## Introduction

Automatic Teller Machines (ATMs) are self-service banking machines that allows customers to access their bank account without the aid of a bank teller or bank clerk. They are used for financial transactions, they operate 24 hour a day helping customers to withdraw cash, deposit cash, transfer funds, check account balance, and print statement of account. They are placed in convenient locations such as the retail outlets, banking premises, grocery stores, shopping malls and gas stations. They make banking transaction easier, by helping banks to meet the demands of their customers; customers do not need to go to the banking hall or even in some cases they do not need to queue in banks just to make basic banking transactions. Some ATM machines allow customers of different banks to perform basic banking transactions without going to their bank or their banks ATM machine. Despite all these advantages, it has been reported in that customers and banks are faced with a lot of ATM fraud and other ATM security related problems. Therefore, there is a need to provide a means of securing ATM transaction against frauds and crimes. This study presents how Short Message Service (SMS) encrypted message can help make ATMs more secured. The proposed technology includes the use of existing Personal Identification Number (PIN) to provide authentication of the card to card issuer host system and the use of SMS encrypted message to authenticate customers before any transaction can take place at the ATM machine.

PROBLEM WITH THE ATM: With the growing number of ATM put in use, ATM security breaches are now a daily occurrence around the world. Attacks on ATM include phishing, shoulder surfing and the installation of ATM skimmer. ATM skimmers are used to read the ATM card number. Cameras are also installed at the ATM to read the PIN and other bank account information’s. This stolen information’s can be used to create fake or cloned ATM cards which can be used to steal money from the customer’s account. ATM PIN verification uses encryption technique. Access to PINs of some cards issued from same bank can help an attacker determine the encryption key used by that bank hence the PIN to any ATM card issued by that bank can then be determined. ATM fraudsters have become more sophisticated, they have used ATM machine to defraud banks. To address these issues, banks and customers are requiring new security enhancements for ATMs in order to provide improved security for financial institutions and prevent ATMs from being compromised.

## Elliptical Curve Cryptography

Elliptical curve cryptography (ECC) is a public key encryption technique based on elliptic curve theory that can be used to create faster, smaller, and more efficient cryptographic keys. ECC generates keys through the properties of the elliptic curve equation instead of the traditional method of generation as the product of very large prime numbers. The technology can be used in conjunction with most public key encryption methods, such as RSA, and Diffie-Hellman. According to some researchers, ECC can yield a level of security with a 164-bit key that other systems require a 1,024-bit key to achieve. Because ECC helps to establish equivalent security with lower computing power and battery resource usage, it is becoming widely used for mobile applications. ECC was developed by Certicom, a mobile e-business security provider, and was recently licensed by Hifn, a manufacturer of integrated circuitry (IC) and network security products. RSA has been developing its own version of ECC. Many manufacturers, including 3COM, Cylink, Motorola, Pitney Bowes, Siemens, TRW, and VeriFone have included support for ECC in their products.

## Architecture Design

After thorough study of the security features in ATM transaction, a security scheme is proposed. Our proposal is not replacing the existing security technology; rather it serves as an additional layer of security that protects the existing authentication system from frauds and crimes. Our concern is to provide a secure end to end communication of OTP to customer’s by encrypting the SMS message used to send the OTP from the bank server to the customer’s mobile phone.

