(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
12 November 2009 (12.11.2009)

PCT

(10) International Publication Number
WO 2009/136404 A2

(51) International Patent Classification:
*H04W 12/08* (2009.01) *G06Q 20/00* (2006.01)

(21) International Application Number:
PCT/IN2008/000250

(22) International Filing Date:
17 April 2008 (17.04.2008)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant: ATOM TECHNOLOGIES LIMITED [IN/IN]; 1st Floor, Malkani Chamber, Off. Nehru Road, Vile Parle (East), Mumbai 400 099, Maharashtra (IN).

(72) Inventor: DEWANG, Neralla; Director of Atom Techlogies Limited, 4, Raj Neelam, Dr. Rajaballi Road, Warden Road, Mumbai 400 026, Maharashtra (IN).

(74) Agent: VINOD, Bhagat, A.; Arjun T. Bhagat & Co., Advocates/Trade Mark & Patent Attorneys, 6-B, Shaheen Apartments, 132, Mody Street, 1st Floor, Fort, Mumbai 400 001 (IN).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, NO, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

**Declarations under Rule 4.17**:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*

— *of inventorship (Rule 4.17(iv))*

**Published**:

— *without international search report and to be republished upon receipt of that report (Rule 48.2(g))*

WO 2009/136404 A2

# (54) Title: A SYSTEM AND METHOD FOR IMPLEMENTING A SECURE TRANSACTION THROUGH MOBILE COMMUNICATING DEVICE

**(57) Abstract**: This invention relates to implementing secure electronic transactions through mobile communicating devices thereby providing for a secure and convenient platform for the merchant and the customer to transact through mobile communicating devices with the help of a GSM service provider and banks. Under this invention the following methods are developed viz. Requesting an electronic card / terminal from the mobile phone; securely loading the customer's electronic card directly on customer's mobile phone; securely sending the card information back to the card issuer (bank) whenever required for authorization during a transaction; securely loading the merchant electronic terminal directly on merchant's mobile phone; securely sending the terminal details to terminal issuer (acquiring bank) whenever the merchant initiates a sale transaction.

# A SYSTEM AND METHOD FOR IMPLEMENTING A SECURE TRANSACTION THROUGH MOBILE COMMUNICATING DEVICE

## TECHNICAL FIELD :

This invention relates to implementing secure electronic transactions through mobile communicating devices.

This invention more particularly relates to a system which provides a secure and convenient platform for the merchant and the customer to transact through mobile communicating devices with the help of a GSM service provider and banks.

Under this invention the following methods are developed viz. Requesting an electronic card / terminal from the mobile phone; securely loading the customer's electronic card directly on customer's mobile phone; securely sending the card information back to the card issuer (bank) whenever required for authorization during a transaction; securely loading the merchant electronic terminal directly on merchant's mobile phone; securely sending the terminal details to terminal issuer (acquiring bank) whenever the merchant initiates a sale transaction.

## PRIOR ART :

The idea of paying for goods and services electronically is not a new one. All around we see evidences of transactions taking place where at least part of the process is carried out electronically. Since the late 1970's and the early 1980's a variety of schemes have been allowed payment to be affected across a computer network.

The Current System:
In current card payment scenario the following parties are involved:

1) Merchant
2) Merchant Acquiring Bank (who gives the Point of Sale terminal to the Merchant)

3) Card Issuing Bank (who gives the payment card to the Customer)

4) Clearing and Settlement Agency (an organization which settles between the Acquiring and Issuing Bank)

Card and Terminal Based Payment System: Figure (1.0)

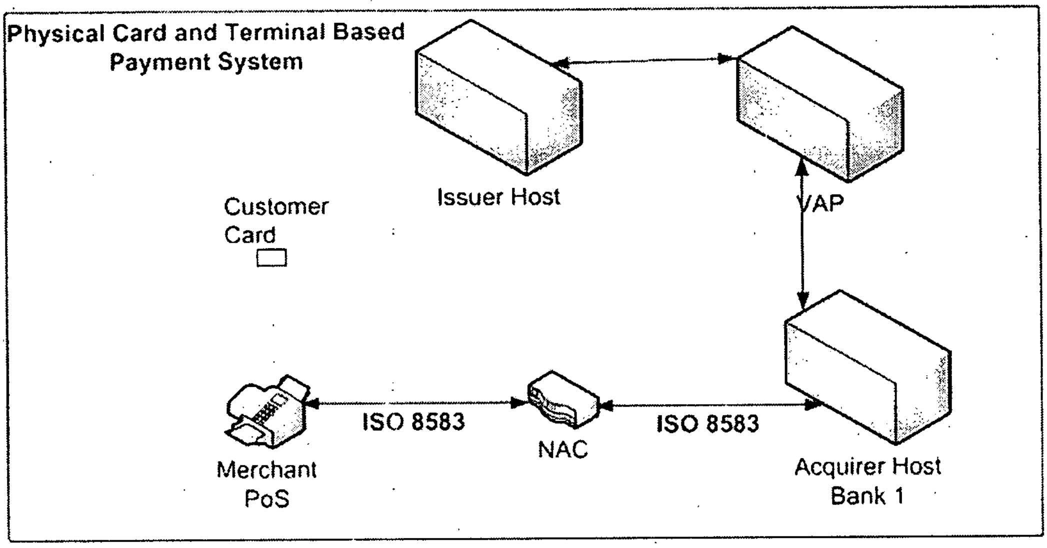


Figure (1.0) illustrates the current physical card / terminal payment system in which the customer presents the card to the merchant who then swipes the same in the physical Point of Sale (PoS) Terminal. PoS dials out to NAC (Network Access Concentrator) which then connects to Acquiring bank Host. Acquiring Bank Host routes the transaction to Visa Access Point (VAP), which is in-turn, connected to the Issuing Bank Host. Issuing Bank Host validates the card and sends it back to Acquirer Host via VAP. The Acquiring Bank Host sends it back to PoS and then receipts are printed by the PoS to be kept by the customer and merchant respectively.

