E-Commerce Security using PKI approach

Mr. Vikas Rattan, Er. Mirtunjay Sinha,
Hindu Institute of Management
Sonepat(Haryana)

Vikram Bali, Rajkumar Singh Rathore
Galgotias College of Engineering & Technology
Greater Noida

***Abstract*—As a most popular business model, E-Commerce provides a more convenient business mode and lower transaction cost. Currently E-commerce security is still an obstacle in development of e-commerce. It is the need of the hour to construct a safe and effective transaction environment. Based on the relationship of e-commerce security and computer network security, an e-commerce security model is presented. The paper puts forward a PKI-based E-Commerce security model utilizing PKI (Public Key Infrastructure), which is a generally adaptive secure infrastructure. Then the paper analyzes the application and security of the model, in order to make beneficial attempt in the field of E-Commerce security. Finally the further research is suggested.**

Keywords- Digital Certificate; E-Commerce Security; Certification Authority(CA); PKI;

\

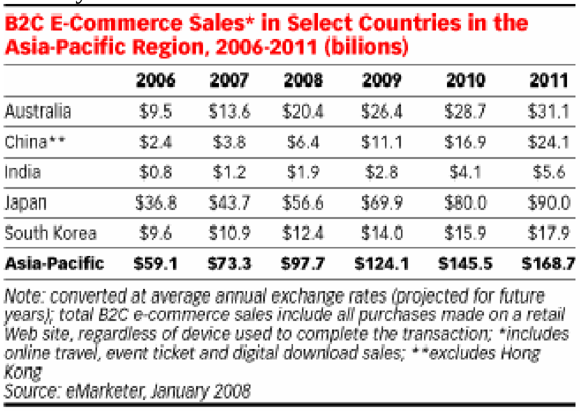
INTRODUCTION

The unpredictable growth of the Internet users in world opened a new business opportunity to the whole world. It got a special attention when IBM put forward the concept of E-Commerce in 1990s, as a new business model, E-Commerce has provided a more convenient transaction mode and lower transaction cost.

On March 31, 2007, TRAI (Telephone Regulatory of India) published data on growth of telecom sector of India. The report shows that by the end of 2007, the Internet users in India reached 40.57 million. India's Internet users increased by 36.28 million as compared to number of users in 2002 which was 3.42 millions; Internet has been penetrating into everywhere of our lives and has enormously changed all the business system.

The Internet subscriber base in India as of 31st March 2009 stood at 13.54 million as compared to 11.09 million during the previous year, registering an annual growth rate of about 22.09%.

During the year 2000-2001, two major Industry Associations produced separate reports on e-commerce in India. One was prepared by the National Committee on Ecommerce set up the Confederation of Indian Industry (CII), while the other was commissioned by the NASSCOM and prepared by the Boston Consulting Group. Both the reports are optimistic about the growth of e-commerce in India. The Confederation of Indian Industry (CII) report estimates the volume of e-commerce to grow to Rs 500 billion (US$ 10.6 billion) in the year 2003. The *NASSCOM-BCG Report*, on the other hand, estimates for the same year that the total volume of ecommerce will be Rs 1,950 billion (US$ 41.5 billion). . The low cost of the PC and the growing use of the Internet has shown the tremendous growth of Ecommerce in India, in the recent years.



B2C E-Commerce Sales* in Select Countries in the Asia-Pacific Region, 2006-2011 (bilions)

	2006	2007	2008	2009	2010	2011
Australia	$9.5	$13.6	$20.4	$26.4	$28.7	$31.1
China**	$2.4	$3.8	$6.4	$11.1	$16.9	$24.1
India	$0.8	$1.2	$1.9	$2.8	$4.1	$5.6
Japan	$36.8	$43.7	$56.6	$69.9	$80.0	$90.0
South Korea	$9.6	$10.9	$12.4	$14.0	$15.9	$17.9
Asia-Pacific	**$59.1**	**$73.3**	**$97.7**	**$124.1**	**$145.5**	**$168.7**

*Note: converted at average annual exchange rates (projected for future years); total B2C e-commerce sales include all purchases made on a retail Web site, regardless of device used to complete the transaction; *includes online travel, event ticket and digital download sales; **excludes Hong Kong*
Source: eMarketer, January 2008

According to the Indian Ecommerce Report released by Internet and Mobile Association of India (IAMAI) and IMRB International, “ The total online transactions in India was Rs. 7080 crores (approx $1.75 billion) in the year 2006- 2007 and expected to grow by 30% to touch 9210 crores (approx $2.15 billion) by the year 2007-2008. According to a McKinsey-Nasscom report the e-commerce transactions in India are expected to reach $100 billion by the 2008. Although, as compared to the western countries, India is still in is its initial stage of development. E-Marketer forecasts that online sales will more than double by reaching $168.7 billion in 2011. Market share is moving toward Australia, India and especially China. China’s share of regional B2C e-commerce will grow more than threefold from 4.1% in 2006 to 14.3% by 2011. At the low end, South Korea’s B2C e-commerce sales will grow by 13.3% over the same period. Between 2006 and 2011, the aggregate CAGR for the five countries will be 23.3%.

