

**THE CONTINUOUS NEED FOR E-COMMERCE AND TECHNOLOGICAL ADVANCEMENT
OF ELECTRONICS PAYMENT SYSTEM IN NIGERIA**

By

Dr. Bashiru Aremu, Ph.D, M.Sc., B.Sc., FCSTA, MSTAN

The Coordinator of Physical Science Department,

College of Natural Science, Al-Hikmah University, Ilorin, Kwara State, Nigeria

P.M.B. 1601, Adewole Estate, Ilorin, Kwara State Nigeria

E-mail: aremuola@yahoo.com

ABSTRACT

The continuous need for e-commerce and technological advancement have brought about electronic payment systems. This paper, reviews the current state of electronic payment systems in Nigeria by examining two main types of e-commerce: Business to business (B2B) and business to consumer (B2C). B2B system operates within a private and corporate network. B2C system on the other hand operates within an open network like the internet. Private and corporate financial networks are considerably more secure than payments made over an open network like the internet. In this paper, we have considered some of the security aspects and have proposed that Nigeria business environment should embrace the B2C system, which is inter-based, as a pragmatic method to pave way for credit card based purchases in Nigeria. Security of electronic payment systems over the internet can be checkmate by cryptography.

KEYWORDS

E-commerce, Electronic payment systems, Security, Offline, Online, Internet, Cryptography.

INTRODUCTION

The exchange of goods conducted face-to-face between two parties dates back to before the beginning of recorded history. Eventually, as trade become more complicated and inconvenient, humans invented abstract representations of value. As time passed, representations of value

become more and more abstract, progressing from barter through bank notes, payment orders, checks, credit cards, and now electronic payment systems (Asokan, et al 1997).

The issue of security in business transaction is not a new phenomenon. Traditional means of payment suffers from security problems such as:

money being counterfeited, signature being forged, and incidence of bounced checks. Indeed, electronic means of payment inherits the same problems with a few additional risks. Electronic documents can be copied easily. Every payment made is usually accompanied with the name of the buyer, thereby, eliminating the anonymity of cash. Having knowledge of a secret cryptography key meant for a buyer can easily be used to produce digital signatures.

The use of electronic means to settle financial transactions among individuals, private and corporate bodies, is growing considerably. As online payment becomes the foundation of systems for e-commerce, the issue of security is of immense concern. The various electronic payment systems have been considered focusing on issues related to security and the Nigeria experience.

PAYMENT MODELS

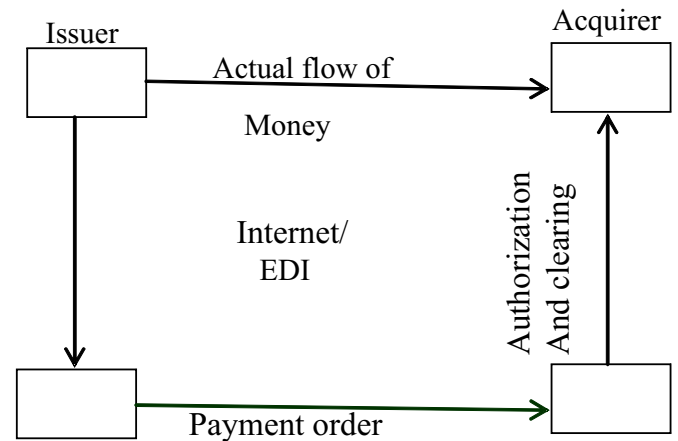
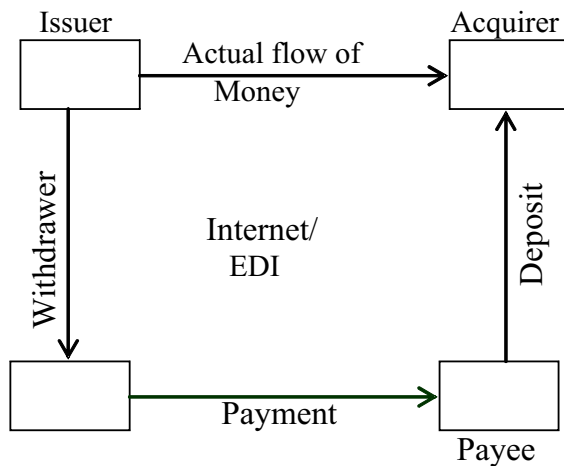
The underlying electronic payment model consists of three parties: a payer, a payee, and at least a bank. The bank's role is divided into two parts: an issuer (the payer's bank) and acquirer (the payee's bank). Electronic payment is accomplished by a flow of money from the payer through the issuer and acquirer to the

payee.

