Authenticating E - Banking Services in Nigeria through Digital Signatures

G. E. Okereke PhD
Computer Science Department
University of Nigeria, Nsukka
E-mail: george.okereke@unn.edu.ng
Phone Number +2348037784613

O. A. Ezugwu
Computer Science Department
University of Nigeria, Nsukka.
E-mail: assumpta.ezugwu@unn.edu.ng
Phone Number: +2348035689222

ABSTRACT

This paper examined in details the architecture of an electronic banking (E-banking) system. It described the meaning, actors and elements of electronic banking, its usefulness and problems. The paper went further to describe digital signature as a vital tool used to authenticate e-banking services. It provides guidance to financial institutions in Nigeria on identification and control of risks associated with electronic banking activities and discusses e-banking risks from the perspective of the services or products provided to customers.

Keywords: Electronic banking, Authentication, Authorization, Public Key Cryptography, and Digital Signature.

African Journal of Computing & ICT Reference Format:

1. INTRODUCTION

Electronic banking also known as electronic fund transfer requires customer authentication. Reliable customer authentication is necessary for financial institutions engaging in any form of electronic transaction. A reliable authentication mechanism can help financial institutions minimize fraud and promote the legal enforceability of their electronic agreements and operations. Stronger customer authentication strategies are necessary to enforce anti-money laundering measures and help banks and other financial institutions detect and reduce identity theft. Customer interaction with financial institutions is migrating from physical recognition and paper-based operations to remote electronic access and transaction initiation.

The risks associated with business transactions with unauthorized or incorrectly identified individuals in an electronic transaction especially E banking environment could result in fund loss and reputation damage through fraud, disclosure of confidential information, corruption of data, unenforceable agreements among several others. There are a variety of authentication strategies financial institutions can adopt to authenticate customers. These include the use of passwords and personal identification numbers (PINs), digital certificates using a public key infrastructure (PKI), physical devices such as smart cards or other types of "tokens," Kerberos, database comparisons, biometric identifiers and radio frequency identification (RFID) or other forms of “contactless” technology that scans customer information without direct contact between a customer and her bank. [1, 2] The level of risk protection afforded by each of these tools varies and is evolving as technology evolves.

Existing authentication strategies involve three basic "factors":

- What the user knows (e.g., password, PIN);
- What the user possesses (e.g., ATM card, smart card); and
- Who the user is (e.g., biometric characteristic, such as a fingerprint or retinal pattern).

Authentication methods that depend on more than one factor typically are more difficult to compromise than single factor systems. Accordingly, properly designed and implemented multi-factor authentication methods are more reliable indicators of authentication and stronger fraud deterrents in electronic banking.
For example, the use of a logon ID/password is single factor authentication (i.e., what the user knows); whereas, a transaction using an ATM typically requires two-factor authentication: something the user possesses (i.e., the ATM card) combined with something the user knows (i.e., PIN). In general, multi-factor authentication methods should be used on higher risk systems like financial transactions. Furthermore, financial institutions should be sensitive to the fact that proper implementation is key to the reliability and security of any authentication system. For example, a poorly implemented two-factor system may be less secure than a properly implemented single-factor system. The success of a particular authentication method depends on more than the technology. It also depends on appropriate policies, procedures and controls. An effective authentication method should have customer acceptance, reliable performance, scalability to accommodate growth, and interoperability with existing systems and future plans.

2. ELECTRONIC BANKING

Online banking in general is of two types: [1] Internet Banking and Electronic Banking. Internet Banking is conducted through a personal computer that can connect to a bank’s website through the Internet. As an example, a customer can access a bank’s website from his home using a modem and a phone line or through other telecommunications connection via an Internet Service Provider (ISP). This type of banking can also be conducted through wireless technology using the PDA or a cell phone. Electronic banking on the other hand is usually conducted using Automated Teller Machines (ATMs), telephones or debit card, but not necessarily through the Internet. Further discussions on this subject will focus on electronic banking.

Electronic banking, and other types of online banking, offers advantages such as speed of banking, improved efficiency, and convenience as well as less paperwork. But since the Internet is a public network, it presents some privacy and security problems. In general online banking poses significant risks both to the financial institution as well as the customers. Electronic banking depends on a networked environment. Network access can be performed through a combination of devices such as personal computers, telephones, interactive television equipment, and card devices with embedded computer chips. The connections are completed primarily through telephone lines, cable systems, and in some instances wireless technology. These systems whether informational or transactional, facilitate interaction between the bank and the customer, often with the support of third party service provider. It is not all networks that carry the same level of risks, and not all networks are equally vulnerable.