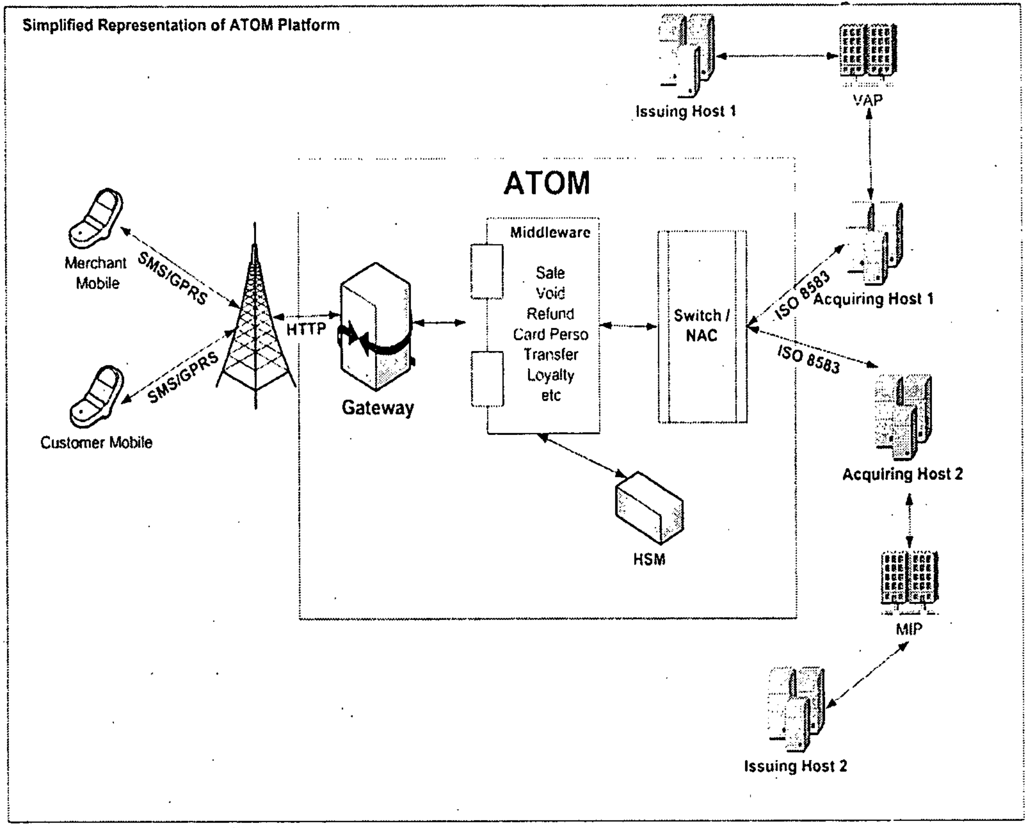
## Our Invention

## Introduction

The Transaction Platform (ATP) of the present invention enables the customers and the merchants to use the mobile phones for conducting secure financial transactions. In addition to mobile based merchant, the platform also facilitates PC based merchant and the internet merchant to connect to ATP.

In this Platform merchant is expected to register with it to avail its Platform merchant services and later registers with the Acquirer as a Merchant to perform payment transaction.

In this Platform customer is expected to register with it to avail its Platform customer services and later registers with the issuer as a cardholder to perform payment transaction.



Simplified Representation of ATOM Platform: figure (1.1)

The following abbreviations and notations are used in this document

**ICCID** Integrated Circuit Card Identification. Unique identifier identifies a SIM Card.

**Acquirer/Acquiring Bank** Obtains merchant's credit card transactions and processes them for payment

**ATOM Customer ID** Unique ID assigned to every customer by the ATOM Platform to identify the customer.

**ATOM Merchant ID** Unique ID assigned to every merchant by the ATOM Platform to identify the customer.

**Authorization Code** A code that a credit card issuing bank returns in an electronic message to POS that indicates approval of the transaction. The code serves as proof of authorization

**Authorization Response** An issuing financial institution's electronic message reply to an authorization request, which may include:
Approval - transaction was approved
Decline - transaction was not approved
Referral - response pending more information, merchant must call the toll-free

**Authorization** The process of verifying the credit card has sufficient funds (credit) available to cover the amount of the transaction. An authorization is obtained for every sale

**Card Association** Any entity whose members issue credit or debit cards or acquire card payment transactions on behalf of their customers.

**Card Index** The location on which the Card detail is stored inside the customer SIM.

**Card Number** Uniquely identifies the card (Debit Card/ Credit Card/ Pre Paid Card like Sodex Ho)

**Customer/Cardholder** Customer associated with the primary account number requesting the transaction from the card acceptor.

**DES** Data Encryption Standard. A block cipher that encrypts data in 64-bit blocks. DES is a symmetric algorithm that uses the same algorithm and key for encryption and decryption.

Developed in the early 1970s, DES is also known as the DEA (Data Encryption Algorithm) by ANSI and the DEA-1 by ISO.

**ECC**

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.

**Encryption**

Encryption scrambles and unscrambles information using mathematical equations and a secret code called a key.

**GSM**

GSM (Global System for Mobile communication) is a digital mobile telephone system that is widely used in Europe and other parts of the world. GSM uses a variation of time division multiple access (TDMA) and is the most widely used of the three digital wireless telephone technologies (TDMA, GSM, and CDMA). GSM digitizes and compresses data, then sends it down a channel with two other streams of user data, each in its own time slot. It operates at either the 900 MHz or 1800 MHz frequency band.

**Issuer / Issuing Bank**

Organizations like banks, building societies and others, which give out cards to customers, are called issuers.

**J2ME**

Java 2 Platform, Micro Edition (J2ME) is the edition of the Java platform that is targeted at small, standalone or connectable consumer and embedded devices, such as cellular phones and personal digital assistants (PDAs).

The J2ME technology consists of a virtual machine and a set of APIs suitable for tailored runtime environments for these devices. The J2ME technology has two primary kinds of components--configurations and profiles.