Figure 1 shows a scenario of a prepaid, cash-like payment system where a certain amount of money is withdrawn from the payer bank account before purchases are made. Payments are effected later from this amount. The following payment systems: electronic cash, smart card based electronic purchases, and bank checks belong to this class.

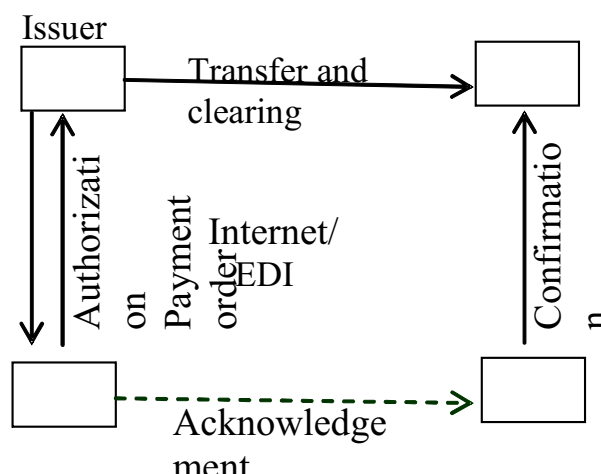
Figure 2 shows a scenario of a bank-card based, check like payment systems with pay-now (debit) system and pay-later (credit) system. In the former system, the payee account is debit at payment time. ATM (automated teller machine) cards belong to this class. In the latter system, the payee's bank account is credited the amount of transaction prior to when the payer's account is debited. Credit card systems belong to this class.

However, the pay-now and pay-later systems fall in the same class from the protocol perspective because payment is implemented always with the payer sending check or credit card slip or other form to the payee.



These types of payment are direct because a form of interaction exists between the payer and the payee. Another form of payment, indirect payment systems, exists in which either the payer

or payee initiates payment without the other party participation online. This is illustrated in figure 3. electric funds transfer fall in this category.



PAYMENTS TECHNIQUES

Offline payment involve the payers and payee only. No third party is involved during payment. The prepaid, cash-like payment systems and all electronic hardware based payment systems, including Mondex, fall in this category. Mondex is the only system that allows offline transferability-a payee can make a new payment himself with the amount received without visiting the bank in between. Mondex has the ability of handling

different currencies simultaneously. It is however, not very popular

Online payments involve, a third party, an authorized server (usually as part of the issuer or acquirer) in each payment. This system involves more communication. The bank-card-based, check- like payment systems and the internet payment systems fall in this category. From the security point of view, online systems are considered more secure than offline systems.

ELECTRONIC PAYMENT SYSTEMS IN NIGERIA

The number of private and corporate financial transactions involved in electronic payment systems in Nigeria is growing tremendously. Commerce always involves buying and selling of goods and services.

Electronic commerce is the common use of business information, the maintenance of business relationship relationships, and the execution of business processes and market transactions while using information technology (Zwass 1996). Electronic business can be classified into business-to business (if enterprises have established a commercial relationship using electronic communications), business-to consumer (if the enterprise wants to use electronic means of communication to sell products or services to consumers), business-to-public (if business and public administration are communicating), and public-to-consumer (if the public administration offers electronic means of contact to consumers), (Gaugler 1999).

In this paper, we will confine ourselves to business to-business (B2B) and business-to-consumer (B2C). these two models do not have the same level of service. Electronic payments in Nigeria appear to have adopted the latter business model, in which payments are carried out through the financial institutions such as the banks. B2B e-commerce automates and streamlines the process of transactions thereby making product

information available while updating it online. Electronic Data interchange (EDI) is used for this type of commerce.

Historically, large companies have used electronic data interchange (EDI) channels as the medium for e-commerce. EDI typically involves expensive infrastructure: inflexible standards, costly software, and dedicated leased lines (Jutla Dawn et al 1999).

Purchase order, electronic funds transfer, and **ATM** are some of the payment mechanisms associated with B2B.

Automated Teller Machine. **ATM** networks are used for obtaining cash and for using debit cards on online authorization by supplying Personal Identification Number (PIN). You can gain access to your bank account through ATM by keying in your PIN- security number known only to you.

Electronic Funds Trasfer. **ETF** is similar to checks, in the sense that it's an instruction to transfer funds from one account to another. It has a fixed overhead cost irrespective of the amount of the transfer. Electronic funds transfers are fast whether overnight or immediate compared to other payment mechanisms. It provides the parties concerned with immediate acknowledgement of their transfers.

Purchase orders. These are not really payment systems per se, but a means to create billing records for future settlement by a direct payment mechanism. B2C business model, on the other

hand is approaching a global common commercial environment, where credit cards supported by global brands such as Visa, Master card. And American Express strives for individual consumers.\

Most payment systems in Nigeria operates in private and corporate networks thereby limiting the scope of commerce. Payments through open networks like the internet is common in the developed countries of the world.

