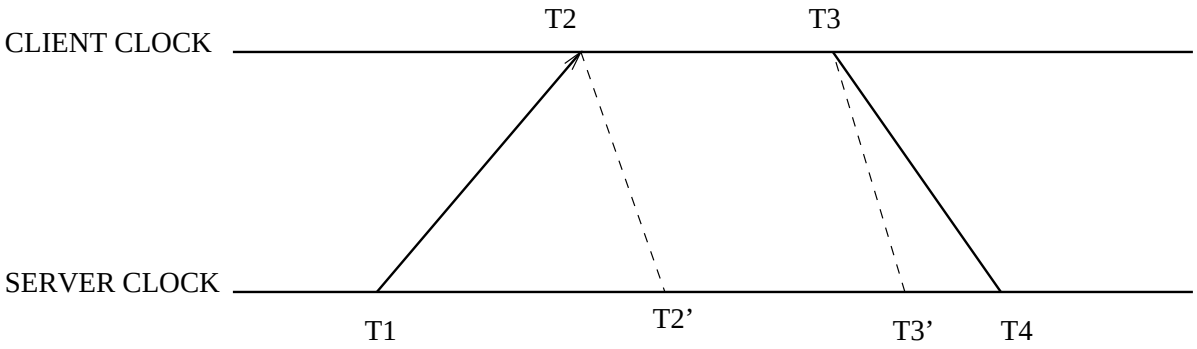
These results are discussed next.

5.2 Real-time Auction System

This is the description of an attempt made at simulating a reliable real-time open-bid auction and providing some degree of fairness to it. Making the auction real-time and open-bid means all customers should come to know of a bid made by someone else and in a minimum amount of time. Moreover, a reliable auctioning protocol should have a bounded and predictable communication delay. If the auction is fair, all customers should get to know of a bid made by someone else at exactly the same time and the bidding session should start simultaneously for all.

In the web-based prototype developed to implement this protocol, a real-time server agent is sent from the server to the client's environment. This agent resides on the local environment of the client. This agent acts as a liaison on behalf of the auction server. The server has a bidding session during which offers from different buyers are recorded and compared. When the bidding session closes, the highest bid receives the goods/service. This application uses HTTP. However, HTTP does not support a many-to-one communication. So, multiple one-to-one connections are set up. The problems related to this approach are clock synchronization, providing fair multicast and timely processing and delivery. These problems are solved through a novel real-time bidding protocol the description of which follows.

The bidding process starts with a registration process. This is used by the server to collect transmission information from the participant. ICMP is used to get the timestamps. The packet round-trip delay Dr and clock offset value Coff is calculated. For this purpose, two messages are exchanged between the server and the client. The local clock value is recorded for each sending and receiving event.



Measuring Delay and Offset

If the times recorded for sending and receiving events at the server and the client are T1 and T4 and T2 and T3 respectively, Dr and Coff are computed as follows :

$$Dr = (T4 - T1) - (T3 - T2)$$

$$Coff = \frac{T2 - T1 + T3 - T4}{2}$$

The clock synchronization can be achieved in two ways :

1. Along with the actual message sent by the server, it also sends another message containing the Coff value for the client's clock and a server timestamp (say T) that indicates when the message can be opened. The real-time agent at the client's site is supposed to keep the message sealed for T + Coff - t time, where t is the local timestamp of message arrival on the client.The value of T is kept same for all clients.

2. The server calculates the time for which the agent should wait. If T is the synchronized delivery timestamp and the current server timestamp is T* then the agent should wait for T - T* - $\frac{Dr}{2}$time after receiving the message. This value is sent to the agent along with the original message.

This protocol implements the second method. The timestamp T is determined using the worst case of one way delay $\frac{Dr(max)}{2}$among all the participants. This ensures that all the participants start at approximately the same time. As the multicasting is simulated using many one-to-one datagram transmissions, some extra overhead of sending these messages needs to be measured and this should be adjusted in each client's waiting time. Bidding process is conducted in rounds. In each round there is a timing constraint in which a client should make a bid. At the end of a bid, the server determines the highest bid received and broadcasts this to all clients. This process continues till no client sends a new bid or the highest bid remains constant for three consecutive rounds. The final result is broadcast by the server to all clients and the bidding process is terminated.

The real-time performance of this protocol is hampered if the value of Dr is large. An admission control scheme needs to be integrated to overcome this problem. Moreover, this protocol makes an assumption that the value of Dr remains constant for the entire auction period. As this may not actually hold, the value of Dr needs to be measured in the beginning of every round. Still, this may not be accurate. In this protocol, multicasting is simulated using many one-to-one protocols. This adds to the complexity as the server must calculate dynamically the waiting time for each client in every message that it sends. IP multicast will be a better option.

