# Authentication Approaches for E-Commerce Transactions: An Overview

Usha Nandwani
Jawahar Education Society's
A.C. Patil College Of Engineering
Navi Mumbai Kharghar

Sangita Chaudhari
Jawahar Education Society's
A.C. Patil College Of Engineering
Navi Mumbai Kharghar

## ABSTRACT
Mostly we use password for Remote Authentication but Smart Card- based scheme is very promising and practical solution to remote authentication. Over the past several years, Smart Cards have achieved a growing acceptance as a powerful tool for Security, Identification and Authorization. Smart Cards have been widely used as simple token hardware in authentication process. As the e-business is growing rapidly via the internet, many organizations are implementing all the infrastructures that allow them to have secure e-business transactions. In this paper we study what is e-business, threats for e-business, security requirements for e-business and various authentication approaches for e-commerce transactions that allow partners to realize secure transactions.

## Keywords
Card, Secure e-business transaction, PKI, Integrity, Authentication, internet, policy based, repudiation based

## 1. INTRODUCTION
E-business—E-business is a term used to describe businesses run on the Internet, or utilizing Internet technologies to improve the productivity or profitability of a business. In a more general sense, the term may be used to describe any form of electronic business that is to say, any business which utilizes a computer. E-business (electronic business), derived from such terms as "e-mail" and "e-commerce," is the conduct of business on the Internet, not only buying and selling but also servicing customers.

Today, major corporations are rethinking their businesses in terms of the Internet and its new culture and capabilities. Companies are using the Web to buy parts and supplies from other companies, to collaborate on sales promotions, and to do joint research. Over the past several years, smart cards have achieved a growing acceptance as a powerful tool for security, identification, and authorization in e-business. Smart card-The smart card is a credit card sized plastic card embedded with an integrated circuit chip. It is a miniature computer with microprocessor chip, input/output port, and operating system, ROM, EEPROM and RAM. The smart card contains built-in security features and multiple functions and applications with its own programs and data. Financial card issuers are moving to replace magnetic stripe cards with chip cards to reduce counterfeiting and fraud. The increasing computational power placed on the chip along with advances in cryptography has made the smart card a very powerful tool for identification. The advent of multi- application smart card operating systems for both contact and contact less applications has put smart cards on the edge of information technology.

## 2. SECURITY TO E-BUSINESS [8]
Gaining unauthorized access to a computer system", other definitions exist but this is one that best describes the threat as far as an organization such as an E-Business is concerned.

### 2.1 Smart Card Security
Smart cards provide computing and business systems the various benefit of portable and secure storage of data and value. At the same time, the integration of smart cards into your system introduces its own security management issues, as people access card data far and wide in a variety of applications.

### 2.2 Elements of data security
In implementing a security system, all data networks deal with the following main elements:

- HARDWARE, including servers, redundant mass storage devices, communication channels and lines, hardware tokens (smart cards) and remotely located devices (e.g., thin clients or Internet appliances) serving as interfaces between users and computers.
- SOFTWARE, including operating system, database management systems, communication and security application programs
- DATA, including database containing customer related information.
- PERSONNEL, to act as originators and /or users of the data; professional personnel, clerical staff, administrative personal, and computer staff

### 2.3 The Mechanisms of Data Security
**An effective data security system works with the following key mechanisms to answer:**

1. DATA INTEGRITY- This mechanism ensures that data was not lost or corrupted when it was sent to you.
2. AUTHENTICATION- This inspects, then confirms, the proper identity of people involved in a transaction of data or value.
3. NON-REPUDIATION-This eliminates the possibility of a transaction being repudiated or invalidated by incorporating a Digital Signature that a third party can verify as correct.
4. CONFIDENTIALITY - Ensures only senders and receivers access the data. This is typically done

by employing one or more encryption techniques to secure your data

5. AUTHORIZATION AND DELEGATION- Authorization is the processes of allowing access to specific data within a system. Delegation is the utilization of a third party to manage and certify each of the users of your system (Certificate Authority)
6. AUDITING AND LOGGING- Provides a constant monitor and troubleshooting of security system function.
7. MANAGEMENT- Allows administration of your security system.
8. CRYPTOGRAPHY / CONFIDENTIALITY- Confidentiality are the use of encryption to protect information from unauthorized disclosure. Plain text is turned into cipher text via an algorithm, and then decrypted back into plain text using the same method.