**Loyalty Program** A program designed to lower the turnover among users of a product or service by rewarding a customer with incentives or other benefits for remaining a customer.

**MAC** An algorithm that allows a receiver to ensure that a block of data has retained its integrity from the time it was sent until the time it was received.

**Merchant** A retailer, or any other person, firm, or corporation that, according to a Merchant Agreement, agrees to accept credit cards, debit cards, or both, when properly presented.

**Merchant ID** Uniquely identifies a given merchant. The acquirer assigns Merchant ID during merchant registration.

**Merchant Category Code** Classifies the type of business being done by the merchant, represented according to ISO 8583:1993 for Card Acceptor Business Code.

**Merchant Discretionary Data** Any merchant related data sent to the customer mobile. Eg., A/C number for bill payment.

**Message** A set of data elements used to exchange information between Customer, Merchant, ATOM Platform and institutions (or their agents).

**Message Type** Unique message identifier identifies the type of the message. Message type is part of the message header to identify the message type.

**PAN** Primary Account Number, the cardholder's account number to which transactions are to be charged.

**PIN** Personal Identification Number. The confidential individual number or code used by a cardholder to authenticate card ownership for ATM or POS terminal transactions.

**PoS** Point of Sale. Location where transaction is originated.

**PSN** PAN Sequence Number, Identifies and differentiates cards with the same PAN.

**Pseudo-random number** A number extracted from a pseudo-random sequence.

**Pseudo-random sequence** A deterministic function which produces a sequence of bits with qualities similar to that of a truly random sequence.

**Random Number** As opposed to a pseudo-random number, a truly random number is a number produced independently of its generating criteria. For cryptographic purposes, numbers based on physical measurements, such as a Geiger counter, are considered random.

**Retrieval Reference Number** This twelve-character fixed length field contains the transaction retrieval reference number returned by the authorizing system. The reference number should be printed on the receipt.

**Secret Key**

In secret-key cryptography, this is the key used both for encryption and decryption.

**Service ID**

Unique ID identifies the service to which the message is to be delivered by the ATOM Platform. In ATOM Platform service ID '03' refers to payment service.

**Session Key**

A key for symmetric-key cryptosystems which is used for the duration of one message or communication session.

**SMS**

Short Message Service. A service for sending messages of up to 160 characters to mobile phones that use Global System for Mobile (GSM) communication.

**Symbian**

An open operating system designed for cell phones that support multimedia messaging, Bluetooth, and Java.

**Track 2**

The second magnetic track on a financial transaction card. It is read-only, and its contents are defined in ISO 7813.

**Terminal ID**

Designates the unique location of a terminal at a merchant. The acquirer issues Terminal ID during merchant registration.

**Transaction ID**

Unique Identifier assigned to a transaction in the ATOM Platform. The Transaction ID is valid only till the completion of the transaction.

**Virtual NAC / PoS**

Software implementation of a Standard Point of Sale terminal / Network Access Controller. An electronic system that accepts financial data and transmits that data to a computer or authorization network for reporting activity, authorization and transaction logging.

**Triple DES / 3DES** A variation of the DES block cipher algorithm that encrypts plain text with one key, encrypts the resulting cipher text with a second key, and finally, encrypts the result of the second encryption with a third key. Triple DES is a symmetric algorithm that uses the same algorithm and keys for encryption and decryption.

## ATOM Platform

ATOM is a scheme that has been successful in taking the e-payments one step ahead to m-payments (mobile payments). To achieve the same ATOM has developed a secure and robust interoperable transaction platform called the ATOM Transaction Platform abbreviated as ATP.

In the case of mobile payments as envisaged by ATOM in the figure 1.1 above, ATOM will be playing the role as described in the illustration above.

## Client side Payment Application

The core payment engine is Java 2 Micro Edition (J2ME) based Customer/Merchant application The J2ME payment application shall be loaded into the mobile supporting J2ME CLDC1.0/MIDP2.0 specification.

The Merchant and the Customer application residing in the mobile are developed as J2ME application so that it can be loaded into the J2ME based mobile phones.

## Loading J2ME Application

The ATOM J2ME application should be loaded into the customer and merchant mobile phone to enable mobile payment. The J2ME MIDP 2.0 phone is required for the application to get loaded into it. The application shall be loaded in the following ways:

1) Data cable connected to PC
2) GPRS internet access
3) Bluetooth and
4) Infrared
5) Pre-installed by the handset manufacturer

**Brief Description of Drawings:**

The invention will be now more clearly explained with the following non limiting figures, where

Fig_1 shows the process of merchant requesting for registration with the Platform

Fig_2 shows the process of the Platform Registering the Merchant

Fig_3 shows the process of merchant requesting for registration with Acquirer

Fig_4 shows the process of Platform forwarding the Merchant Request to the Acquiring Bank.

Fig_5 shows the process of Merchant – Acquirer confirmation detail loading into the Merchant Mobile

Fig_6 shows the process of Customer requesting for registration with the Platform

Fig_7 shows the process of Platform Registering Customer

Fig_8 shows the process of Customer requesting for loading of electronic card into the Mobile

Fig_9 shows the process of Electronic card loading into the customer Mobile

Fig_10 shows the process of Electronic card load Confirmation sent back to the Platform

Fig_11 shows the process of Sale Transaction

Fig_12 shows the process of void Transaction

Fig_13 shows the process of refund Transaction

**Steps Involved for a Merchant to perform Payment Transaction**

**Merchant Registration with ATOM Platform**

The Merchant is expected to first register with ATOM Platform as an ATOM Merchant. This is a pre-registration process for any merchant to avail ATOM Platform merchant services.

**Merchant request for registration with ATOM Platform**

The Merchant application loaded into the merchant Mobile is a generic ATOM Merchant application without any merchant specific details. To get the applet personalized for a particular merchant, the applet needs to be personalized with Merchant specific information. To avail ATOM Platform merchant services, the interested merchant is first expected to get registered with ATOM Platform.