However, neglecting the minor problems described above, this model does provide a real-life auctioning environment in which buyers can bid in real-time and a fair policy for bidding exists that gives no undue advantage to any of the buyer.

5.3 Multi-round Anonymous Auction Protocols

In addition to the real-time concerns associated with auctions, there are also privacy concerns. A corrupt auctioneer can observe a consumer's behavior on an auction of a commodity good, and can use shills to hike the price arbitrarily. Moreover, a bidder should also not come to know about other bidders. This makes sealed bid auctions necessary. This paper describes an efficient protocol for sealed bid auctions in which the value of the specific bids are kept secret even at the completion of the auction.

The protocol assumes the following requirements for the auction:

- No auction bid should be revealed except for the winning bid.
- No winner should be able to repudiate his bid.
- The auction should be carried out in real-time.

There are n bidders, m auctioneers, and a seller. At most t = m - 1 auctioneers can conspire to try to reveal the value of a hidden bid. The seller publishes k prices, w1,...,w k, for a good. A bidder prepares a bid-vector with a bid for each of the k bidding prices. If his valuation of the good is higher than the bidding price he bids his secret ID value; otherwise, he bids 0. Bidders' secret ID values are randomly generated for each price and encrypted with the seller's public key in order to ensure anonymity. These bid-vectors are arbitrarily divided into m parts such that the sum of all these parts gives the true value. Each part is sent to an auctioneer. Each auctioneer computes the sum of all the bid-vectors received by him and sends it to the seller. The seller then computes the sum of all the results sent by all the auctioneers. If the value is 0 for a bidding price, no buyer placed a bid for that price. The seller can decrypt the sum of the secret ID values with his private key. If there is a match with a bidder's ID value, only one buyer made a bid for that price. If there is no match, there is a clash. If there is a clash for the highest price that a bidder is willing to pay, a tie-breaker is held by repeating the process for different set of price values. But, even the seller does not get to know who all are tied.

This protocol can simulate a number of different auctions:

1. Secret English Auction : Hold one auction round for each bidding price and keep increasing the bidding price whenever there is a tie.

2. Secret Dutch Auction : Start descending prices till a bidder places a bid for a price.

3. Binary tree Auction : Divide the entire bidding domain into two intervals. If the higher interval contains more than one bid, recurse on the higher interval. Else, recurse on the lower interval. The auction ends when there is exactly one bid on the higher interval.

4. Hierarchical Auction : Generalize the 'Binary Tree Auction' by dividing entire domain into k intervals.

There is a trade-off involved in this auction protocol. If we make the bids fine-grained, the length of bids sent in each round increases. On the other hand, if we make the bids coarse-grained, the number of auction rounds increases. The optimal trade-off can be achieved using the estimated value of the probability distribution of the bids, the bandwidths of the auctioneers and the bidders, the values of n and m, and the time taken to start the bidding. This paper gives a result based on these values that can be used to minimize the amount of time taken to complete the auction.

This demonstrates the use of multi-round sealed-bid auctions to ensure the privacy of a bidder. The expected number of rounds can be optimized and the optimal values to minimize communication delay can be calculated. However, this fails to address the problem of fairness and reliability. Moreover, this protocol deals only with passive attacks (a group of auctioneers collaborating on information). This protocol is ineffective against active attacks (auctioneers attempting to lie about the values that they receive).

6 Payment Methods

The most important issue related to E-commerce is money transfer. How do I pay for a good bought over the Internet securely and without divulging any additional information regarding my financial status ? Several payment methods are currently being implemented by different vendors. These electronic payment protocols can classified into five categories. They are:

1. ATM-model Transactions involve only a Financial Institution and an accountholder who deposits or withdraws money from his/her account.

2. Unmediated Two-Party Transactions involve those methods in which the buyers and the sellers are the only two parties involved in the transaction. This allows barter and service exchange.

3. Mediated Three-Party Transactions involve a mediator in the form of a Third party whom both parties can trust. This involves payments with credit or debit cards or cheques.

4. Micropayments involves payment protocols specifically built to deal with electronic payments where service or information is meterd out and charged on very small increments.

5. Anonymous digital cash involves such payment protocols that allow for the privacy of the cash user by allowing him to be anonymous. An enormous amount of work is being done in this field as it has the widest applicability. Some of the payment methods in this field are E-cash, NetCheque and Payme.