Banks should be careful of insider attack, which is potentially the most damaging because the bank’s personnel, which can include consultants as well as employees, may have authorized access to critical computer resources. Combined with detailed knowledge relating to the bank’s practices and procedures, an internal attacker could access value transfer systems directly or exploit trusted relationship among networked computers to gain a level of access that allows him to bypass established security controls. After that, the attacker could potentially transfer money or other assets inappropriately. For this reason, the first thing a bank should do is to review and evaluate the security of its internal network.
E-banking involves three main security problems: [2]

1. **Spoofing**: this involves a method of assuring customers that they are doing business with the right bank.

2. **Electronic Eavesdropping**: this involves a method of assuring customers that their account number information is not accessible to online eavesdroppers.

3. **Data Alteration**: this involves a method of assuring customers that eavesdroppers cannot alter their personal information. These can be achieved through: authentication – to guard against spoofing; privacy – to guard against eavesdropping; data integrity – to prevent data alteration; and non-repudiation – to guard against denial of a previous act.

### 3. AUTHORIZATION AND AUTHENTICATION

In security engineering, and computer security in general, authorization is a part of operating system that protects computer resources by allowing those resources to be used by resource consumers that have been granted authority to use them. Resources include data, files, computer programs, computer devices and functionalities provided by computer applications.

The authorization process is used to decide if person, program or device K is allowed to have access to data, functionality or service J. Most modern, multi-user operating systems include an authorization process. This makes use of the authentication process to identify consumers. When a consumer tries to use a resource, the authorization process checks that the consumer has been granted permission to use that resource. Permissions are generally defined by the computer's system administrator in some types of "security policy application", such as an access control list or a capability, on the basis of the "principle of least privilege": consumers should only be granted permissions they need to accomplish just their jobs. Older and single user operating systems often had weak or non-existent authentication and authorization systems.

"Anonymous consumers" or "guests", are consumers that have not been required to authenticate. They often have very few permissions. On a distributed system, it is often desirable to grant access without requiring a unique identity. Familiar examples of authorization tokens include keys and tickets: they grant access without proving identity. There is the concept of "trusted" consumers. Consumers that have been authenticated and are indicated as trusted are allowed unrestricted access to resources. "Partially trusted" and guests are subject to authorization for their use of protected resources. The security policy applications of some operating systems, by default, grant full access to all consumers to all resources. Others do the opposite, insisting that the administrator takes deliberate action to enable a consumer to use each resource.

Even when authorization is performed by using a combination of authentication and access control lists, the problems of maintaining the security policy data is not trivial, and often represents as much administrative burden as proving the necessary user identities. It is often desirable to remove a user's authorization: to do this with security policy application requires that the data be updateable. Website authorization and membership management systems often involve the use of Java or JavaScript code which exists in the client site HTML source code. (Example: AuthPro) Drawbacks to such systems are the relative ease in bypassing or circumventing the protection by switching off JavaScript and Meta redirects in the browser, thereby gaining access to the protected web page.

Others take advantage of server-side scripting languages such as JSP, ASP or PHP to authenticate users on the server before delivering the source code to the browser. Some systems take advantage of technology in which web pages are protected using such scripting language code snippets placed in front of the HTML code in the web page source saved in the appropriate extension on the server, such as .jsp, .asp or .php. For additional security, many of the larger websites like Yahoo and Google completely obfuscate any reference to file names in the URL that appears in the address window of the browser. In public policy, authorization is a feature of trusted systems used for security or social control. In banking, an authorization is a hold placed on a customer's account when a purchase is made using a debit card or credit card.

### 4. ELECTRONIC AUTHENTICATION

Verifying the identities of customers and authorizing e-banking activities are integral parts of e-banking financial services. Since traditional paper-based and in-person identity authentication methods reduce the speed and efficiency of electronic transactions, financial institutions have adopted alternative authentication methods, including:

- Passwords and personal identification numbers (PIN)
- Digital certificates using public key infrastructure (PKI)
- Microchip based devices such as smart cards or other types of tokens,
- Database comparisons e.g. fraud screening applications, and
- Biometric identification devices.
The authentication methods listed above vary in the level of security and reliability they provide and in the cost and complexity of their underlying infrastructures. As such, the choice of which technique(s) to use should be commensurate with the risks in the products and services for which they control access.

The Electronic Signatures in Global and National Commerce (E-Sign) Act establishes some uniform federal rules concerning the legal status of electronic signatures and records in commercial and consumer transactions so as to provide more legal certainty and promote the growth of electronic commerce. The development of secure digital signatures continues to evolve with some financial institutions either acting as the certification authority for digital signatures or providing repository services for digital certificates.