Fig_1

The merchant registration request logic is built into the Merchant application as part of the standard functionality.
The registration request data is sent in a single SMS.

**ATOM Platform Registering Merchant**

ATOM platform on receiving registration request from the interested merchant will perform necessary validation in the system for duplicate request and generates a unique ATOM Merchant ID. ATOM platform also generates Merchant specific security keys for loading into the merchant mobile.

Fig_2

The registration data is sent in a single SMS.

**Merchant Registration with Acquirer**

To perform payment transaction the ATOM merchant should require arrangement with acquiring bank.

**Merchant request for registration with Acquirer**

The merchant having existing relationship with the acquiring bank or a merchant interested in having relationship with the Acquirer shall request for merchant acquirer registration. The interested merchant will send the terminal request along with the acquiring bank name to ATOM platform which is then forward to the respective Acquiring banks for further processing.

Fig_3

The merchant-acquirer registration request logic is built into the Merchant application as part of the standard functionality.
The registration request data is sent in a single SMS.

**ATOM Platform forwarding the Merchant Request to the Acquiring Bank.**

The data of the person interested in having relationship with the Acquirer will be forwarded to the respective acquiring bank along with the merchant contact detail. The acquiring bank is expected to contact the person who is interested in having relationship and further process the request on their own mode of Mobile.

Fig_4

The communication channel for transferring the merchant request data between ATOM platform and the acquiring bank shall be through agreed upon medium. It may be through e-mail, CD, etc.

**Merchant – Acquirer confirmation detail loaded into the Merchant Mobile**

The Acquiring bank on processing the merchant request shall register the merchant in their system; the acquirer will send the merchant detail to ATOM platform to load it on to the merchant.

Fig_5

ATOM Platform receives the merchant registration detail from the Acquiring bank and sends it to the merchant mobile. The merchant can carry out payment transaction only after the registration data is personalized into his Mobile.

The communication channel for transferring the merchant registration detail between ATOM platform and the acquiring bank shall be through agreed upon medium. It may be through e-mail, CD, etc. The communication channel between ATOM platform and Merchant Mobile is through SMS/GPRS.

### Steps involved for a Customer to perform Payment Transaction

The customer is expected to register with ATOM platform to avail atom customer services. The ATOM platform enables the registered customer to perform payment transactions securely and conveniently. The person interested in performing payment transaction in his mobile shall first register with ATOM platform and later, request the Issuing bank to load the electronic Credit / Debit card into his mobile.

### Customer Registration with ATOM platform

### Customer request for registration with ATOM Platform

The Customer application loaded into the customer mobile is a generic ATOM Customer application without any customer specific details. To get the application personalized for a particular customer, the application needs to be loaded with customer specific information. To avail ATOM Platform customer services, the interested customer is first expected to register with ATOM Platform.

Fig_6

The customer registration request logic is built into the customer applet as part of the standard functionality.

## ATOM Platform Registering Customer

ATOM platform on receiving registration request from the interested customer will perform necessary validation in the system to check for duplicate request and generates security Keys and registers the customer with ATOM loyalty scheme for availing loyalty points in the system.

Fig_7

The registration data is sent in a single SMS.

## Customer request for loading electronic card into the Mobile

The Customer is expected to send the card load request to atom platform after registering with ATOM to perform financial transactions. The ATOM platform facilitates the customer to perform payment transactions, provided the customer mobile is loaded with electronic card issued by the issuing bank. To load the electronic card into the customer mobile, ATOM customer shall request the issuer to load the electronic card. The ATOM platform receives the request from the customer and sends it to the appropriate issuing bank to process the customer request for card loading.

Fig_8

The customer card load request logic is built into the customer applet as part of the standard functionality.

The data transferred to the issuing bank shall be through e-mail, CD, etc.

## Electronic card load into the customer Mobile

The Issuing bank after verifying the interested customer shall prepare card personalization data and transfers the electronic card data to ATOM platform.

The Issuing bank shall first registers with ATOM and shall generate the required Master Key(s) into the HSM residing with ATOM. ATOM uses this key to encrypt the card data of the customer before loading it into the customer mobile.

The transaction performed by the customers using the electronic card loaded into their mobile is treated as a card present transaction

Fig_9

**Electronic card load Confirmation sent back to ATOM Platform**

The customer mobile on receiving the card load data will respond with confirmation detail to ATOM platform.

FIG_10

**How it works**

ATOM has created a transaction platform to enable transactions through mobile phones. The application has two parts – Application on the mobile phone (Front-end Application) and ATOM Transaction Platform (Backend).

The merchant initiates the transaction from his mobile phone and enters the customer id and amount. This request is received by ATOM Transaction Platform (Backend) and sent to customer's mobile phone for payment. Customer selects the appropriate card stored on the mobile and sends the card details for authorization. ATOM Transaction Platform (Backend) receives the details from the customer and sends to Acquiring Bank for authorization from Issuing Bank. On receiving the confirmation from Acquiring Bank, Transaction Platform (Backend) sends receipts to Customer and Merchant.

ATOM enables secure electronic transactions through mobile phone. ATOM has developed a method for:

1. Requesting an electronic card / terminal from the mobile phone

2. Securely loading the customer's electronic card directly on customer's mobile phone

3. Securely sending the card information back to the card issuer (bank) whenever required for authorization during a transaction

4. Securely loading the merchant electronic terminal directly on merchant's mobile phone

5. Securely sending the terminal details to terminal issuer (acquiring bank) whenever the merchant initiates a sale transaction

Card issuers (banks) will use electronic cards on mobile phone provided there is a secure method of transmitting the card information to / from the phone. If the Track 2 data is sent in clear to / from the mobile phone there is a possibility of data being intercepted and misused. Therefore it is necessary to send the data in an encrypted format.