6.1 Requirements for Payment Methods

- ***Security*** : Since payments are generally made over open networks, the infrastructure supporting E-commerce should be resistant to eavesdropping and modification of messages. So, the infrastructureshould allow for authentication, provide confidentiality and preserve integrity of payment data.

- ***Reliability*** : The infrastructure should be able to withstand denial of service attacks and network failures.

- ***Scalability*** : The payment method should be able to handle the increase in the number of users and merchants, without deterioration of performance.

- ***Anonymity*** : The identity of the parties to the transaction should be protected and it should not be possible to monitor an individual's spending patterns, or find out his source of income.
- ***Flexibility*** : Other payment methods should be incorporated as some of them are widely popular for specific purposes and cannot be easily replaced for those purposes.
- ***Convertibility*** : It should be possible to convert one electronic currency to another electronic currency.
- ***Ease of Integration*** : There should not be a high initial set-up cost.
- ***Ease of Use*** : Users should not be made to feel like he is not using the currency he is used to.

6.2 Ecash

Ecash is a fully anonymous electronic cash system, from a company called Digicash. Ecash is the electronic equivalent of real paper cash, and can be implemented using public-key cryptography, digital signatures and blind signatures.

The Ecash system consists of three main entities:

- Bank (mint) issues coins, validates existing coins and exchanges real money for Ecash.
- Buyers who have accounts with a bank, from which they can withdraw and deposit Ecash coins.
- Merchants who can accept Ecash coins.

Ecash is implemented using RSA public-key cryptography. Every user in the system has his own public/private key pair. This public-private key pair is used for all authentications.

- **Withdrawing Ecash coins :**

The user's cyberwallet software (responsible for carrying transactions on behalf of the customer) calculates how many digital coins of what denominations are required. The software then generates random numbers for these coins. These numbers are large enough to ensure that there is little chance of anyone else regenerating the same numbers. The serial numbers are then multiplied by a random factor. The coins are then packaged into a message, digitally signed with the user's private key, encrypted with the bank's public key and then sent to bank. (Blind Signature Technique). The bank checks for signatures and then debits the withdrawal amount from the owner's account. The bank cannot know the serial numbers of the coins and so cannot trace them later. Then the bank returns them to the user after encrypting with the user's public key.

- Spending Ecash:

The cyberwallet sends the merchant a collection of coins that it already has by encrypting them using the Merchant's public key. When the merchant receives the money, it has to check that the money has not been spent before and that it is indeed valid. The merchant hence sends the coins to the merchant by signing it using his private key and encrypting the message using bank's public key. The bank decrypts the message using his public key, checks for the merchant's signatures and then verifies that the coin has never been used before.

6.3 NetCheque

Netcheque is a distributed accounting service, developed at the Information Science Institute of the University of Southern California, supporting the credit-based model of payment. In this approach, charges are posted to the customer's account and the customer is billed for or subsequently pays the balance of the account to the payment service. NetCheque works much like the normal cheque in which a person signs a check which is authenticated by a financial institution.

The system is based on the Kerberos system. The cheque itself contains information about the amount of the cheque, the currency unit, an expiration date, the account against which the cheque was drawn, and the payee with signatures. A number of accounting servers can be provided and th same user can have accounts on more than one accounting servers. The consistency of the account information in each accounting server is maintained using a series of locks.

6.4 NetCash

NetCash is a framework for electronic cash developed at the Information Sciences Institute of the University of Southern California. Although the cash is identified, there are mechanisms to allow for exchange of coins. The system is based on distributed currency servers where electronic checks, such as NetCheque, can be exchanged for electronic cash. The use of multiple currency servers allows the system to scale well.

The NetCash consists of buyers, merchants, and currency servers. An organization managing a currency server obtains insurance for the new currency from a central certification authority. The currency server mints electronic coins. The currency server keeps track of all the serial numbers of all outstanding coins. This may be used to prevent double spending of coins. Random exchange of coins can be used to make the process of tracing of coins difficult.

6.5 PayMe

Ecash and NetCash both have their strengths and weaknesses. Ecash is a fully secure system that allows for very strong anonymity. However, a central database of all coins ever issued needs to be maintained. This poses scalability problems. NetCash provides for scalability, but compromises on anonymity.

Payme is an on-line electronic cash system designed to take the best of both Ecash and NetCash. The entities involved are banks and users. Each bank mints its own identified electronic cash with serial numbers. Coins have fields for the coin value, serial number, bank id, bank host name and port number and expiry date. Double spending of coins is prevented by the bank maintaining a database of coins in circulation. This scales better than the blind signature electronic cash approach.

