Secure E-Commerce Protocol

Khalid Haseeb khalid.haseeb@icp.edu.pk
Lecturer
Department of Computer Science
Islamia College University
Peshawar, 25000, Pakistan

Dr.Muhammad Arshad Muhammad.arshad@icp.edu.pk
Assistant Professor
Department of Computer Science
Islamia College University
Peshawar, 25000, Pakistan

Shoukat Ali shoonikhan@yahoo.com
Lecturer
F.G Degree College
Peshawar Cantt, 25000, Pakistan

Dr.Shazia Yasin shazia.khalid@icp.edu.pk
Associate Professor
Department of Physics
Islamia College University
Peshawar, 25000, Pakistan

Abstract

E-commerce has presented a new way of doing business all over the world using internet. Organizations have changed their way of doing business from a traditional approach to embrace e-commerce processes. As individuals and businesses increase information sharing, a concern regarding the exchange of money securely and conveniently over the internet increases. Therefore, security is a necessity in an e-commerce transaction. The purpose of this paper is to present a token based Secure E-commerce Protocol. The purpose of this paper is to present a paradigm that is capable of satisfying security objectives by using token based security mechanism.

Keywords: Trusted Third Party (TTP), Pretty Good Privacy (PGP), Secure Socket layer (SSL), Secure Electronic Transaction (SET).

1. INTRODUCTION

E-commerce refers to a wide range of online business activities for products and services. Security is the basic need to secure information on internet [1]. It also pertains to any form of business transaction in which the parties interact electronically rather than by physical exchanges or direct physical contact. A security objective is the contribution to security that a system or a product is intended to achieve. E-commerce has become a dynamic force, changing all kinds of business operations world-wide. E-commerce is conducted on global network i.e. Internet which is untrusted. So confidentiality is required during transmission and it must be kept secure against all type of threats The related concepts and business practices not only influence communications, the routines of daily life and personal relationships, they represent opportunities for initiating new international and domestic business ventures. However, as the Cyber is used increasingly as a platform for e-commerce transactions, security becomes a primary issue for Internet applications. Security has emerged as an increasingly important issue in the development of an e-commerce organization. The eradication of trust in e-commerce applications may cause prudent business operators and clients to forego the use of the Internet for now and revert back to traditional methods of doing business. Gaining access to sensitive information and replay are some common threats that hackers impose to E-commerce systems [2].

The successful functioning of E-commerce security depends on a complex interrelationship between several applications development platforms, database management systems, systems software and network infrastructure [3] . By doing online business, it is a facility of reaching to everyone. Exploring the opportunities challenges conventional notions of business competition through electronic flows of information and money [6]. Payment on Internet or network is a critical important chain of whole e-commerce, which contains the payment activity [4]. Security protection starts with the preservation of the confidentiality, integrity and availability of data and computer resources [5]. These three tenets of information security are sometimes represented in the Confidentiality, Integrity and Authentication Triad in the Figure 1.

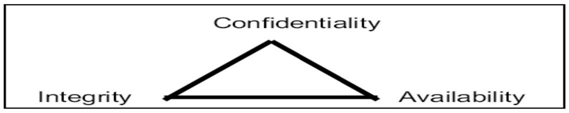


FIGURE 1: The Confidentiality, Integrity and Authentication Triad.

Including the elements of the Confidentiality, Integrity and Authentication Triad, the six security needs in E-commerce are:

i. Access Control.
ii. Privacy/Confidentiality.
iii. Authentication.
iv. Non Repudiation.
v. Integrity.
vi. Availability.

Access control ensures only those that legitimately require access to resources are given access [3].

Confidentiality is concerned with warranting that data is only revealed to parties who have a legitimate need, while privacy ensures that customers' personal data collected from their electronic transactions are protected from indecent and/or unauthorized disclosure [6]. Issues related to privacy can be considered as a subset of issues related to access control.

Authentication provides for a sender and a receiver of information to validate each other as the appropriate entity. This means having the capability to determine who sent the message and from where and which machine.

Non-repudiation is a property of the transaction that positively confirms that a particular client did indeed request the transaction in question without having the ability to deny making the request [4].

Integrity ensures that if the context of a message is altered, the receiver can detect it. It is possible that as a file, electronic mail, or data is transmitted from one location to another, its integrity may be compromised.

Availability as defined in an information security context ensures that access data or computing resources needed by the appropriate personnel are both reliable and available in a timely manner.