INTERNET PAYMENT SYSTEMS

The commercial development of the internet has led to the creation of several payment systems specifically designed for internet commerce (Treese et al 1998) such as First Virtual, cyber cash, electronic cash, online credit cards, and micro payments. Credit card are the most popular among them.

Internet payment is the foundation of internet commerce. In spite of the considerable growth in the use of internet for e-commerce, Nigeria has not benefited much from this wonderful technology. Internet payment system in Nigeria is at best at it's infancy. We are not talking about the development of technologies for internet payment systems, we are talking about the utilization of technologies that are already available that are not fully harnessed.

On the internet, and the electronic world in general, most system use, electronic world in

general, most systems use, electronic funds transfer, purchase orders and credit cards, some other newer systems, such as electronic checks and electronic cash have not yet received widespread use.

SECURITY CONSIDERATIONS

Electronic funds transfer over private and corporate financial networks is considerably more secure financial networks considerably more secure than payments made over open networks like the internet. Generally, electronic payment systems must exhibit integrity, authorization, confidentiality, availability, reliability, and accountability.

Integrity: if a payment system guarantees integrity, it means that its data are kept intact irrespective of accidental errors or malicious intent.

Authorization: provides the most vital relationship in a payment system, a means of asking, "what are you allowed to do?" payment can be authorized such as telephone or e-mail, password authorization, and signature authorization.

Confidentiality describe the means whereby knowledge of transaction contents is restricted from unauthorized disclosure.

Availability and reliability is the ability to make or receive payments within an appropriate period of time. In the event of network or system failure, no

payer would agree to take responsibility for a loss of money.

Accountability is the ability of a payment system to ensure that the partners involved in a communication activity are truly the sender and recipient, so that, in case of any breach, the communicating partners can be held accountable.

CRYPTOGRAPHY

Cryptography has become an essential technique for providing privacy, authentication, message integrity, and non repudiation on an open network. Cryptography systems that provide these techniques are growing rapidly.

Privacy is the ability to keep the message secret and only the sender and intended recipient know the content of the message.

Authentication give the knowledge to the recipient that the message is genuine and where it came from. The sender is aware that the message is going to the intended recipient.

Integrity is maintained when the recipient knows that the messages was not corrupted accidentally or intentionally while in transit.

Non repudiation is a situation where the sender of the message cannot deny sending the message.

Secret Key Cryptography is a shared key cryptography system where the payer and a verifier (the issuer) both have the same secret keys. It does not support non repudiation, since either the sender or intended recipient could have

created the message.

Public key cryptography is different from the shared key cryptography. Typically, a payer and a verifier create their own key pair (private and public key pair) but the private signing key is made secret. The recipient can authenticate the sender of a message by verifying a digital signature.

The concept of digital signature has been introduced by Diffie W and Hellman M. (Diffie et al 1976). A digital signature scheme is a public key algorithm that allows to authentic a message by means of a piece of information, called the signature, the generation of the signature requires the knowledge of the corresponding public key is necessary. If the public key is publicly accessible, then everybody can verify the signature, while only the signer, who knows the private key, is able to sign (camenisch jan L et al 1994). Rivest, shamir, Adleman (RSA) is one of the known public key cryptosystem. Non repudiation can be provided using digital signatures.

Generally, the Secure Socket Layer (SSL) is a security scheme that is based on public key signatures. It is a socket layer communication interface that enables two parties to communicate securely over an open network. SSL is not a payment system but it can be used to secure payment messages. It does provide non repudiation. Payment systems based on public key cryptography include: Cyber cash, E-cash, Net cash, and secure Electronic Transactions (SET).

SET was the brainchild of Master card, Visa, IBM, Microsoft, Netscape, and a few others, and it has become a standard for credit card based online payment schemes over the internet. SET provides easy, fast and secure transactions over the internet. It provides strong encryption and authentication of all of the parties in a credit card transaction to maintain securely communicating credit card numbers between the payer and acquirer.

ANONYMOUS ELECTRONIC PAYMENT SYSTEMS

Most cash-like payment systems provide anonymity and untrace ability. Typically, payers would want all payment private without unrelated third parties to ascertain and monitor their payments. They wished that the payees and in some cases the bank would not be able to really observe and monitor their payment. Anonymity hide the identity of payer whereas intractability separates two different payment by a particular payer. Cash is anonymous and untraceable. Cryptography has made it possible for all payment systems to be made untraceable by outsider .E-cash (online), is a payment system that supports anonymity and intractability against payee and issuer Ventication can be made using a special from of signatures know as blind signatures.