It is possible to use PKI (Public Key Infrastructure – RSA or ECC, Asymmetric Cryptography) and encrypt the Track 2 data. However, it takes a lot of time due to limited resources on the phone to decrypt data using asymmetric cryptography. It would therefore become impractical to use mobile phone as a payment device because of the time taken to do these encryption / decryption operation during a transaction. Symmetric encryption becomes the only method to do secure electronic transactions through mobile phone within a reasonable time.

However, if the same (one common key) symmetric key is used to send / receive encrypted data to / from every user at any stage (registration with ATOM, Request for a card / terminal, Sale transaction etc) then it is possible for someone to hack and retrieve the key. With this key the hacker can then read all encrypted data sent / received by the system to all customers. Therefore the symmetric key used for encryption / decryption should be different for every customer. This means the application installed by the customer on the mobile phone should contain a unique symmetric key for every customer.

ATOM application resides on the customer's / merchant's mobile phone and achieves the above in following steps.

1. On starting the application it generates a public key and private key pair for the customer / merchant using Asymmetric Cryptography - ECC (Elliptic Curve Cryptography 192 bit).

2. The private key is stored in the mobile phone.

3. The public key of the customer / merchant is sent to ATOM system for registration over sms / gprs / ussd.

4. ATOM registers the customer / merchant on its systems and generates a symmetric key for the customer / merchant, which will be used for decrypting any data sent from ATOM system to the customer / merchant mobile phone.

5. A copy of customer / merchant symmetric key is encrypted using the customer / merchant public key sent to ATOM during registration.

6. The encrypted symmetric key is then sent to the customer / merchant's mobile phone over sms / gprs / ussd.

7. Even if an intruder intercepts the data between ATOM's system and customer / merchant's mobile phone they cannot retrieve the customer / merchant's symmetric key.

8. ATOM application residing on the customer / merchant's mobile phone receives this encrypted message and retrieves the symmetric key using the private key, which was stored in the mobile phone.

9. The symmetric key (CCMK) is then stored in the mobile phone.

This way every customer / merchant gets a unique symmetric key which will be used for encrypting / decrypting the data while sending / receiving.

After a customer is registered with ATOM and has received the symmetric key, the customer can request an electronic card from Card Issuer (bank) directly from the mobile phone application.

This request is received by ATOM and sent to the appropriate Bank. The Bank does the necessary processing before issuing a card to the customer and once the bank decides to issue a card to the customer it generates a Track 2 file. This Track 2 information is sent to ATOM for loading the customer mobile.

Once the Track 2 information is sent to ATOM by the bank for loading it in the phone ATOM encrypts using a customer specific symmetric key (CAMK, generated using the parameters defined by the bank). The encrypted Track 2 data and CAMK is then encrypted using the CCMK (already stored on customer's mobile) and sent to the customer mobile phone. The application in the phone receives the data and stores encrypted Track 2 and CAMK after decrypting it using the CCMK already sent.

This way ATOM securely loads an electronic card on the customer's mobile phone. A similar process is followed for loading an electronic terminal on the merchant's mobile phone.

Whenever there is a request received by the application on customer's phone to authorize the customer the encrypted Track 2 data (stored on the mobile phone) is sent back by the application to the card issuer encrypted using a session key derived from CAMK. The issuer has a copy of CAMK and can therefore successfully decrypt and compare the data received from the customer's mobile phone. This way the card issuer can securely receive the data from the customer mobile phone during any transaction authorization.

ATOM has created a unique process for securely loading the electronic card and terminal on the mobile phone. The application architecture provides maximum data security while transmitting information to / fro from the mobile phone. The electronic card / terminal can be requested by the customer / merchant directly from the mobile phone.

## Security

One of the core services of the any transaction platform is to provide maximum end-to-end transaction security. ATOM platform uses PKI based Asymmetric cryptography (used only in key exchange) and symmetric key based cryptography (for data encryption and MAC) to secure the mobile transactions.

ATOM generates its own master key for deriving merchant/customer specific master keys for data encryption and generating Message Authentication Key (MAC) using ICCID. Every merchant card and the customer card are loaded with the derived keys unique to the customer or the merchant. Encryption using session key, which is derived from the card specific master keys will maximize overall data security shall further protect all the transactions.

The issuer will generate their own Issuer Master Key for deriving customer specific and card specific encryption key. This key is used for deriving session key for encrypting the payment data transferred from the customer mobile to ATOM platform.

The advantage of using session key is that for every session new key is derived and the derived session key is used for encrypting the data. This enables the ATOM platform to be most securing payment platform.

Typically the critical messages are secured as follows.

The data elements are concatenated together to form a data packet and are encrypted with the derived session key (Key unique per session) and the header for the data is prepared. The Header and the encrypted data packet are concatenated together and Message Authentication Code is calculated using the derived MAC session key (Key unique per session). The final payload will have MAC, HEADER and the ENCRYPTED DATA.

The security of Atom Transaction Platform can be broadly categorized under

A. Transaction Security

B. Operational Security

## A. Transaction Security

ATP being a financial platform, security is of prime importance. Every financial and non – financial message to and from Customer and Mobile terminals to Atom Transaction Platform and vice versa is encrypted using well-defined security algorithms like DES3 and Elliptic Curve.

Most cryptographic algorithms works on blocks of data obfuscating it with cipher text derived using a key. Similar is the case with Atom.

The cryptographic keys that are used as part of the Atom Transaction Platform are mentioned below.