2. RELATED WORK

Several research papers have been presented discussing security aspects in E-commerce. E-commerce software packages should also work with Secure Electronic Transfer (SET) or Secure Socket Layer (SSL) technologies for encryption of data transmissions. (SSL) protocols, which allow for the transmission of encrypted data across the Internet by running above the traditional TCP/IP protocols. SSL protects the communication between a client and a server and provides authentication to both parties to secure communication. SSL provides point to point security. Storage of sensitive data in repositories or databases makes e-commerce system ideal target [7]. Hackers seem any target to data repositories due to availability of data on a single place. E-commerce has become a critical component in any business competitive strategy. Organizations are gaining opportunities and benefits such as global presence and improved competitiveness from web-based e-commerce. Algorithm provides the capability to generate and verify signatures. Signature generation makes use of a private key to generate a digital signature [8].

SSL allows many key exchange algorithms, but some algorithms such as Diffie-Hellman key exchange have no certificate concept [9].

3. PROBLEM DEFINITION

PGP has been considered to provide security to E-commerce [10]. But it is not a full proof solution because PGP is specifically used for E-mail security which can provide Authentication and Confidentiality, which are enough for E-mail security but not for E-commerce security. PGP can not deal with Reply and Man in the Middle security threats against E-commerce transaction. Figure 2 depicts only Authentication and Confidentiality to provide E-commerce security which are not enough.

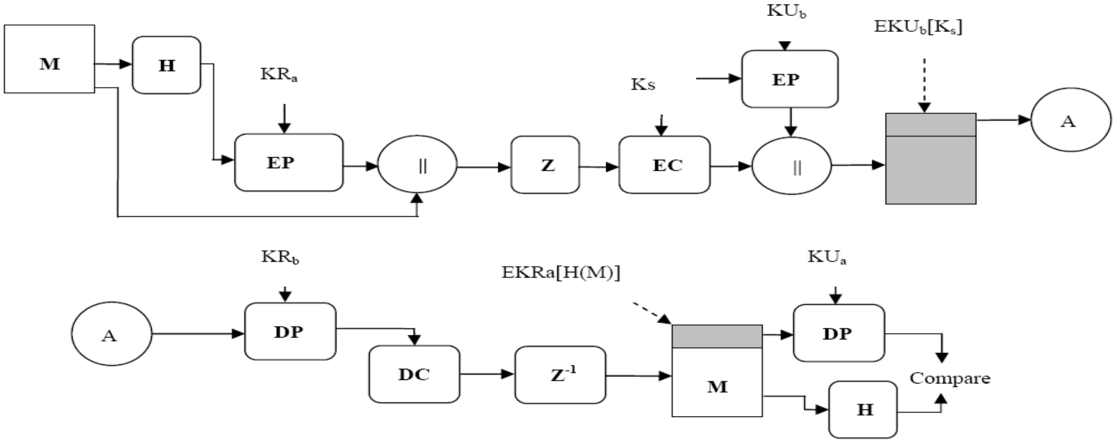


FIGURE 2: PGP Based E-commerce Cryptography [10]

Analyzing threats is difficult and time consuming but secure approach cannot be build without understanding the threats that can occur during communication and we cannot determine the appropriate technology for taking counter measures against these threats. We encounter those threats in the following categories that can break E-commerce security

i. Information disclosure threat
ii. Data Tampering threat
iii. Repudiation threat
iv. Replay threat
v. Man in the middle threat

The following table shows the security comparison of different E-commerce Security protocols.

E-commerce Protocols	Confidentiality	Non Repudiation	Integrity	Replay Attack	Man in the middle Attack
SSL	Yes	No	Yes	No	No
PGP	Yes	No	Yes	No	No
SET	Yes	No	Yes	No	No

TABLE 1: Security comparison of E-commerce protocols

To provide strong security framework, security requirements must kept in mind. Authentication, confidentiality and integrity are the main security objectives. For web and Internet related applications non repudiation, Reply and man in the middle threats are other major security objectives.

4. PROPOSED SOLUTION

Before commencing an E-commerce transaction, both parties must be registered by a TTP. TTP will provide transaction tokens to both the parties involved for sending data. TTP can be beneficial in solving many disputes that can occur during transaction between two parties. When both parties will get transaction tokens then both parties can communicate with each other and SEP provides protection against security threats.

The steps performed by SEP (shown in Figure 3) are:

i. At first customer would have to request TTP for the issuance of token.

$E_{KU\ (TTP)}$ [ID_A, Req_A, Time, K_{UA}, N_A]

ii. TTP will decrypt the customer request using its private key and respond to customer with a token. The token will be encrypted using the TTP private key.

T_A=$E_{KR\ (TTP)}$ [ID_A, Req_A , Time, K_{UA}, N_A]

iii. Customer will send token to merchant

T_A→M

iv. When merchant received customer token then merchant would have to request for an issuance of token to TTP.