From the data we can see that E-Commerce has a promising development in India. Security is often sited as a major barrier to further development of e-commerce on the open Internet, such as clients' information divulging, credit card embezzling, and so on. These problems warn people in E-Commerce and make them reluctant to trade and pay on Internet. Security has become one of the bottlenecks that restrict the development of E-Commerce. Therefore, the most pivotal and important topic is how to establish a secure and well-suited applied condition to provide adequate protection to the related transaction information for each entity in an E-Commerce transaction.PKI(Public Key Infrastructure) is known as solution to these problems.

Architecture of E-commerce Transaction System

E-commerce security system can be divided into two categories E-commerce transaction security and network security. E-commerce transaction security focuses on problems occurring when the traditional business is operated on the internet. It secures all the e-transactions to be processed safely by using network security as a base.

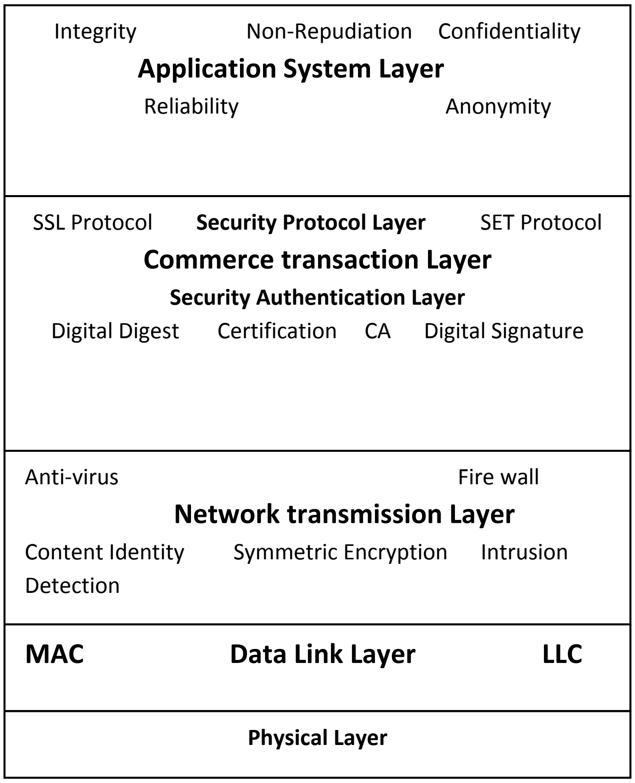


Fig 1: Architecture of EC Security Technology

The E-Commerce security architecture is made up of five parts shown in figure. 1. Each layer builds its functionality on the layer beneath it and provides technical support to its upper layer. Computer network security can be divided into Physical layer, Data Link Layer, Network Transmission Layer, Commerce Transaction Layer and Application system layer. PKI (Public Key Infrastructure) is a security application architecture (including protocol, service and standard) that has been developing on the basis of digital certificate and the public key encryption system. PKI adopts public key of certificate management to bind the user's public key and other sign information together, validate the user's identity on Internet via a third party trusty organization—Certificate Authority.

PKI consists of the following basic components as: public key encryption technology, digital certificate, authoritative authenticating organization, public key backup and retrieve system, certificate withdraw system, application interface, and so on.

DIGITAL CERTIFICATE

Digital certificates are digital documents that associate an e-commerce resource with its specific public key. A certificate is a data structure containing public key and pertinent details about the key owner. A certificate is considered to be a tamper-proof electronic ID when it signed by the Certification Authority for the e-commerce environment A digital certificate is made up of a unique distinguished name (DN) and certificate extensions that contain the information about the individual or host that is being certified. Some information in this section may contain the subject's e-mail address, organizational unit, or location.

In India certifying authority is Root Certifying Authority of India (RCAI). The CCA has established the RCAI under section 18(b) of the IT Act to digitally sign the public keys of CAs in the country. The RCAI is operated as per the standards laid down under the act The requirements fulfilled by the RCAI include the following: The license issued to the CA is digitally signed by the CCA.