### I. Platform Specific Keys (Master Keys)

### i. ATOM Master Key (ZAMK)

ATOM Master key is the ATOM proprietary master key used for creating card specific master keys.

| **Key Type** | **Key Length** |
|---|---|
| 3 DES Key | 16 Bytes |

**Key Ownership: ATOM**
**Key Custodian: ATOM**

### ii. Master Message Authentication Key (ZMAK)

Master Message Authentication key (ZMAK) shall be generated by ATOM using the Key generation tool of the HSM and stored in the HSM, which is later used by the ATOM personalization system to derive and securely transfer the ICC Message Authentication Key (CMAK/MMAK) to the customer and Merchant mobile.

| Key Length | Key Type |
|---|---|
| 16 Bytes | 3 DES Key |

**Key Ownership: ATOM**

**Key Custodian: ATOM**

i. **Master Loyalty Master Key (ZLMK)**

Loyalty Master Key (ZLMK) shall be generated by ATOM using the Key generation tool of the HSM and stored in the HSM, which is later used by the ATOM personalization system to derive and securely transfer the customer specific ICC Loyalty Master Key (CLMK) to the customer mobile.

| Key Type | Key Length |
|---|---|
| 3 DES Key | 16 Bytes |

**Key Ownership: ATOM**

**Key Custodian: ATOM**

**ATOM Elliptic Curve Key Encryption Key (ZEKK)**

ATOM Elliptic Curve Key Encryption Key (ZEKK) shall be generated by ATOM using Key generation tool of the HSM and stored inside the HSM, which is later used by the ATOM platform during key exchange of Customer/Merchant Card Master and the Message authentication key to the customer mobile.

| Key Type | Key Length |
|---|---|
| 3 DES Key | 16 Bytes |

**Note:** This key is not applicable for the application residing inside the SIM.

**Key Ownership: ATOM**

**Key Custodian: ATOM**

### v. Issuer Master Key (IMK)

Issuer Master Key (IMK) shall be generated by bank using the Key generation tool of the HSM and stored in the HSM, which is later used by the ATOM personalization system to derive and securely transfer the ICC Account Master Key (IAMK) to the customer SIM. Each issuing bank should generate their own IMK in the HSM for deriving Account Master Key for the cardholders.

| Key Type | Key Length |
|---|---|
| 3 DES Key | 16 Bytes |

**Key Ownership: Issuer Bank**
**Key Custodian: ATOM**

### vi. Terminal Master Key (TMK)

This is terminal specific key for each terminal, which is loaded by the Acquiring bank. This key is used to decrypt the Terminal PIN Key (TPK) / Terminal Authentication Key, the keys sent by the acquiring bank (TPK/TAK is encrypted with Terminal Master Key by the acquiring bank and transferred to the terminal), which is used to encrypt the PIN/ generate MAC for the data flowing from the terminal to acquirer.

| Key Type | Key Length |
|---|---|
| 3 DES Key | 16 Bytes |

**Key Ownership: Acquirer Bank**
**Key Custodian: ATOM**

### vii. Terminal PIN Key (TPK)

Terminal PIN Key (TPK) is a DES (or Triple-DES) data-encrypting key, which is used to encrypt Pins for transmission, within a local network, between the terminal and the terminal data acquirer. Every terminal will have unique TPK

| Key Type | Key Length |
|---|---|
| 3 DES Key | 16 Bytes |

**Key Ownership: Acquirer & ATOM**

**Key Custodian: ATOM**

### viii. Terminal Authentication Key (TAK)

Terminal Authentication Key (TAK) is a data-encrypting key, which is used to generate and verify Message Authentication Code (MAC) when data is transmitted, within a local network, between a terminal and the terminal data acquirer. For transmitting, a TAK is encrypted under a TMK. Every terminal will have unique TAK.

| Key Type | Key Length |
|---|---|
| 3 DES Key | 16 Bytes |

**Key Ownership: Acquirer & ATOM**

**Key Custodian: ATOM**

## II. Customer Key's

The customer terminal is the storehouse of financial data (TRACK 2) pertaining to the customer in digital format. This data being confidential needs to be protected against theft, cloning and any other misuse that might occur. So the data in its static form as well as when they are transferred through any other media are encrypted using proper ciphering algorithms. Given below are the keys that are used to protect the data.

### i. Customer Card Master Key (CCMK)

Customer Card Master Key (CCMK) is derived from ZAMK and ICCID. The derived CCMK is sent to customer mobile using OTA with OTA encryption.

| **Key Type** | **Key Length** |
|---|---|
| 3 DES Key | 16 Bytes |
| | |

CCMK is used to derive Session Key to encrypt the data flowing from Customer Mobile to ATOM Platform and vice versa.

### ii. Customer Message Authentication Key (CMAK)

Customer Message Authentication key (CMAK) shall be generated by ATOM using the ZMAK and ICCID, which is later used by the ATOM application residing in the customer mobile to derive Message Authentication Code (MAC) session key to create Message Authentication Code for the data flowing from Customer mobile to ATOM platform and vice versa.

| **Key Type** | **Key Length** |
|---|---|
| 3 DES Key | 16 Bytes |

### iii. Customer Loyalty Master Key (CLMK)

Customer Loyalty Master Key (CLMK) shall be generated by ATOM using the ZLMK and ICCID, which is later used by the ATOM application residing in the customer mobile to create session key to generate cryptogram for payment through ATOM loyalty points

| **Key Type** | **Key Length** |
|---|---|
| 3 DES Key | 16 Bytes |

### iv. Customer Account Master Key (CAMK)

This is account specific key and CAMK is created for every card stored inside the customer mobile (e.g. If the customer has got 3 card details stored inside the mobile, then 3 unique CAMK is derived for these cards). CAMK derivation takes as input the IMK, Primary Account Number (PAN) and the PAN sequence number (PSN).

| Key Type | Key Length |
|---|---|
| 3 DES Key | 16 Bytes |

CAMK is used to generate Application.Cryptograms (ARQC/TC/AAC) using its derived key.