$E_{KU\ (TTP)}$ [ID_B, Time, K_{UB}, N_B]

v. TTP provides a token to merchant and encrypted using private

T_B=$E_{KR\ (TTP)}$ [ID_B, Time, K_{UB}, N_B]

vi. Merchant will send token to customer

$T_B \rightarrow C$

Now both parties have an authentic token and can communicate to each other in secure manner.

vii. Customer encrypts its ID, time and nonce N_A (generated in token) using its private key. Again encrypts it along with the new nonce N_1 (generated by customer side) using public key of the merchant and sends it to the merchant.

$E_{ku\,(B)}\,[N_1, E_{KR\,(A)}\,[ID_A, \text{Time}, N_A]]$

viii. Merchant encrypts its ID, time and nonce N_B (generated in token) using its private key. Again encrypts it along with the new nonce N_2 (generated by Merchant side) using the public key of the customer

$E_{ku\,(A)}\,[N_2, E_{KR\,(B)}\,[ID_B, \text{Time}, N_B]]$

ix. Customer respond with the nonce N_2 (generated by merchant) send in step 8 encrypted using the public key of merchant

$E_{ku\,(B)}\,[E_{KR\,(A)}\,[N_2]]$

Using these steps customer and merchant shares a lot of information to each other for the purpose to recognize each other and to solve future disputes in E-commerce transaction. SEP completes E-commerce transaction in secure manner.

5. PROTECTION AGAINST SECURITY ATTACKS

This section provides Protection against attacks. Secure E-commerce Protocol (SEP) covers security aspects in E-commerce as discuss below.

Authentication

Customer sends ID, nonce and time that will sign by private key of customer and then encrypted the whole package by public key of Merchant (step 7).

Merchant decrypts the package with its private key. After Decrypt the Customer Package merchant will access Customer ID. As the package is sign by private key of customer. So in way Merchant can determine that customer is Authentic

Non-Repudiation

There are two possible way to perform Non-Repudiation in proposed solution:

a) As both the customer and Merchant get their tokens from TTP , which will contain their IDs, Nature of request , time of issuance of token, their respective public keys and a nonce (generated by the customer and Merchant respectively). The trusted third party will keep a copy of the original request for the token send by the customer and merchant (step 1 and step 4) and a copy of the transaction tokens issued to them (step 2 and step 5). Therefore Non-Repudiation problem can be solved using the TTP.

b) In step 7 and 8, both customer and Merchant send some information to each other. This information

contains a subpart encrypted by using their private keys.

$E_{KR\,(A)}\,[ID_A, \text{Time}, N_A]$

$E_{KR\,(B)}\,[ID_B, \text{Time}, N_B]$

SEP uses this information as evidence to resolving Non Repudiation Problem.