5. DIGITAL SIGNATURE ENCRYPTION TO E BANKING

The digital signature is a computerized equivalence of the conventional handwritten signature designed to make transactions between a bank (or receiver) and her customer (or sender) faster, smoother and secure [4, 5]. Two important properties of the current “paper mail” system must be preserved: (a) messages are private, and (b) messages can be signed. A message can be signed digitally using a privately held decryption key. Anyone can verify this signature using the corresponding publicly revealed encryption key. Digital signatures cannot be forged, and a signer cannot later deny the validity of his signature. This has obvious applications in electronic funds transfer and electronic mail systems. We examine the concept of digital signature using the public key encryption. In this method, two keys are kept by the customer namely a public key and a private key. While the public key is made known to the bank, the customer keeps the private key secret. By encrypting the instruction or the message sent by a customer's computer system, the bank is able to determine the authenticity of the supposed customer and his message. The bank would thus be in position to decide whether or not to grant the request of the customer.

5.1 General Concept of Digital Signature

For user B to send a signed message M to user A in a public key cryptosystem, he first computes his signature, S for the message M using $D_B$ (user B’s private or decryption key) [6, 7]:

$$S = D_B(M), \text{ ............... (1)}$$

Deciphering an unenciphered message is reasonable by property (d) of the public key cryptosystem: each message is the ciphertext for some other message). User B then encrypts S using $E_A$ (i.e., user A’s public key), and sends the result $E_A$ to user A. He needs not send M as well since the receiver (user A) can compute it from S.

The recipient (user A) first decrypts the ciphertext with $D_A$ to obtain S. User A knows who is the presumed sender of the message (user B in this case); this can be given if necessary in plaintext attached to S. The receiver then extracts the actual message with the encryption procedure of the sender, $E_B$ in this case (available on the public file).

$$M = E_B(S), \text{ ............... (2)}$$

The recipient (user A) now possesses a message – signature pair (M, S) with properties similar to those of signed paper document. The sender cannot later deny having sent this message, since no one else could have created S = $D_B$ (M), since $D_B$ is his private key.

The receiver can convince a “judge” that

$$E_B(S) = M,$$

and thus has proof that the signed message came from the sender. The recipient clearly cannot modify M to a different version $M'$, since this would involve creating a corresponding signature

$$S' = D_B(M')$$
as well.

Therefore user A has received a message signed by user B, which user A can prove that user B sent, but which user A cannot modify. (Nor can user A forge user B’s signature for any other message). Therefore electronic signature is not only message dependent but also signer dependent.

5.2 Applications to E-Banking

Suppose a customer (sender), S wants to open an account with a bank (receiver), R. Then the customer would essentially choose two keys namely a public key and a private key such that the latter is kept secret by the customer while the former is given to the bank. Anytime the customer contacts the bank to establish a transaction, the bank would secretly choose a random number and encrypt it using the alleged customer’s public key. The bank would then ask the supposed customer to send back to it the chosen random number in order to verify the customer’s signature.
If the ‘customer’ were not the owner of the account in question, then he would not be able to decrypt the bank’s message since he does not know the decryption key. In making this method of financial transaction even more secure, the following measures are considered:

(a) The bank chooses a different random number at different transactions.
(b) The bank asks its customer to send the following information along with the message:
   (i) Time of transmission
   (ii) Date of transmission
   (iii) A password
   (iv) A sequence number
   (v) A checksum of the plaintext which includes the time, date and sequence number.

This way the transaction between a customer and a bank is further strengthened.

6. CONCLUSION

This paper presented a mechanism which uses digital signature encryption to authenticate and authorize transactions between a financial institution and her customers. Most financial institutions in Nigeria are reluctant to engage in E banking transaction out of fear of fraud. E transactions facilitate and enhance the businesses of financial institutions with their customers resulting in higher profit and convenience. Digital signature encryption assures banks and other financial institutions of the security of their E transactions and allays fears associated with fraud in E banking system.

REFERENCES

Authors’ Briefs

**Engr. Dr. George E. Okereke** is a Senior lecturer at the Department of Computer Science, University of Nigeria, Nsukka. He has B.Eng. in Computer Science & Engineering from Enugu State University of Science and Technology, MSc. in Computer Science and Ph.D in Electronic Engineering both from University of Nigeria, Nsukka. His research interests are security measurements, security engineering, computer forensics, web programming and computer architecture. He has published several research and technical papers and is a member to several professional bodies.

**Obianuju Assumpta Ezugwu** is a lecturer at Computer Science Department University of Nigeria, Nsukka. She has both BSc and MSc in Computer Science from University of Nigeria. She is a Research Fellow in the same Department. Her research interests are Software development and Cloud computing. She is a member of several professional bodies.