### v. Customer Elliptic Curve Key (CECK)

Customer Elliptic Curve Key (CECK) shall be generated by the application loaded into the customer mobile (Application developed in J2ME / Symbian) during Customer registering with ATOM. This key is used for loading the derived Customer Card Master key (CCMK) and the Customer Message Authentication Key (CMAK) to the application residing in the mobile.

| Key Type | Size |
|---|---|
| 1. Elliptic Curve Domain Parameters over Fp.<br>2. Hash value generated using the named curve secp192k1 (Koblitz) | 24 Bytes |

## II. Merchant Key's

### i. Merchant Card Master Key (MCMK)

Merchant Card Master Key (MCMK) is derived from ZAMK and ICCID. The derived MCMK is sent to merchant mobile using OTA with OTA encryption.

| Key Type | Key Length |
|---|---|
| 3 DES Key | 16 Bytes |

The Merchant Card Master Key (MCMK) is used only for deriving session keys and never for data encryption.

ii. **Merchant Message Authentication Key (MMAK)**

Merchant Message Authentication key (MMAK) shall be generated by ATOM using the ZMAK and ICCID, which is later used by the ATOM application residing in the merchant mobile to derive Message Authentication Code (MAC) session key to create Message Authentication Code for the data flowing from Merchant mobile to ATOM platform and vice versa.

| **Key Type** | **Key Length** |
|---|---|
| 3 DES Key | 16 Bytes |

ii. **Merchant Elliptic Curve Key (MECK)**

Merchant Elliptic Curve Key (MECK) shall be generated by the application loaded into the merchant mobile (Application developed in J2ME / Symbian) during Merchant registering with ATOM. This key is used for loading the derived Merchant Card Master key (MCMK) and the Merchant Message Authentication Key (MMAK) to the application residing in the mobile.

| **Key Type** | **Size** |
|---|---|
| Elliptic Curve Domain Parameters over Fp.<br>Hash value generated using the named curve secp192k1 (Koblitz) | 24 Bytes |

B. **Process / Operational Security**

I. **PIN based Security**

i. **Encryption & Decryption of PIN**

The clear pin entered by the customer is encrypted using the session key generated using a random number and the Card Account Master Key (CAMK) of the customer. Once the encrypted clear pin reaches the ATP switch, the encrypted PIN and the Random number are sent to the switch's HSM where the clear PIN is decrypted using the session key generated by the HSM using the random number and is re-encrypted using the Terminal Pin Key (TPK) of the Acquirer.

### ii. PIN Translation

In the case where the transaction is an OFF-US transaction the customer Pin has to be authenticated by the Issuer. In such a case the Pin entered by the atom customer, which is, encrypted using the session key generated under the Customer Card Master Key has to be re-encrypted under the Terminal PIN key of the Acquirer to be sent to the Acquirer. This process is called Pin translation. The Switch HSM of Atom does the necessary pin translation.

### iii. PIN Storage

Pins are never stored at ATOM databases. Instead PIN offsets are generated for the clear pin, which are mapped to mobile numbers. The Switch HSM calculates the natural pin from the clear pin and the pin offset and returns a status flag depending on the pin validation result.

So at no point of time is the clear pin available to ATOM.

### iv. PIN Selection

During the card load process for the customer, as explained as part of ATP- Process, the Issuer performs the due diligence on the customer before issuing him a credit or a debit card. Once this is complete the Issuer authorizes the issuance of an electronic card though the ATOM Transaction Platform. Once the card is loaded on to the customer's terminal he is asked to enter a 4-digit pin of his choice. This pin is encrypted using the Customer Account Master Key (CAMK), which is loaded during the card load response.

This clear pin is sent to the Issuer using an ISO8583 Change pin message.

**Financial Transactions**

ATOM platform supports the following financial transactions:

1) Sale
2) Void
3) Refund

**Sale Transaction**

Sale refers to a transaction type that approves a transaction and settles it at the next settlement period.
In Atom platform, the merchant is expected to initiate the sale transaction.

Fig_11

Step 1:

The Merchant initiates the sale transaction by choosing the terminal from the list of personalized terminals (Merchant shall have more than one terminal loaded into the same mobile), enters the customer ATOM ID or customer Mobile number and enters the amount in the ATOM merchant application and sends it to the ATOM platform. The payment request is encrypted and sent to ATOM platform.

Step 2:

ATOM platform verifies the decrypted payment request and validates the merchant. ATOM Platform then forwards the request to customer mobile.. The data during transmission is encrypted.

Step 3:

Customer receives the merchant payment request and the application loaded into the customer mobile automatically validates the decrypted payload and decrypts the data.

The customer enters TIP amount (if any) and chooses the card for making payment from the list of loaded cards. The customer also enters the card PIN (if any) for the chosen card. The payment confirmation is then encrypted and sent to ATOM platform.

Step 4:

ATOM platform decrypts the customer response and validates the Cryptogram, decrypts the payload and send it to Virtual POS to process the payment by sending the Payment authorization request to acquirer host. The Virtual POS simulates the actual hardware POS and the message format will be similar to the actual POS message format (ISO 8583). To the acquirer host the data will look like as it is from the actual POS. So there is no need for change in any of the module in the acquirer side to accept ATOM platform request.

Step 5:

The acquirer host on receiving the payment authorization validates the merchant and sends the authorization request to the issuer bank. The Issuer bank then send the authorization response back to the acquirer host with the retrieval reference number which is then forwarded to the Virtual POS in the ATOM platform. The connectivity between the ATOM platform and the acquiring host, and the connectivity between the acquirer and the issuer is outside the scope of this document.

Step 6:

ATOM platform generates Authorization Response Cryptogram and sends the confirmation or the failure receipt based on the Authorization response Code to the merchant.

Step 7:

ATOM platform generates Authorization Response Cryptogram, calculates the ATOM loyalty points awarded and sends the confirmation or the failure receipt based on the Authorization response Code to the customer.

## Void Transaction

Void transaction refers to reversal of an approved transaction, one that has been authorized but not settled. Settled transactions require processing of a credit in order to be reversed.

In ATOM platform merchant initiates the void transaction.

Fig_12

Step 1:

The Merchant selects the void menu and chooses the Terminal from the list (if more than one terminal is loaded into the merchant mobile) and enters the Retrieval Reference Number (RRN). The data is encrypted and transferred to ATOM platform.

Step 2:

ATOM Platform decrypts the void request and searches the Retrieval Reference Number in the database for validity. On successful search, ATOM platform prepares the void request data through Virtual POS and send it to the respective acquiring host for processing.

Step 3:

The acquirer then validates the merchant and forwards the request to Issuer for processing. The Issuer on performing the operation sends the response back to the acquirer and routed to the Virtual POS of the ATOM platform.