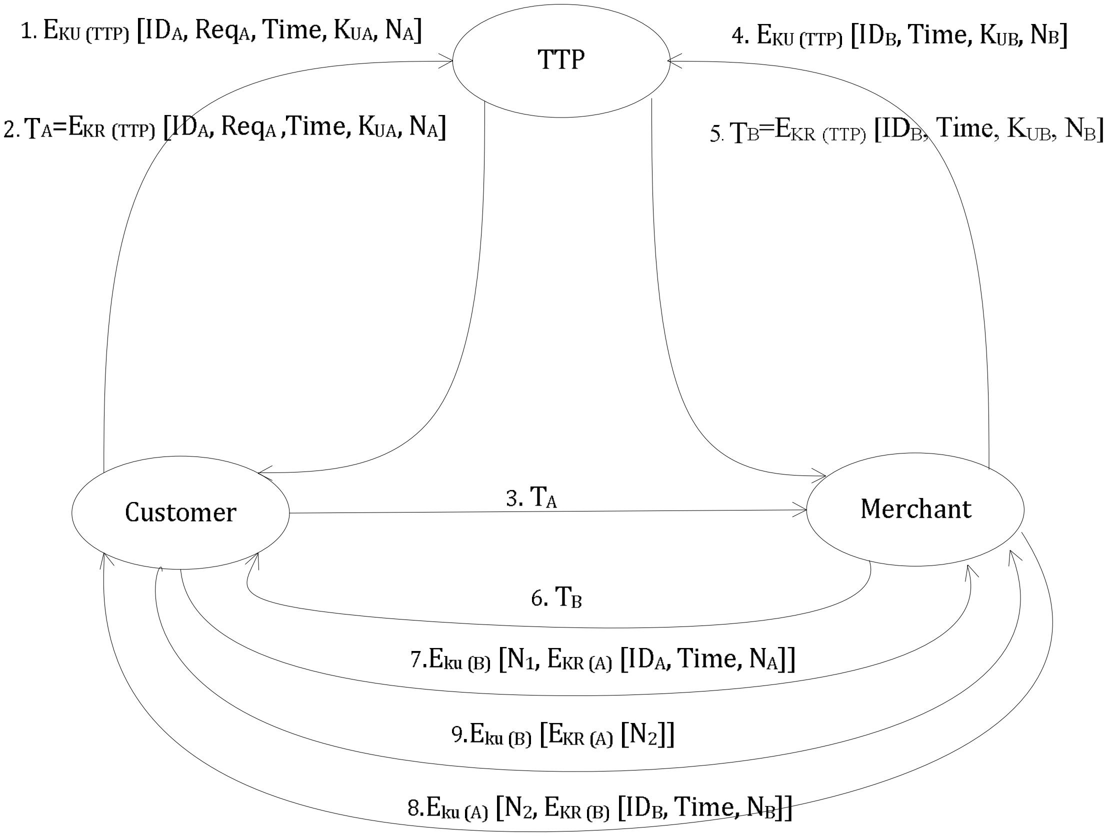

1. $E_{KU\ (TTP)}$ [ID_A, Req_A, Time, K_{UA}, N_A]
TTP
4. $E_{KU\ (TTP)}$ [ID_B, Time, K_{UB}, N_B]
2. T_A=$E_{KR\ (TTP)}$ [ID_A, Req_A ,Time, K_{UA}, N_A]
5. T_B=$E_{KR\ (TTP)}$ [ID_B, Time, K_{UB}, N_B]
Customer
3. T_A
Merchant
6. T_B
7.$E_{ku\ (B)}$ [N_1, $E_{KR\ (A)}$ [ID_A, Time, N_A]]
9.$E_{ku\ (B)}$ [$E_{KR\ (A)}$ [N_2]]
8.$E_{ku\ (A)}$ [N_2, $E_{KR\ (B)}$ [ID_B, Time, N_B]]

FIGURE 3: SEP Steps

Integrity

On the customer side the hash code is generated using SHA-1, which is then encrypted using the customer's private key. The encrypted hash code is combined with the original transaction message and sends towards merchant. The merchant side separates the hash code form the message, decrypts it using the customer's public key. At the same time, the merchant will also calculate the hash code of the received transaction message using the same SHA-1 algorithm. Transaction message will be received correctly if calculated hash code and decrypted hash code will be same.

Reply Attack

In case of key exchange a reply attack can take place, which is easily solved in the proposed solution. At first a reply attack can take place in step 1. The untrusted party can catch the token request send by the user and after some time reply it the trusted third party for getting a fake token. But as the token request contains ID, time and nonce, on this information trusted third party can easily figure out it as a replay attack and request generated by bad party will discard.

Man in the Middle Attack

The man in the middle attack works by involving three people in a communication session (server, client and third untrusted party).Third untrusted party sits between the client and the server on the network and analyzed traffic that from client to server and from server to client.

In proposed solution the trusted third party provides a token that contains ID, Public key, issuer name, Hash code, Nonce and token signed by trusted third private key. The client checks the token originality by checking the signature and name of the issuer.

6. IMPLEMENTATION

We have developed an algorithm to secure E-commerce transaction as discussed earlier. The algorithm is implemented by using the console application of .Net environment. The implementation process contains transactional entities. One is root entity second is customer entity and the third entity is merchant. Root entity act as an interface between other two entities. To achieve successful and protected communication root entity must be involved in transaction. The entities involved in transaction requests for authentic token through security mechanism SEP by using console environment to root entity .On other hand the root entity provides an authentic tokens to both transaction entities through SEP using console environment. The entities involved in transaction, requests for authentic token through security mechanism SEP by using console environment to root entity .On other hand the root entity provides an authentic tokens to both transaction entities through SEP security module using console environment.. To implement the proposed solution we used visual studio 2008 that runs on Microsoft operating system platform 64 bit computer. We used visual C# as a tool to implement proposed solution. Implementation is console based application designed to be used through text-only computer interface and used .Net framework 3.5 to provides a set of cryptographic objects, supporting hashing, encryption, and generating digital signatures. Figure 4 depicts the implementation process in detail.