The PayMe system uses its own secure communication protocol, the Payme Transfer Protocol (PMTP). PMTP is the set of secure messages designed to provide the communications. It uses both symmetric and public-key cryptography. There are six message types. For each message type, there are three different possible message identifiers, corresponding to the request, response and refusal messages. The message types are:

1. Withdraw Coins concerns the withdrawal of coins by a account holder from the bank for that account.
2. Deposit Coins attempts to deposit coins into a bank account. The bank is responsible for checking the validity of the coins sent to it. Banks have accounts with each other. This allows for deposition of cash at a bank other than the one from which it was issued.
3. Request Bank Signature requests a bank statement for an account.
4. All users who hold valid coins can exchange them for new ones. The bank does not know who is asking for the renewal of coins.
5. Ask for payment messages is used to ask a buyer for a payment amount.
6. Pay coins attempts to pay coins to the merchant. The buyer remains anonymous to the merchant.

PMTP prevents eavesdropping by the effective use of encryption. Moreover, there is a nonce which is used within each message to ensure that the message can be used for one occasion only. This prevents replay of messages.

6.6 SET(Secure Electronic Transactions)

Visa and MasterCard have jointly developed the SET protocol as a method to secure payment card transactions over open networks.

6.6.1 Objectives

- ***Security*** : It should allow for authentication of cardholders, merchants, and acquirers. It should provide confidentiality of payment data. It should preserve the integrity of the payment data.
- ***Interoperability*** : It should allow for any combination of hardware and software platforms.
- ***Market Acceptance*** : The implementation should allow for "bolt-on" implementation of the payment protocol to existing client applications.

6.6.2 Features of the specification

- SET's use of message encryption ensures confidentiality of information.
- SET provides for digital signatures, which ensures the integrity of the payment information.
- SET uses digital signatures and cardholder certificates to ensure the authentication of the cardholder account.
- SET provides for the use of digital signatures and merchant certificates to ensure authentication of the merchant.

6.6.3 Payment System Participants

- **Cardholder** - A cardholder uses a payment card that has been issued by an Issuer. SET ensures that in the cardholder's interaction with the merchant, the payment card account information remains confidential.
- **Issuer** - An issuer is a Financial Institution that establishes an account for a cardholder and issues the payment card.
- **Merchant** - With SET, the merchant can offer its cardholders secure electronic interactions. A merchant that accepts payment cards must have a relationship with an Acquirer.
- **Acquirer** - An acquirer is the Financial Instituion that establishes an account with a merchant and process payment card authorizations and payments.
- **Payment Gateway** - A Payment Gateway is a device operated by an Acquirer or a designated Third Party that processes merchant messages, including payment instructions from cardholder.
- **Brand** - Financial Institutions have founded payment card brands that protects and advertise the brand, establish and enforce rules for use and acceptance of their payment cards, and provide network to interconnect the Financial Institution. Other Brands are owned by financial service companies that advertise the brand, and establish and enforce rules for use and acceptance of their payment cards. These brands combine the role of the Issuer and Acquirer in interactions with cardholders and merchants.
- **Third Parties** - Issuers and Acquirers sometimes choose to assign the processing of payment card transactions to third-party processors.

6.6.4 Security Measures

Integrity of data is ensured by the use of Digital Signatures. A combination of public key and private key cryptography is used for this purpose. However to ensure the correctness of the key transmitted, a touted third party is needed. This Certificate Authority issues certificates to everyone. These certificates are needed to authenticate a user. The certificates are:

- Cardholder certificates function as an electronic representation of the payment card. Because they are digitally signed by a Financial Institution, they cannot be altered by a third party and can only be generated by a Financial Institution.
- Merchant certificates ensure that the merchant has a relationship with a Financial Institution allowing it to accept the payment card. They are digitally signed by the merchant's Financial Institution. There may be multiple certificate pairs per merchant - one for each payment card brand that it accepts.
- Payment gateway certificates are obtained by Acquirers for the systems that process authorization and capture messages. These are issued to the Acquirer by the Payment Brand.
- Acquirer certificates are required to operate a Certificate Authority that can accept and process certificate requests directly from merchants over public and private networks. Acquirers receive their certificates from the payment card brand.

- Issuer certificates - An Issuer must have certificates in order to operate a CA that can accept and process certificate request directly from cardholders over n/w. Issuers receive their certificates from the payment card brand.