All public keys corresponding to the signing private keys of a CA are digitally signed by the CCA. That these keys are signed by the CCA can be verified by a relying party through the CCA's website or CA's own website.

The RCAI is operated using SmartTrust software. Authorized CCA personnel initiate and perform Root CA functions in accordance with the Certification Practice Statement of Root Certifying Authority of India. The term Root CA is used to refer to the total CA entity, including the software and its operations.

Root Certificate:

A root certificate is a self-signed certificate. A root certificate, the top-most certificate of the tree, is based on the ITU-T X.509 standard. All certificates below the root certificate inherit the trustworthiness of the root certificate.

Obtaining a client or a server certificate from a CA involves the following steps:

1. The e-commerce user requiring certification generates a key pair (private key and certificate request containing the public key).
2. The user signs its own public key and any other information required by the CA.
3. The signed information is communicated to the CA.
4. The CA verifies that the user does own the private key of the public key presented.
5. The CA needs to verify the user's identity. This can be done using out-of-band methods, for example, through the use of e-mail, telephone, or face-to-face communication. A CA can use its own record system or another organization's record system to verify the user's identity.
6. Upon a positive identity check, the CA creates a certificate by signing the public key of the user, thereby associating a user to a public key. The certificate will be forwarded to the RA for distribution to the user.

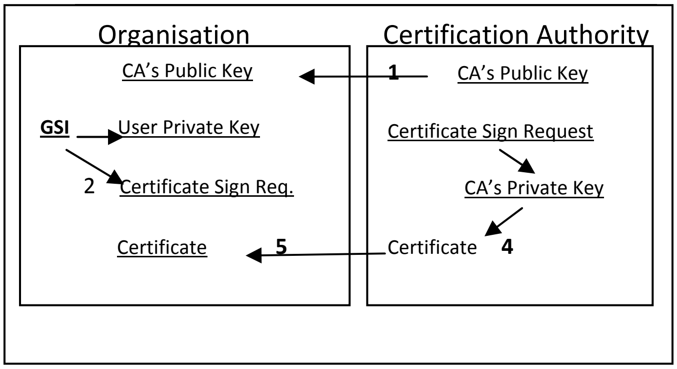


Fig 3: Certification process

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	

Fig 2 : Digital Certificate

This is the standard mechanism followed by mode of certifying authorities all over the world. In India following companies obtained the certificates from RCAI, They are Safescrypt, NIC, IDRBT, TCS, MtnlTrustline, iCertCA, GNFC, e-MudhraCA. Once they are being certified they can issue the certificates to the next level but the entire authentication and authorization responsibility lie with the certificate issuing authority. The certificates are issued for fix duration after that the organization has to renew its certificate from the certifying authority.

PKI-BASED SECURITY MODEL OF E-COMMERCE

Representation of the model

In the E-Commerce business model there are customers, merchants, PKI, banks etc. All the above sides rely on the PKI as their security mechanism and communicate through Internet. In order to establish the secure communication between the E-COMMERCE server and E-COMMERCE client, a handshake must be established. This handshake is responsible for determining the SSL settings, exchanging public keys and the basis for the mutual authentication process. The handshake process is as follows:

1. An E-COMMERCE client contacts a remote E-COMMERCE server to start a secure session by using a digital X.509 ID certificate.
2. The E-COMMERCE client automatically sends to the server the client's SSL version number, cipher settings, randomly generated data, and other information the server needs to communicate with the client using SSL.
3. The E-COMMERCE server responds, automatically sending the E-COMMERCE client the site's digital certificate, along with the server's SSL version number, cipher settings, and so on.
4. The customer's client examines the information contained in the server's certificate, and verifies that:

a. The server certificate is valid and has a valid date.
b. The CA that issued the server certificate has been signed by a trusted CA whose certificate is built into the client.
c. The issuing CA's public key, built into the client, validates the issuer's digital signature.
d. The domain name specified by the server certificate matches the server's actual domain name.
5. If the server can be successfully authenticated, the E-COMMERCE client generates a unique session key to encrypt all communications with the E-COMMERCE server using asymmetric encryption.
6. The user's client encrypts the session key itself with the server's public key so that only the site can read the session key, and sends it to the server.
7. The server decrypts the session key using its own private key.

8. The E-COMMERCE client sends a message to the server informing it that future messages from the E-COMMERCE client will be encrypted with the session key. The E-COMMERCE server then sends a message to the E-COMMERCE client informing it that future messages from the server will be encrypted with the session key.

9. An SSL-secured session is now established. SSL then uses symmetric encryption (which is much faster than asymmetric PKI encryption) to encrypt and decrypt messages within the SSL-secured *pipeline*.