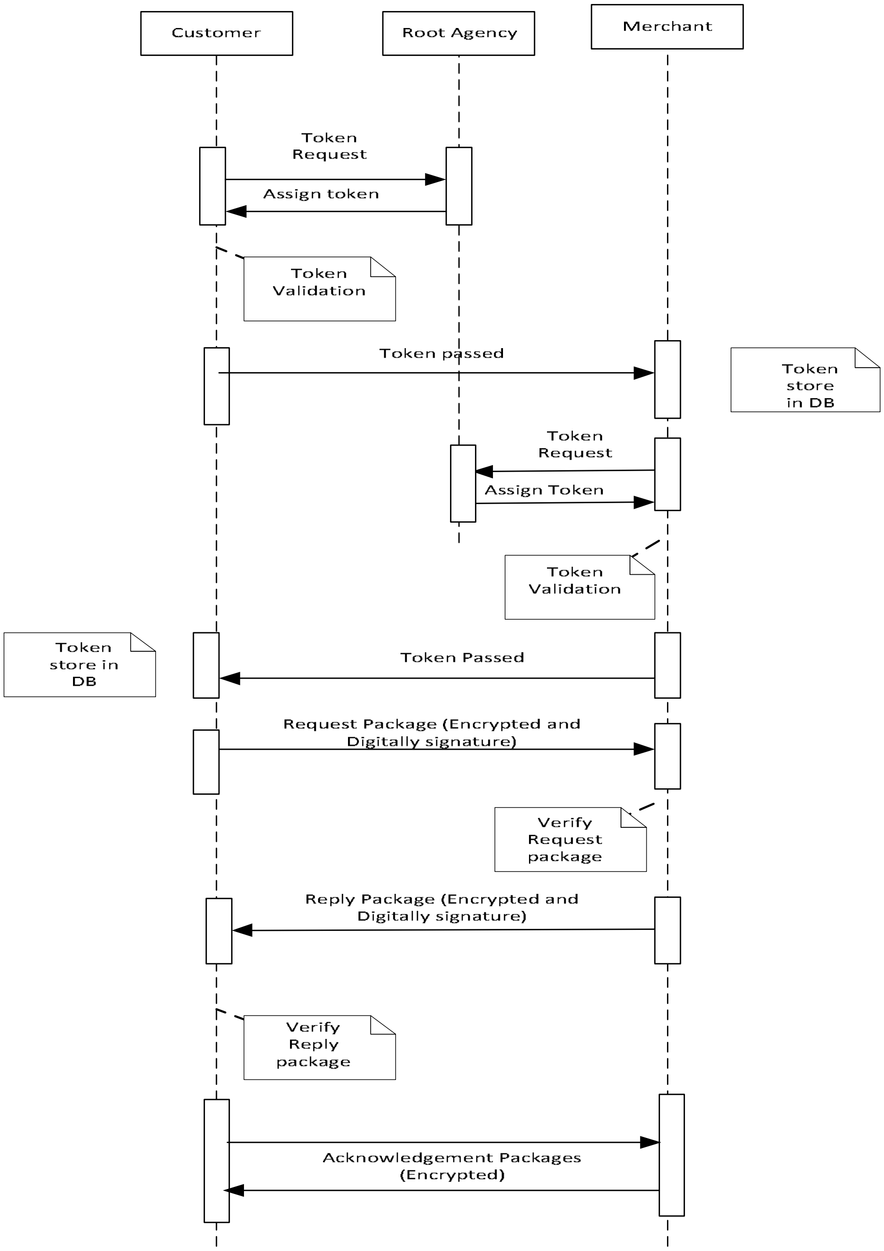
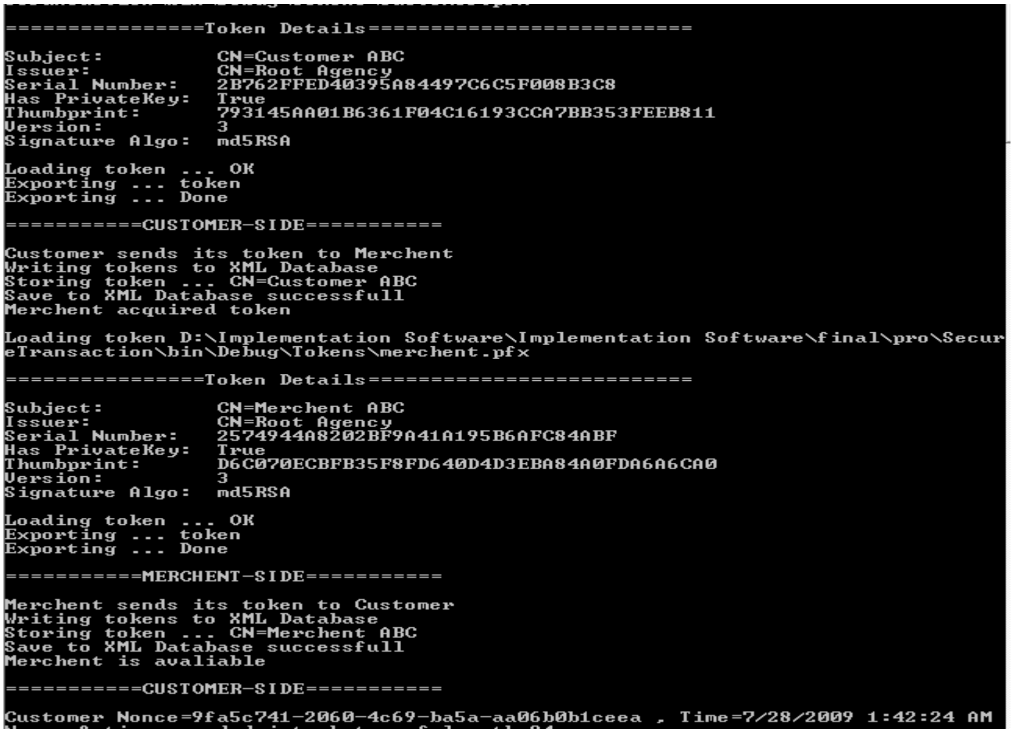