SET certificates are verified through a hierarchy of trust. Each certificate is linked to the signature of the entity that digitally signed it. By following the trust tree to a known trusted party, one can be assured that the certificate is valid.For Example, a cardholder certificate is linked back to the certificate of the Issuer . The Issuer's certificate is linked back to a root key through the Brand's certificate. The public signature key of the root is known to all SET s/w and may be used to verify each of the certificates in turn. The root key is at the root of this hierarchy.

6.6.5 Transactions

Transactions in a SET are carried out through exchange of messages between the Payment System Participants. Some of the typical transactions are:

- Cardholder registration - This consists of a sequence of messages exchanged between the Cardholder Computer and the Certificate Authority process. This starts with an initiate request by a Cardholder Computer, followed by an initiate response, followed by a registration form request, followed by a registration form , followed by a cardholder certificate request followed by a cardholder certificate.
- Merchant registration - This consists of a sequence of messages exchanged between the Merchant Computer and the Certificate Authorization Process. This involves an initiate request by a Merchant Computer, followed by a registration form being sent by the Certification Authority,followed by a merchant certification request which is followed by the merchant certificates.
- Purchase request - The Cardholder computer sends a initiate request to the Merchant Computer which is answered by an initiate response by the Merchant Computer. This is followed by a purchase request by the Cardholder computer which is replied by the purchase response by the Merchant Computer.
- Payment Authorization - The Merchant Computer sends an authorization request to the Payment Gateway which is answered by an authorization response.
- Payment Capture - The Merchant Computer sends a payment capture request to the Payment Gateway which is answered by a capture response.

Some other transactions supported by SET are Certificate Enquiry and Status, Purchase Enquiry, Authorization Reversal, Capture Reversal, Credit, Credit Reversal, Payment Gateway Certificate Request, Batch Administration and Error Message.

7 Conclusion

The idea of conducting on-line trade is definitely a fascinating one, but to make that a viable option, the security issues must be dealt with. To achieve that target, protocols like SET are being proposed. We might hope that in future, we will not not need to worry about security precautions while conducting electronic trade. Another need of the hour is to standardize the whole thing. The legal issues related to E-commerce also needs to be looked into. Not only that, the upcoming protocols need to worry about real-time behavior, reliability and fairness issues.

However, looking at the amount of interest E-commerce has generated and the amount of money involved, many big companies are spending a lot of money and time in research in this field. As such, we can believe that in the not too distant future, E-commerce is going to be at least as common as the normal trade.

8 Bibliography

References

[1] Electronic Commerce: Structures and Issues, Vladimir Zwass, International Journal of Electronic Commerce, Volume 1, Number 1, Fall, 1996.

[2] Internet Commerce Basics, Danielle Gray and Jim Ettwein, International Journal of Electronic Markets, Vol.7-No.4, 1997.

[3] Designing a Generic System for Process-Oriented Support of Business Transactions Using the Internet, Braun, Bremer, Schmidt and Kathr, International Journal of Electronic Markets, Vol.8-No.2, 1998.

[4] A Web-Based Negotiation Support System, Yuan, Rose, Archer, McMaster and Shuarga, International Journal of Electronic Markets, Vol.8-No.3, 1998.

[5] Internet Open Trading Protocol - IOTP, Version 1.0, IETF TRADE Working Group.

[6] NetCash: A design for practical currency on the Internet, Gennady Medvinsky and B.Clifford Newman, First ACM Conference on Computer and Communications Security, November 1993.

[7] Requirements for Network Payment: The NetCheque Perspective, B.Clifford Neuman and Gennady Medinsky, Proceedings of the IEEE Compcon '95, March 1995.

[8] Scaleable, Secure Cash Payment for WWW Resources with the Payme Protocol Set, Michael Peirce and Donal O'Mahony.

[9] http://www.DigiCash.com

[10] SET Book 1 : Business Description, May 1997

[11] Internet Auctions , Manoj Kumar and Stuart L. Feklman.

[12] Real Time Issues for Internet Auctions, Michael P. Wellman and Peter R. Wurman, IEEE Workshop on Dependable and Real-Time E-Commerce Systems, 1998.

[13] Multi-round Anonymous Auction Protocols, Kikuchi, Harkavy and J.D. Tygar, IEEE Workshop on Dependable and Real-Time E-Commerce Systems, 1998.

[14] The Design of an Internet-based Real-Time Auction System, Ching-Shan Peng, Jose Miguel Pulido, Kwei-Jay Lin and Douglas M. Blough, IEEE Workshop on Dependable and Real-Time E-Commerce Systems, 1998.