## 2.4 Following are basic steps to follow to secure all systems.

- ANALYSIS: Types of data to secure; users, points of contact, transmission. Relative risk /impact of data loss.
- DEPLOYMENT of your proposed system
- ROAD TEST: Attempt to hack your system; learn about weak spots, etc.
- SYNTHESIS: Incorporate road test data, re-deploy
- AUDITING: Periodic security monitoring, checks of system, fine-tuning

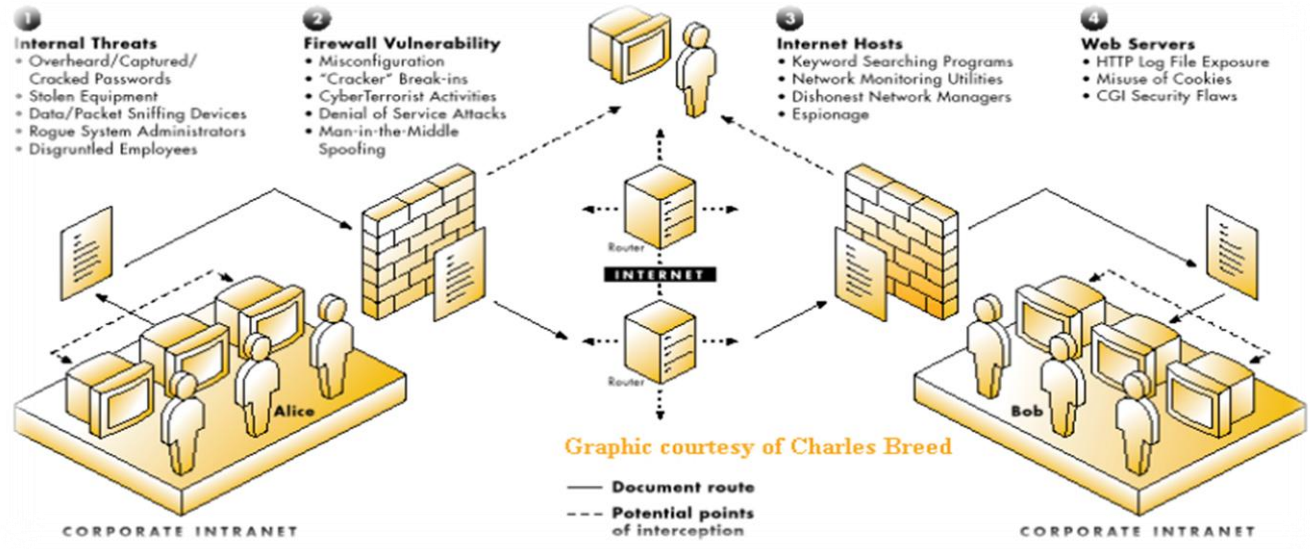


**Figure 1. Threats in e-business.[source: 8 ]**

When analyzing the threats to your data an organization should look closely at two specific areas: Internal attacks and external attacks. The first and most common compromise of data comes from disgruntled employees. Knowing this, a good system manager separates all back-up data and back-up systems into a separately partitioned and secured space. The introduction of viruses and the attempted formatting of network drives is a typical internal attack behavior. By deploying employee cards that log an employee into the system and record the time, date and machine that the employee is on, a company automatically discourages these types of attacks. External attacks are typically aimed at the weakest link in a company's security armor. The first place an external hacker looks at is where they can intercept the transmission of your data

## 2.5 Other types of problems that can be a threat to your assets include:

- Improperly secured passwords (writing them down, sharing)
- Assigned PINs and the replacement mechanisms
- Delegated Authentication Services
- Poor data segmentation
- Physical Security (the physical removal or destruction of your computing hardware)

## 2.6 Advantages of e-business

- Quicker and easier communications
- strengthened marketing capabilities and reach
- increased hours of operation (a website provides 24 hour 7 day information to existing and potential customers)
- access to broader information through research
- reducing the cost of doing business by lowering transaction costs and increasing efficient methods for payment, such as using online banking and reducing stationery and postage cost

# 3. SECURITY REQUIREMENTS FOR E-BUSINESS

E-business is very widely implemented by many companies in order to simplify purchasing processes by customers. There is almost an uncountable number of ways that an e-business

setup could be attacked by hackers, crackers and disgruntled insiders. Common threats include hacking, cracking, masquerading, eavesdropping, spoofing, sniffing, Trojan horses, viruses, bombs, wiretaps, etc.