FIGURE 4: Implementation Sequence Diagram

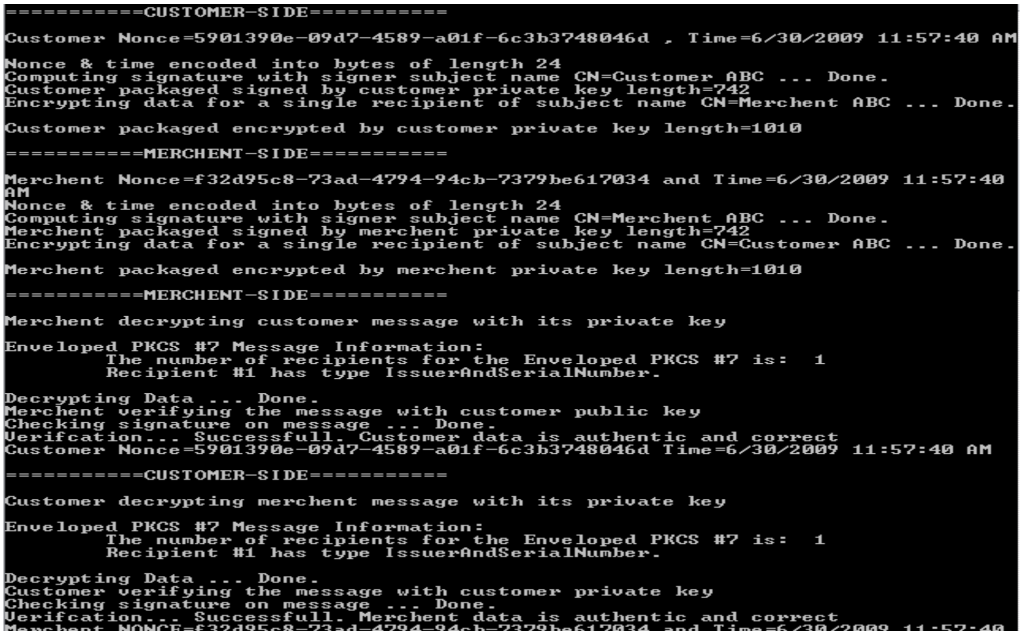
7. RESULTS

To secure transaction application generates tokens that are used by customer and merchant. Tokens have different attributes such as serial number, subject, hash code, issue name and public key. Customer and merchant first verify the authenticity of tokens and then perform communication in a secure domain shown in figure 5. Application encodes the package to transmit over the network and then decodes at receiving side to achieve original data. Application also provides authentication and integrity checks to customer and merchant packages to protect against threats shown in figure 6.



```
================Token Details========================

Subject:          CN=Customer ABC
Issuer:           CN=Root Agency
Serial Number:    2B762FFED40395A84497C6C5F008B3C8
Has PrivateKey:   True
Thumbprint:       793145AA01B6361F04C16193CCA7BB353FEEB811
Version:          3
Signature Algo:   md5RSA

Loading token ... OK
Exporting ... token
Exporting ... Done

===========CUSTOMER-SIDE===========

Customer sends its token to Merchent
Writing tokens to XML Database
Storing token ... CN=Customer ABC
Save to XML Database successfull
Merchent acquired token

Loading token D:\Implementation Software\Implementation Software\final\pro\Secur
eTransaction\bin\Debug\Tokens\merchent.pfx

================Token Details========================

Subject:          CN=Merchent ABC
Issuer:           CN=Root Agency
Serial Number:    2574944A8202BF9A41A195B6AFC84ABF
Has PrivateKey:   True
Thumbprint:       D6C070ECBFB35F8FD640D4D3EBA84A0FDA6A6CA0
Version:          3
Signature Algo:   md5RSA

Loading token ... OK
Exporting ... token
Exporting ... Done

===========MERCHENT-SIDE===========

Merchent sends its token to Customer
Writing tokens to XML Database
Storing token ... CN=Merchent ABC
Save to XML Database successfull
Merchent is avaliable

===========CUSTOMER-SIDE===========

Customer Nonce=9fa5c741-2060-4c69-ba5a-aa06b0b1ceea , Time=7/28/2009 1:42:24 AM
```

