International Journal of Advance Foundation and Research in Computer (IJAFRC)
Volume 1, Issue 12, December 2014. ISSN 2348 – 4853

E-Commerce Using Public Key Infrastructure.

Gunjan Jiwnani(Post-Graduate), Sarvesh Tanwar(Assistant Professor)
Mody University of Science and Technology, lakshmangarh(MUST)

A B S T R A C T

Nowadays the E-commerce is a booming sector resulting into new business economics. It has changed the rules of the games for buyers and sellers who are seeking business online, enlarging their scope and place of business beyond global dimensions. We feel the online purchase is somewhat a concern for buyers who fear of not buying online due to security issues. We tried to present an approach using Asp.net using c# which can remove security lagging in the ecommerce business though use of PKI (Public Key infrastructure) approach. We hope to secure the ecommerce platform for better and secured buying experience for the customers which can not only provide a secured shopping platform for such type of businesses models but will also attract safer and better selling and buying options for the customers.

Keywords – Digital Certificate, E-commerce security, Certification Authority (CA), PKI;

I. INTRODUCTION

In the recent years, E-commerce has grown rapidly these days. It shows a new way of doing transactions all over the world through Internet. Organizations have changed their way of doing business from traditional commerce to E-commerce [3]. Although, both vendor and user still remain concern about security issues in online payment system. Therefore, the requirement to build a more secure system is becoming a matter of concern for both the parties [1]. As a result, PKI is an effective solution to the E-commerce security. In symmetric-key cryptography, the message confidentiality was done by message authentication code (MAC). If receiver received a message with a correct MAC, he could verify that it hadn't changed but in MAC it is difficult to convince the third party and it is open to forgery attack while in asymmetric key cryptography for message confidentiality, digital signatures are used which a message is signed with the sender's private key and verified by using sender's public key.

This verification proves that sender had access to the private key, therefore is the person who is associated with the public key, and it also ensures that the message has not been changed as change in message will result in changes to the message digest. This works fine in case of simple communication but if the message say "Pay $10,000 signed by sender" and sender denied having sent it (i.e. Non – Repudiation), then receiver will not be able to prove that sender sent it. A Digital signature does not have this failing. To make the digital signature for the message, sender encrypts the hash value of message with his private key. Sender did this because in digital signature:

1. Only sender should be able to sign a message.
2. Everyone else should be able to verify the signature.

i.e. act of signing a message should require sender to use a secret key. On the other hand, anyone should be able to verify the signature and so sender's public key work for this. But, with a digital signature, you have only done half of the work. The digital signature does not tell you "Who is the owner", it tells "the owner is whoever controls the private key associated with this public key". So, we still need a solution for authentication mechanism. (Like a proof). This is where certificates come into action.

A Certificate is a piece of data which contains an identity proof ("Sender" OR "Receiver") and a public key and is signed by a "Certification Authority": the CA, when it signs the certificate it says: "this is the public key owned by that person" i.e. A certificate binds the public key to an individual. Generally, certificates contain an expiration date, the name of the certificate authority (CA) that has issued the

certificate, and a unique serial number. Since the CA also uses a digital signature, it also falls under the scope of non-repudiation. The certificate proves that the public key is of this individual only if the CA is honest and used reliable procedures like meeting sender or receiver face-to-face with ID card verification. If certificate fails, A Certificate is a piece of data which contains an identity proof ("Sender" OR "Receiver") and a public key and is signed by a "Certification Authority": the CA, when it signs the certificate it says: "this is the public key owned by that person" i.e. A certificate binds the public key to an individual. Generally, certificates contain an expiration date, the name of the certificate authority (CA) that has issued the certificate, and a unique serial number. Since the CA also uses a digital signature, it also falls under the scope of non-repudiation. The certificate proves that the public key is of this individual only if the CA is honest and used reliable procedures like meeting sender or receiver face-to-face with ID card verification. If certificate fails, the wrong certificate can be used. So, the main scrutiny of CA is that the certificate can be verified automatically. This verification can be done by web browsers when they connect to a HTTP site they validate the server's certificates against the "Root CA". To sum up this discussion, we can say that e-commerce security resolve around the need to preserve the confidentiality, the integrity and the availability of information and systems, the authenticity of the communicating parties and the non-repudiation of transactions [2].