D Chaum introduced the concept of blind signatures (chaum 1983), which is an extension of the concept of digital signature. There are now

parties involved in the signature: a sender who chooses the message to be signed, and the signer who provide the sender with information allowing him or her to compute the signature. The main difference to ordinary digital signatures is that the signer does not receive any information, neither on the message nor on the resulting signature. More formally, the signer's information and the resulting message signature pair are statistically independent (Camenisch Jan L et al 1994).

Payment systems based on value cards also provide payer's anonymity. A value card is a smart card storing information that can be used by means of payment. A phone card is a typical example of a value card: units are stored on the card and debited when making a call. Some value cards can be reloaded and may be hence seen as an electronic purse (Camenisch et al 1994)

Other payment systems like anonymous credit cards and Net cash support anonymity and untraceability but they are based on trusted third parties which conceal information about the flow of all payment made between the payer and payee. We are of the opinion that the implementation of anonymous electronic payment systems should be very attractive to Nigerians, who generally cherish the anonymity and untraced ability associated with cash payments.

THE TASKS AHEAD

Electronic commerce lets people purchase good and exchange information on business transaction online. The most popular e-commerce channel is the internet. Although the internet's role as a business channel is a fairly recent phenomenon, its impact, its impact, financial and otherwise, has been substantially greater than that of other business channels in existence for several decades (Simon S.Y. Shin et al 2000).

The challenge, therefore, is for Nigeria business environment to embrace the B2C business model where payees can make use of electronic means of communication to sell products or services to consumers, typically, using the credit cards. This will usher in the use of credit card based purchases in the business scene. Technological infrastructure such as internet is a precondition for B2C. Internet services are not meant for sending or receiving e-mails alone. Internet is a medium of e-commerce and efforts must be intensified to explore it. private and corporate financial transactions can be done via an open network such as the internet, thereby increasing the frontier of e-commerce.

Government must create the enabling environment to support e-commerce so that organizations or individuals can afford to have access to the internet. Nigeria economy is largely government driven. Over the years, government policy had hindered the provision of some essential infrastructures for technological

advancement such as the internet. Government establishments and agencies appear to be the worst of it. we hope that as Nigeria moves from government to private driven economy, we shall experience a dramatic change in terms of the provision and access to internet.

Conclusion

We have presented electronic payment models and techniques, and discussed the types of payments systems practiced in Nigeria. We also presented other payment system: internet and anonymous. The Internet payment system is not popular in Nigeria perhaps because credit card purchases are not widely available yet. Europe and other developed countries of the world that cherish comfort, convenience and efficiency have since been enjoying this wonderful technology.

You can stay in your house and shop on the internet. All the customer has to do is, point, click, and buy.

We hope and believe that as Nigeria graduate from the Government led economy to the private sector driven economy, Nigeria will benefit from the Internet technology as a means of settling payments.

References

Asokan N., Phillipe A., Steiner M., Waidner M.,
“The State of the Art in Electronic Payment

Systems", IEEE Computer Society, September 1997, pp. 28-35.

Chaum D., "Blind Signature System," Advances in Cryptology, Crypto '83, plenum, p. 153.

Camenisch Jan L., Piveteau Jean-Marc., Stadler M.A., "Security in Payment System," Proceedings of ESORICS 94.

Diffie W and Hellman M., "New Directions in Cryptography," IEEE Trans., Info., Theory, 1976, pp. 644-654.

Gaugler Thomas., "Interorganisatorische Informationssystem (IOS): Ein Gestaltungsrahmen fur das Informationsmanagemnet, "Phd thesis Instut Fur informatik, universitat Zurich, 1999.

Jutla D, Bodorik P., Hajnal C., Davis C., "Making Business Sense of Electronic Commerce IEEE Computer Society, March 1999. pp. 67-75.

Knorr K and Rohrig S., "Security of Electronic Business Applications: Structure and Quantification "A paper jointly funded by the Swiss National Foundation under grant SPP-ICS 5003-045359 of the Department of Computer Science, University of Zurich, Switzerland, knorr@ifi.unizh.ch.

Simon S.Y. Shim., Vishnis S. Pendyala., Meera Sundaram., E-commerce Frameworks," IEEE Computer Society, October, 2000, pp. 40-47.

Treese G.W and Stewart L.C., "Designing Systems for Internet Commerce, "Addison Wesley Coy., 1998.

Weaver A.C., Vetter R.J., Whinston A.B., Swigger K., "The Future of E-commerce," IEEE Computer Society, October, 2000, pp. 30-31.

Zwass V., "Electronic Commerce: Structures And Issues, "International Journal of Electronic Commerce, 1(1):3-23, 1996.