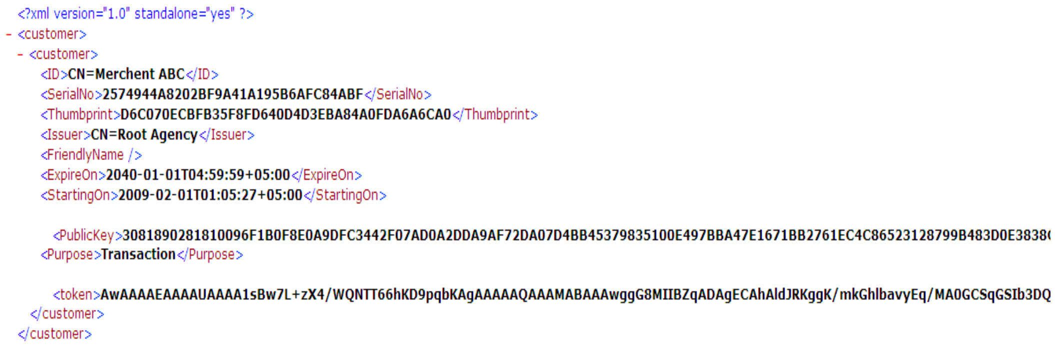
FIGURE 5: Tokens Generation and Exchanging between Transactional Entities



```
===========CUSTOMER-SIDE===========

Customer Nonce=5901390e-09d7-4589-a01f-6c3b3748046d , Time=6/30/2009 11:57:40 AM

Nonce & time encoded into bytes of length 24
Computing signature with signer subject name CN=Customer ABC ... Done.
Customer packaged signed by customer private key length=742
Encrypting data for a single recipient of subject name CN=Merchent ABC ... Done.

Customer packaged encrypted by customer private key length=1010

===========MERCHENT-SIDE===========

Merchent Nonce=f32d95c8-73ad-4794-94cb-7379be617034 and Time=6/30/2009 11:57:40
AM
Nonce & time encoded into bytes of length 24
Computing signature with signer subject name CN=Merchent ABC ... Done.
Merchent packaged signed by merchent private key length=742
Encrypting data for a single recipient of subject name CN=Customer ABC ... Done.

Merchent packaged encrypted by merchent private key length=1010

===========MERCHENT-SIDE===========

Merchent decrypting customer message with its private key

Enveloped PKCS #7 Message Information:
        The number of recipients for the Enveloped PKCS #7 is:  1
        Recipient #1 has type IssuerAndSerialNumber.

Decrypting Data ... Done.
Merchent verifying the message with customer public key
Checking signature on message ... Done.
Verifcation... Successfull. Customer data is authentic and correct
Customer Nonce=5901390e-09d7-4589-a01f-6c3b3748046d Time=6/30/2009 11:57:40 AM

===========CUSTOMER-SIDE===========

Customer decrypting merchent message with its private key

Enveloped PKCS #7 Message Information:
        The number of recipients for the Enveloped PKCS #7 is:  1
        Recipient #1 has type IssuerAndSerialNumber.

Decrypting Data ... Done.
Customer verifying the message with customer private key
Checking signature on message ... Done.
Verifcation... Successfull. Merchent data is authentic and correct
Merchent NONCE=f32d95c8-73ad-4794-94cb-7379be617034 and Time=6/30/2009 11:57:40
```

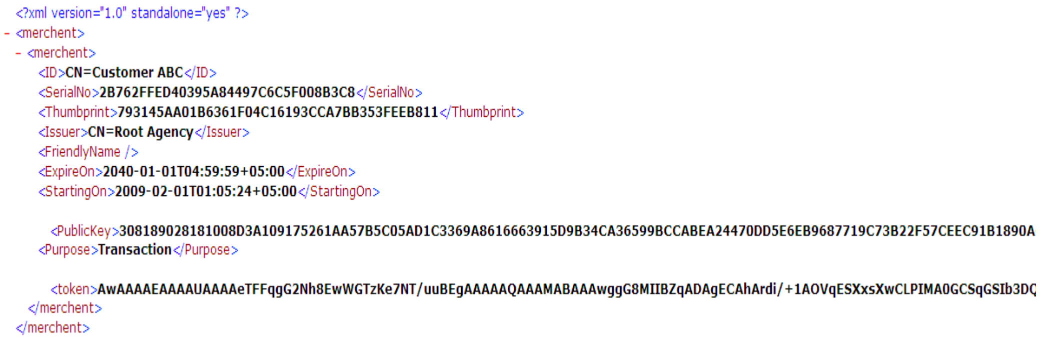
FIGURE 6: Encoding and Decoding Packages**.**