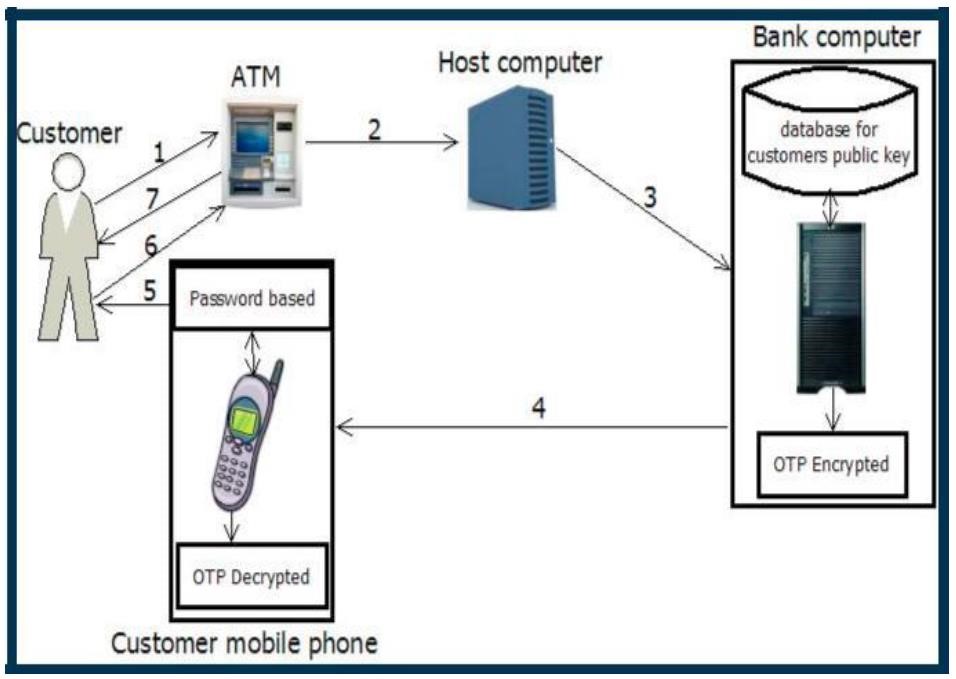
There are two banking modules in the proposed secure model, one at the bank server and the other on customer’s mobile phone. The module at the bank server will contain a database where the entire customer’s encryption key will be stored. This encryption key will be used to encrypt SMS message containing the generated OTP before it is sent to the customer’s mobile phone. The module on the customer’s mobile phone will contain the decryption key for decrypting received encrypted SMS from the bank server. This module is password based; the customer needs to enter a password before access is granted to the module. This is done in order to secure the module from unauthorized users. Both modules use Elliptic curve encryption for encrypting and decrypting the SMS message containing the OTP.

Elliptic curve is an asymmetric encryption technique. The study also explained that Elliptic curve encryption technique is a suitable asymmetric encryption technique for encrypting SMS transmitted message due to its ability of using smaller key size to obtain same security as compared to other asymmetric encryption techniques. Asymmetric encryption technique is used in the proposed model in order to prevent the decryption key from being compromised. On like the symmetric encryption technique which uses same key for encryption and decryption, the Asymmetric encryption uses two related keys, public and private key

The public key will be stored in the bank server database while the private key will be stored in customer’s mobile phone. If the database containing the customers encrypting key is compromised, the decryption key will definitely not be compromised since the decryption key is stored in the customer’s mobile phone. Using asymmetric encryption to encrypt the SMS message containing the OTP at the bank computer and decrypting it after it is received at the customer’s mobile phone will prevent the OTP against eavesdropping and interception, thereby providing security to ATM transactions.

Customer’s public and private keys can be generated by physically connecting the customer’s mobile phone to the bank computer using a cable. The public key is stored in a database at the bank server as the encrypting key while the private key will be stored on the customer’s mobile phone as the decrypting key. These keys can only be renewed if the customer’s mobile phone is physically connected to the bank’s computer.

In the proposed technology, if the customer initiates a transaction at the ATM, after entering the PIN, if the PIN is authenticated, the bank server generates the OTP, gets the customer’s public key from the database, encrypt the OTP and send it to the customer’s mobile phone via SMS. Customer on receiving the encrypted SMS decrypts it using the private key to get the OTP. This additional layer on the existing security technology will help protect the OTP’s transmission from malicious attack and eavesdropping, thereby providing security to ATM transactions. This technology is illustrated in the below figure.



We know that ECC (Elliptic Curve Cryptography) uses the Discrete Logarithm Problem, which acts like a trapdoor function. But similar kind of function is also used by RSA and some other methods. So, why ECC?

This is because to get similar security levels on both RSA and Elliptic Curve, the latter does its job much better and efficiently.

The small key sizes make ECC very appealing for devices with limited storage or processing power, like our smart phones. The smaller space it takes to store the keys with the same level of security, much better.

## Conclusion

An asymmetric based encryption solution for securing OTP transmitted via SMS is introduced in this study. It is a scheme that provides an end to end security for SMS message containing the OTP send by bank server to customers for authentication, thereby providing security to ATM banking transaction. This scheme can be used by banks to provide confidentiality and authenticity to the bank-customer’s communications through ATM. However, this scheme is not limited to ATM security, it can also be used to provide secured communication between banks and customer’s in mobile and online banking.