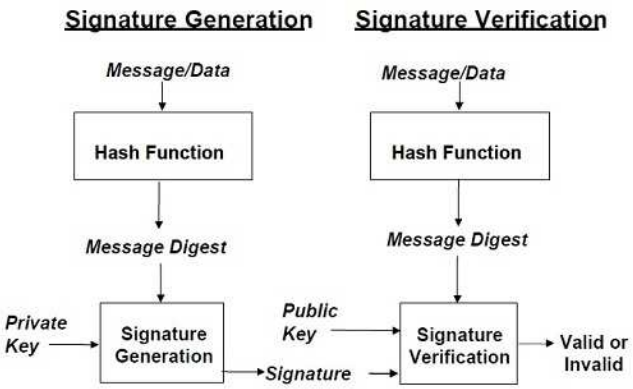

Figure 1. PKI (Public key Infrastructure) [9]

II. PUBLIC KEY INFRASTRUCTURE(PKI)

PKI is not an authentication method, rather it is an infrastructure that uses digital certificates as an authentication mechanism and is built to better manage certificates and their associated keys. A Digital certificate is a way to identify the user or computer claiming to be the owner of a specific public key. The purpose of a PKI is to allow the distribution and use of public keys and digital certificate to provide secure communication. Systems that often require PKI based security mechanisms include Email, various chip card applications, value exchange with e-commerce, home-banking and electronic portal systems [3].

Public key encryption, also called asymmetric encryption, is popular because it is more secure than secret key (symmetric encryption).Two mathematically related keys, a public key and a private key work together as one used for encrypting and other for decrypting. The public key is made known to everyone who wants to communicate with the owner of key pair. The problem with public key encryption is the difficulty of knowing whether a public key is really owned by the person it is claimed to be. Thus a method was needed for verifying the identity of the holder of key pairs. That's where digital certificates are used. A trusted third party, called a certification authority, issues a certificate to a user then other users can rely on the key holder's identity. This works like issuance of identity card by the government or organizations. Managing digital certificates and their associated keys is complex, so the PKI was created to provide a framework for the issuance, renewal, revocation and management of certificates. PKIs and their certificates are built on the X.509 specifications.

Figure 2. PKI (Public key Infrastructure) [10]

Certificate Version	
Certificate serial Number	
Signature's Algorithm ID	
Issuer Name(CA)	
Validity Period	
Subject Name(Owner)	
Subject Public key	
Issuer's unique identifier	Version2
Subject Unique Identifier	
Extensions	Version 3
Issuer's Digital Signature	

Figure 3. Digital Certificate [5]

III. IMPLEMENTATION OF PKI FOR E-COMMERCE

(SELF BUILT CA BASED ON BOUNCY CASTLE OPEN SOURCE FRAMEWORK)

1. Login

Figure 4. Login panel for E-Commerce

1. Its the online shopping website through which user can buy the products.
2. If a user does not have a certificate then it will be provided with the certificate or if it is already issued then it verifies whether it's a valid certificate or not.[

2. Generation Of Certificate

Figure 5. Self Signed Certificate Generator

1. Here, we are generating a certificate which consists of a key pair (public and private key). This certificate will be assigned to a user.
2. Public and private key are generated using RSACryptoServiceProvider () class in c#.
3. Then we are storing the certificate into key store.
4. Certificate type: Common formats for X.509 are
   PEM: Primary enhanced mail
   cer, crt, der : binary formats
   PKCS#7, PKCS#12: PKCS#12 contain X.509 certificates, public key and private key, and it is protected by passwords.
   Pfx: personal information exchange.
   In this implementation we are using PKCS#12 for certificate type.
5. Key length is of size 2048 bits.
6. In hash type we are considering SHA1with RSA,SHA256withRSA, SHA512withRSA
7. We save the output file in a temporary location on our local machine.