When customer and merchant exchange tokens to each other the application store both tokens in XML data files to eliminate non-repudiation problem in future shown in figure 7 and figure 8.



```
  <?xml version="1.0" standalone="yes" ?>
- <customer>
  - <customer>
      <ID>CN=Merchent ABC</ID>
      <SerialNo>2574944A8202BF9A41A195B6AFC84ABF</SerialNo>
      <Thumbprint>D6C070ECBFB35F8FD640D4D3EBA84A0FDA6A6CA0</Thumbprint>
      <Issuer>CN=Root Agency</Issuer>
      <FriendlyName />
      <ExpireOn>2040-01-01T04:59:59+05:00</ExpireOn>
      <StartingOn>2009-02-01T01:05:27+05:00</StartingOn>

        <PublicKey>3081890281810096F1B0F8E0A9DFC3442F07AD0A2DDA9AF72DA07D4BB45379835100E497BBA47E1671BB2761EC4C86523128799B483D0E3838
      <Purpose>Transaction</Purpose>

        <token>AwAAAAEAAAAUAAAA1sBw7L+zX4/WQNTT66hKD9pqbKAgAAAAAQAAAMABAAAwggG8MIIBZqADAgECAhAldJRKggK/mkGhlbavyEq/MA0GCSqGSIb3DQ
    </customer>
  </customer>
```

FIGURE 7: Customer XML file



```
  <?xml version="1.0" standalone="yes" ?>
- <merchent>
  - <merchent>
      <ID>CN=Customer ABC</ID>
      <SerialNo>2B762FFED40395A84497C6C5F008B3C8</SerialNo>
      <Thumbprint>793145AA01B6361F04C16193CCA7BB353FEEB811</Thumbprint>
      <Issuer>CN=Root Agency</Issuer>
      <FriendlyName />
      <ExpireOn>2040-01-01T04:59:59+05:00</ExpireOn>
      <StartingOn>2009-02-01T01:05:24+05:00</StartingOn>

        <PublicKey>308189028181008D3A109175261AA57B5C05AD1C3369A8616663915D9B34CA36599BCCABEA24470DD5E6EB9687719C73B22F57CEEC91B1890A
      <Purpose>Transaction</Purpose>

        <token>AwAAAAEAAAAUAAAAeTFFqgG2Nh8EwWGTzKe7NT/uuBEgAAAAAQAAAMABAAAwggG8MIIBZqADAgECAhArdi/+1AOVqESXxsXwCLPIMA0GCSqGSIb3DQ
    </merchent>
  </merchent>
```

FIGURE 8: Merchant XML file

8. CONCLUSION

There are many issues involved in securing E-commerce Transaction e.g. Privacy, Integrity Access Control, Confidentiality and Non Repudiation. These issues are still ongoing research problem. The Internet, which is the primary medium used for conducting E-commerce transactions, is not designed to handle transactions securely. In this paper an approach has been suggested, which covers Authentication, Integrity and Non Repudiation security objective in a secure manner. In this paper Secure E-commerce Protocol is proposed to provide protection against attacks. SEP presents security mechanism to increase the level of security objectives using simple cryptographic techniques.

9. REFERENCES

[1] William Stallings, “Cryptography and Network Security”, 3rd edition, Prentice Hall,2003

[2] D. Berlin, "Information Security Perspective on Intranet," presented at Internet and E-Commerce Infrastructure, 2007.

[3] S. R. S. KESH, AND S. NERUR, "A Framework for Analyzing E-Commerce Security," *Information Management and Computer Security*, vol. 10, no. 4, no. pp. 149-158.

[4] X.Sahi and P.C. Wright, “ E-Commercializing Business Operations” Communication of ACM, Feburary,2003 vol.46. no.2 page 83-87.

[5] C. BARNES, "Hack Proofing Your Wireless Networks," Syngress Publishing, Rockland, 2002.

[6] P. RATNASINGHAM, "Trust in Web-Based Electronic Commerce Security," *Information Management and Computer Security*, vol. 6, no. 4, no. pp. 162-166, 1998.

[7] Anup K. Ghosh “E-Commerce security: No Silver Bullet” IFIP Conference Proceedings; Vol. 142, P: 3 – 16, 1998

[8] P. C. O. A.J Menezes, and S.A. Vanstone, *Handbook of Applied Cryptography*: CRC Press, 1996.

[9] L. X. QIN Zhiguang, GAO Rong, "A survey of E-commerce Security," *Electronic Science and Technology of China* vol. 2, no. 3, Sept 2004.

[10] N. M. A. Al-Slamy, "E-Commerce Security," *IJCSNS International Journal of Computer Science and Network Security*, vol. 8, no. 5, May 2008.

[11] Dale Barr, “Public Key Infrastructure”, TECHNOLOGY AND PROGRAMS DIVISION Volume 11, Number 3, December 2004

[12] Cetin K. Koc, "Next Generation E-Commerce Security" Information Security Laboratory December 2, 1999