10. Now that the first E-COMMERCE resources have authenticated, the second E-COMMERCE resource will now authenticate using the same process.

11. Once the session is complete, the session key is eliminated. As long as both E-COMMERCE resources have a valid digital certificate, the process of mutual authentication will succeed.

Now we discuss the practical e-commerce scenario in which following entities are involved customer, merchant and Bank. Digital certificates are issued to customer, merchant and bank by CA of PKI. Each of authority have there private keys with them and their public keys are available with everyone. All sides of the transaction must exchange the digital certificate and validate the authenticity and dependability of the certificate before the E-Commerce transaction. Thus the certificates can be utilized to identification and information encryption during the transaction.

The following is the interpretation of each part of Fig.4:

1. The buyer uses its own private key and the seller's public key to encrypt the order, and then use its own private key and the bank's public key to encrypt the payment instruction. This ensures that the seller can only obtain the order information and the bank can only obtain the payment instruction delivered by the seller. This mechanism can keep the buyer's account information secret to the seller. In addition to signing the order, the buyer should encrypt the order information

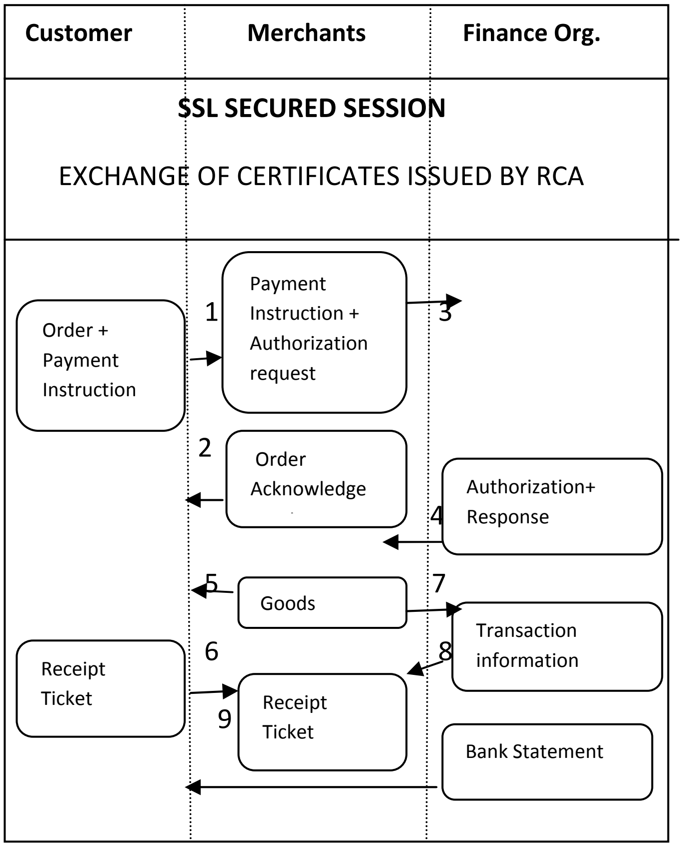


Fig 4: E-commerce transaction mechanism

2. The seller confirms the order after receiving the buyer's order and signs the confirmation information with private key of customer. Then the buyer can validate the signature by seller's public key. So the buyer can acknowledge that the seller has received his order formally.
3. The seller delivers the payment instruction to the bank after the order confirmation. The bank use the buyer's public key to identify the buyer and use its own private key to check the secrecy of the payment instruction.

4. If the buyer's account is adequate for the deal, the bank sends accredit information to the seller and obligates the required money of the deal so as to transfer to the seller after the all transaction process.

5. The seller delivers the goods to the buyer according to the order.

6. The buyer signs on the Receipt Ticket for the seller when receive and check the goods according to the order and then uses its private key to sign the information of Receipt Ticket and deliver it to the seller.

7. The seller sends the Receipt Ticket signed by the buyer and the transfer instruction to the bank, the information of which is signed with the seller's private key and is encrypted with the bank's public key
8. The bank transfers the money of the deal from the buyer's account to the seller's account and gives notice to the seller, and the notice is encrypted with the bank's private key , so the receiver can identify the reliability of the information by the bank's public key .
9. The bank sends bills periodically to the buyer. The bills are encrypted with the bank's private key , so the receiver can identify the reliability of the bills by the bank's public key , and the buyer will acquaint with the change of his account

B. Security analysis of the model

Security in e-commerce is analyzed from various aspects most important of them are authentication, integrity, timeliness and confidentiality. In this section we will try to analyze the efficiency of our model on the basis of these criteria.