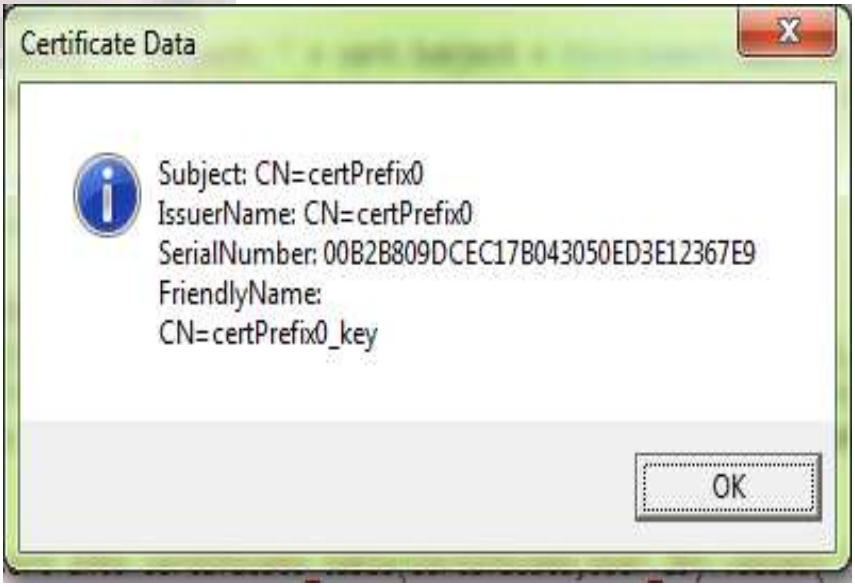

Figure 6.Certificate data

1. After selecting the products, user will be redirected to payment gateway for the payment.
2. All the certificate data and payment information will be encrypted using private key issued by the CA, and passed to the server for further processing.

3. Working

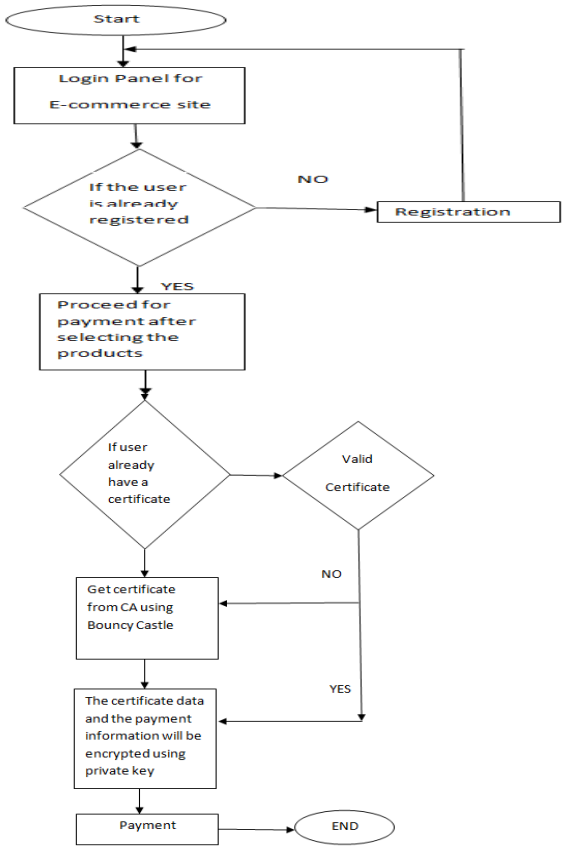

Figure 7. Flowchart of PKI Implementation for E-commerce

IV. FUTURE WORK

PKI is the future of ecommerce platform and by use of such approaches the overall ecommerce market will attract more revenue in terms of sales and profit. Looking at its importance we are committed to develop a secured PKI based approach to secure every such platform where any ecommerce application is being used making it more secured and easy to implement and use.

V. CONCLUSION

We have tried to remove security lagging in the ecommerce business though use of PKI (Public Key infrastructure) approach in which we are using the private key for encryption. We hope to secure the ecommerce platform for better and secured buying experience for the customers.

VI. REFERENCES

[1] Jing LIU, Quan Cheng, Yihui Qin, "Analysis and Solution for Virtual Personal Payment System for Online Banking", International Journal for u and e, Science and Technology, Vol 7(2014).

[2] Sokratis k. katsikas, "The Role of Public Key Infrastructure in Electronic Commerce", Department of Information and Communication Systems, University of Aegean, Greece.

[3] Liu Shan, "The PKI authentication system with the integration of Biometric Identification and Non-symmetric key technology", Proceedings of the 2009 International Symposium on Web Information Systems.

[4] Vikas rattan, Vikaram Bali, "E-Commerce Security using PKI Approach", International Journal on Computer Science and Engineering. Vol. 02 2010.

[5] B.Diffie, "New Directions in Cryptography", IEEE Transactions on Information Theory (1996).

[6] C.Mazumdar Sengupta, M.S Barik, "E-Commerce Security a life cycle Approach" (2005).

[7] http://dret.net/lectures/webfall08/security#(30)

[8] http://www.arx.com/learn/about-digital-signature/digital-signature-faq/