## 3.1 The various problems are seen in e-business: [5], [6]

- Lack of understanding on how e-business operation works.
- Lack of awareness regarding the security involved in e-business.
- Lack of understanding relating the trust involved in e-business
- Lack of confidentiality relating to e-business
  Or online transactions

## 3.2 To overcome above problems following steps must be taken in consideration:

- To learn about e-business and how its business operation works
- To analyze and increase the awareness regarding security involved in e-business
- To analyze the understanding relating the trust involved in e-business.
- The increase the confidentiality of trust and security relating to e-business.
- To provide solutions in order to overcome e-business trust and security problems and also its prospects

# 4. AUTHENTICATION APPROACHES FOR E-BUSINESS

## 4.1 Public key infrastructure for securing e-business [3]

PKI, which is functioning as a chain of trust in security architecture, can enable security services of cryptography to e-payments, in order to take advantage of the wider base either of customer or of trading partners and the reduction of cost transaction achieved by the use of Internet channels.
In a PKI a trust anchor is any CA, which is trusted without the trust is being referenced through the PKI certificates [9], [10]. Simply the PKI enables the establishment of a trust hierarchy. The transaction entities are unfamiliar and they must establish a trust relationship with a CA. CA authenticates the entity and then issues for each entity a digital certificate. That digital certificate is now signed by the CA and can be considered as a personal identification. These certificates are capable of establishing trust between the unknown entities as long as they trust the CA. The motive of this trust establishment is to offer a way to transmit data securely over insecure heterogeneous networks. The public keys are placed in a storage area named *trusted party*. Both the name and public key of the entity with the digital signature of the trusted party is called a *Certificate*. The certificate is important for authentication because it is containing the name, key and signature of the entity. PKI is the tool for the establishment of a trust hierarchy. It is the underlying principal of every PKI, due to the fact that electronic commerce operates with trust mechanisms comfortable with risk management operation. The parties-entities (unknown to each other) transacting in open environment as the Internet, do not have sufficient trust established between them to perform business, contractual, legal, or other types of transactions. The implementation of a PKI using a CA provides this trust. This implementation of trust is capable of immunizing the essential part of electronic commerce, the electronic payments.

## 4.2 Agent and Non-Agent based trust management infrastructure for e-business [2]

Trust Management is an important factor that is necessary for all transactions. The basic e-business requirements like non-reputation of both trustee and of trustier are found to be problem arising due to lack of trust information. Several frameworks have been designed by researchers based on reputation models, but all these mechanisms failed in preventing users from producing false information while making a reputation. Also sufficient information regarding the new users who have just started doing business online is not available. To overcome the drawbacks The model based on Trusted third parties namely Policy based and Reputation based models is introduced .Agents based model is found to be more efficient with respect to time and trust calculation when compared to the model which works under non Agent environment.
The framework of the proposed system consists of different components like ITA (Intermediate Trust Authority), CTA (Central Trust Authority), and CA (Certificate Authority). This model has a component called Central Trust Authority (CTA) which maintains the trust information of all the entities involved in the electronic business. The different kinds of entities present in the system are: the customer with different roles as buyer and seller, the organization which does business electronically acts as an Intermediate Trust Authority (ITA), and the Certificate Authority (CA).The main functionality of ITA is to retrieve trust information from the Central Trust Authority (CTA) on behalf of individual customers. The CTA is assumed to have members from different countries to formulate the rules and policies. The Certificate Authority (CA) is an independent body that issues digital certificates and keys as an authority. The entities that want to do electronic business should get a digital certificate from CA. The details of digital certificate issued are maintained by CTA along with the rating value for trust information. The ITA can also request information from CTA to analyze the trust rating of an entity along with the information that is available in its own database.
CTA also holds the certificate information within the database.
A framework which has been developed using Agents is found to be more efficient with respect to time and trust calculation when compared to the model which works under non-agent environment. In non-agent environment process such as certificate verification using policy based, Trust value updating and calculation using repudiation have to be done as a sequence of operations whereas in agent model architecture, separate dedicated agents have been developed for doing certificate verification and trust calculation which ultimately decreases time factor. The trust model that has been designed focuses on the behavior of the trustee to provide more accurate trust value. In repudiation based trust model, not only individual trust will be taken apart from the trust weight from peers but also give a more accurate trust value.

## 4.3 Smart card based infrastructure for e-business [1]

However, implementing a PKI is not enough. Keys, certificates and digital signatures must be protected the same way you protect a passport or your credit cards. Storing digital certificates on the LAN or on your computer makes it fairly easy for others to copy the certificate and then use it to

impersonate you. Smart cards are an ideal secure storage device.

Keys, certificates and digital signatures are stored in the card. The card also performs the onboard cryptography operations. network. By using the smart card, storing multiple digital signatures, certificates, private keys, IDs and passwords on a smart card solves the security and portability issues. Sensitive information stored in the card is protected by a PIN. Usually, the user enters the PIN to unlock the card and allows applications the access to the protected information (IDs, Passwords, Keys, Certificates,). The user is no more asked to enter his username and password that can compromise the security of the transaction. The communication between the card and the client program is protected by session keys generated by the card. It is almost difficult to an attacker to spy the cryptography mechanism executed by the card. Before initiating the transactions, the user and the server, the parties participating in the e-business transaction, should be authenticated to each other.