1) Authentication [14]

PKI architecture provides the full proof authentication mechanism using X.509 certificate. IN PKI based e-commerce model, the authentication is done by awarding certification to each party involved in the business system.

2) Confidentiality

In the PKI architecture, all the partners who trust the Certificate Authority (CA) of PKI can obtain the digital certificates by registering with Register Certifying Authority (RCA). RCA takes care of the confidentiality of private key's issued with the digital certificate and in most of cases RCA is a government authority which is trusted by every certificate holder and provides 100% insurance about the confidentiality of information. The information encrypted by one entity's public key can be decrypted by its private key this way both the partners of the transaction can decide a series of activities such as encryption algorithms, key exchange, and so on.to provide confidentiality of information and transactions.

3) Integrity

Integrity is one of the main concern of any business activity so as of e-commerce system. Integrity is classified into following categories

I) *Integrity of Transaction*. when money is sent from consumer to supplier the integrity of transaction must be maintained i.e. Debit and credit of amount must mapped in an integrated manner. Failure to this will lead to an inconsistent state which is highly undesirable.

II) Delivery of Product. The consumer must receive the product in good condition before the payment for the product. It is impossible that the buyer pay the money without receiving the product.

4) Timeliness

Timeliness means putting the check on the reproduction of same request in future. In PKI based security system if any transaction takes more time than the predicted time the session will be automatically switched off and parties have to start a new session from the scratch. PKI based security system provides time-stamp with each request which leads towards the validation of data between concerned parties.

The PKI architecture provides undeniable service that can discriminate the dishonest behaviors in E-Commerce transaction process. If some dishonest behaviors exist in the transaction process, the related entities may be punished according to the PKI policy and legal regulations.

CONCLUSION

The rapid development of the Internet and ecommerce, made it important to provide the confidentiality, integrity and non-repudiation to provide secure transactions. Digital signature is the solution of these problems and presented in this paper. The paper is only an elementary research about the application of PKI technology in the field of E-Commerce security. Digital signature is not only applied to e-commerce system, but also widely used in contemporary technologies.

REFERENCES

[1] F.G.Hatefi, F.Golshani. New framework for secure network management. Computer Communications, 1999, 22(7): 629-637.

[2] Diffie, W, M.Hellman. New directions in cryptography. IEEE Transaction on Information Theory, 1976, 22(6):644-654.

[3] WYT Howes, S Kille. X.500 Lightweight directory access protocol. http: //www.ietf.org /rfc /rfc1487.txt, 1993-7-9.

[4] Hui Lei, Gholamali C. Shoja. A distributed trust model for e-commerce application. IEEE International Conference on e-Technology e-Commerce and e-Service, Hong Kong, 2005, 290-293.

[5] Karl Aberer, Zoran Despotovic. Managing trust in a peer-2-peer information system. In Proceedings of the tenth international Conference on Information and Knowledge Management, Atlanta, Georgia, USA , 2002, 310-317.

[6] Michael Myers. X.509 internet public key infrastructure online certificate status protocol-OCSP. http://www.ietf.org/rfc/ rfc2560.txt. 1999-7-21.

[7] D.Chaffey, E-Business and E-Commerce Management: Strategy, Implementation and Practice. Financial Times / Prentice Hall, 2001.

[8] S.M.Furnell, "Using security: easier said than done?", Computer Fraud & Security,. pp. 6-10, April 2004.

[9] Zhang Hong, Gong Jian, Huang Xianying, Infrastructure of PKI-Based EC Security, Sichuan Ordnance Journal, Oct.2003.

[10] IResearch Consulting Group, The Research Reporter of 2005 China Online Payment, Aug.2005.

[11] Geng Li-xiao,Zeng Zhen-xiang,Zhang Xue-min," Resarch on PKI based E-commerce security Mechanism. 1-4244-1312-5/07/$25.00 © 2007 IEEE, Page 3545-3548.

[12] An Analysis of E-Commerce: E-Risk, Global Trade, and Cybercrime by Dr. Katherine T. Smith ,Department of Marketing, Texas A&M University.

[13] Efendi, J., M. Kinney, and L.M. Smith. 2008. Profitability Analysis of B2B Buy-Side E- Commerce Systems. Working Paper, Texas A&M University.

[14] Sinha (April 2009), "Ecommerce in India – The Real Challenges"

[15] Miller, Roger (2002), "The Legal and E-CommerceEnvironment Today", Thomson Learning, pp. 741 pages.

[16] Rastogi, Rajiv; "Country's report on E Commerce Initiatives".

[17] http://cca.gov.in/rw/pages/rcai_about.en.do