Another advantage of this solution is the portability of the smart card that allows the person performs the transaction from any computer in the

## 4.4 Model based security policy assessment for e-business environment [4]

A model based security policy assessment approach that integrates fault tree analysis technology and top- down architecture driven system analysis method. The assessment process includes security attribute scenarios generation, e-business security model construction, fault tree based threat model construction, and security policy evaluation. It can be used to analyze the security policy for the e-business environment from two different perspectives: 1) Compliance analysis between security policy and e-business security model, intended to elicit all possible discrepancies; 2) Adequacy analysis of security policy for identified threats, aiming at verifying and demonstrating whether the security policy are appropriate for the emerging secure risks.

**Table1. Comparison between various authentication approaches for e-business**

| Approaches | Security requirements | | | | Cryptographic algorithm | | Security-type | Attacks | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | I | C | A | N | Sym | Asym. | | CS | RA | DA | BFA | DDOS |
| **Public key based** | Yes | Yes | Yes | Yes | No | Yes | DC and DS | No | Yes | Yes | No | Yes |
| **Non-Agent based** | Yes | No | Yes | No | Yes | No | Feedback of user | Yes | Yes | Yes | Yes | Yes |
| **Agent based** | Yes | No | Yes | Yes | Yes | Yes | DC, Feedback of user | Yes | No | Yes | Yes | Yes |
| **Model based** | No | Yes | Yes | Yes | Yes | No | PWD, encryption | Yes | Yes | Yes | Yes | Yes |
| **Smart card based** | Yes | Yes | Yes | Yes | Yes | Yes | DC, DS, Keys, ID and PIN | No | No | No | No | Yes |

**I-Integrity, C- Confidentiality, A-Authentication, N-Non repudiation , Sym- Symmetric, Asym- Asymmetric, CS- Channel Sniffing, RA- Riplay attack, DA- Dictionary attack, BFA- Bruite force attack, DC- Digital certificate,DS-Digital signature**

# 5. CONCLUSION

As per overview of various authentication approaches and comparisons of different approaches [table1] we conclude that smart cards are widely acknowledged, as one of the most secure, efficient and reliable forms of an electronic identification (ID) token. A smart card includes an embedded integrated circuit chip that can be either a microcontroller chip with internal memory or a secured memory chip alone. The card communicates with a reader transfers data between the card and the reader. With an embedded microcontroller, smart cards have the unique ability to store large amounts of data, carry out their own on-card functions (e.g., data storage and management, encryption, decryption, and digital signature calculations) and interact intelligently with a smart card reader. Smart card is powerful tool for security, Identification and Authorization. Smart Cards have been widely used as simple token hardware in authentication process. As the e-business is growing rapidly via the internet, many organizations are implementing all the infrastructures that allow them to have secure e-business transactions.

## 6. REFERENCES

[1] Fourar-Laidi, H., "A smart card based framework for securing e-business transactions in distributed systems.", Journal of King Saud University – Computer and Information Sciences (2012), 2012.05.002, pp. 1-5.

[2] Sathiyamoorthy, E., Narayana Iyenger, N., Ramachandran, V., "Agent based trust management framework in distributed e-business environment", International journal of computer science & information technology(IJCSIT), Vol.2., No.1, February 2010.pp. 14-28.

[3] Theodosios, T., George, S., George, P., "Considerations of Public Key Infrastructure (PKI), Functioning as a Chain of Trust in Electronic Payments Systems", International Journal of Information and Communication Engineering 2:5 2006, pp. 330-337

[4] Wang, C., Yanli, F., "Model Based Security Policy Assessment for E-Business Environment", Proceedings of the Second Symposium International Computer Science and Computational Technology(ISCSCT '09) Huangshan, P. R. China, 26-28, Dec. 2009, pp. 088-*093*

[5] Eben, O., "A Systematic Approach to e-Business Security", University of New Brunswick, Fredericton, Canada. 2001,.

**[6]** Srinivasan, S., "Role of trust in e-Business success," Information Management and Computer Security, Vol. 12, No. 1, 2004, pp. 66-72

[7] A Healthcare CFO's Guide To Smart Card Technology And Applications 2/09 "The Smart Card Alliance", card Logix Corporation," smart card & security basics"

[8] M. Henderson, R. Coulter, "Modelling Trust Structure for Public Key Infrastructure", ACISP 2002, Lecture Notes in Computer Science Col 2384, 2002, pp.55-70

[9] S. Gritzalis, D. Gritzalis, "A Digital Seal solution for deploying Trust on Commercial Transactions", Information Management and Computer Security, Vol.9, No.2, 2001, pp.71-79

[10] Rivest, R. et al., "A method for obtaining digital signatures and public-key cryptosystems". 1978. Communication of the ACM 21 (2), 120–126.