Step 4:

ATOM platform prepares the success / failure receipt based on the reply from the acquirer. The receipt is encrypted and sent to the merchant mobile.

Step 5:

ATOM platform prepares the success / failure receipt based on the reply from the acquirer. The receipt is encrypted based and sent to the customer mobile.

**Refund Transaction**

Refund is a transaction type that transfers funds to the cardholder's account, rather than from the account. This transaction type is typically used to refund a customer's money for an order that was previously settled, e.g., returns or overcharges.

Fig_13

Step 1:

The Merchant selects the refund menu and chooses the Terminal (Terminal on which the earlier sale operation is performed) from the list (if more than one terminal is loaded into the merchant mobile), enters the Retrieval Reference Number (RRN) and the refund amount. The data is encrypted and transferred to ATOM platform.

Step 2:

ATOM Platform decrypts the refund request and searches the Retrieval Reference Number in the database for validity. On successful search, ATOM platform prepares the refund request message format through Virtual POS and send it to the respective acquiring host for processing.

Step 3:

The acquirer then validates the merchant and forwards the request to Issuer for processing. The Issuer on performing the operation sends the response back to the acquirer and routed to the Virtual POS of the ATOM platform.

Step 4:

ATOM platform prepares the success / failure receipt based on the reply from the acquirer. The receipt is encrypted and sent to the merchant mobile.

Step 5:

ATOM platform prepares the success / failure receipt based on the reply from the acquirer. The receipt is encrypted and sent to the customer mobile

We claim :-

1) A system and method for implementing secure transaction through mobile communicating device comprising of the following steps which entail requesting of an electronic card / terminal from the mobile phone; securely loading the customer's electronic card directly on customer's mobile phone; securely sending the card information back to the card issuer (bank) whenever required for authorization during a transaction; securely loading the merchant electronic terminal directly on the merchant's mobile phone; and securely sending the terminal details to terminal issuer (acquiring bank) whenever the merchant initiates a sale transaction.

2) A system and method for implementing secure transaction through mobile communicating device as mentioned in claim 1 above comprising of :

a) mobile communicating device capable of being loaded with java 2 micro edition (j2me) based merchant application at the merchant side,

b) a mobile communicating device capable of being loaded with java 2 micro edition (j2me) based customer application at the customer side,

c) a robust and secure transaction platform capable of providing rich set of merchant and customer services and connecting to both the said mobile devices and other stakeholders directly or indirectly to enable mobile transactions; the said platform comprises means for registering the merchant and the customer, means for validating the users, means for using PKI based asymmetric cryptography(ECC) to distribute symmetric key used for secure data transfer; ATOM platform uses PKI based Asymmetric cryptography (used only in key exchange) and symmetric key based cryptography (for data encryption and MAC) to secure the mobile transactions.

ATOM application resides on the customer's / merchant's mobile phone and achieves the above in following steps.

(i) On starting the application it generates a public key and private key pair for the customer / merchant using Asymmetric Cryptography - ECC (Elliptic Curve Cryptography 192 bit).

(ii) The private key is stored in the mobile phone.

(iii) The public key of the customer / merchant is sent to ATOM system for registration over sms / gprs / ussd.

(iv) ATOM registers the customer / merchant on its systems and generates a symmetric key for the customer / merchant, which will be used for decrypting any data sent from ATOM system to the customer / merchant mobile phone.

(v) A copy of customer / merchant symmetric key is encrypted using the customer / merchant public key sent to ATOM during registration.

(vi) The encrypted symmetric key is then sent to the customer / merchant's mobile phone over sms / gprs / ussd.

(vii) Even if an intruder intercepts the data between ATOM's system and customer / merchant's mobile phone they cannot retrieve the customer / merchant's symmetric key.

(viii) ATOM application residing on the customer / merchant's mobile phone receives this encrypted message and retrieves the symmetric key using the private key, which was stored in the mobile phone.

(ix) The symmetric key (CCMK) is then stored in the mobile phone.

This way every customer / merchant gets a unique symmetric key which will be used for encrypting / decrypting the data while sending / receiving.

3) An invention as claimed in claims 1 and 2 above which enables secure transactions via mobile phones through the use of a transaction platform which application has two parts – Application on the mobile phone (Front-end Application) and ATOM Transaction Platform (Backend).

The merchant initiates the transaction from his mobile phone and enters the customer id and amount, which request is received by ATOM Transaction Platform (Backend) and sent to customer's mobile phone for payment after which the customer selects the appropriate card stored on the mobile and sends the card details for authorization which details are then received by ATOM Transaction Platform (Backend) from the customer and it is then sent to the Acquiring Bank for authorization from Issuing Bank. On receiving the confirmation from Acquiring Bank, Transaction Platform (Backend) sends receipts to Customer and Merchant.

4) An invention as claimed in claim 2 above wherein use of the ATOM platform by the said means maintains various master keys to generate customer/merchant specific keys.

5) An invention as claimed in claim 2 above wherein use of the ATOM platform by the said means also uses session key (valid only for that session) to maximize overall data security,

6) A system for conducting financial transaction using mobile communicating devices as claimed in claims 1 and 2 above wherein the transaction platform is also enabled with loyalty engine to facilitate customers to avail/redeem loyalty points on sale operation; loyalty merchant can participate in the program and provide loyalty points based on the sale value; the loyalty point calculation is individually configurable for the merchants and similarly the customer is awarded with the loyalty points on any

purchase (if the merchant is participated in atom loyalty) and the points can be accumulated over multiple purchases and later, the customer can use the accumulated loyalty points to pay for any of the purchase.

7) A method of transaction through mobile communicating device comprising the steps of registering the merchant and the customer and loading electronic card / terminal in to the customer / merchant mobile which includes merchant pre-registering with the Platform for availing the service of financial and non financial transaction, wherein a generic application software is loaded to the merchant's mobile without any merchant specific details and the applet get personalized for a particular merchant, with Merchant specific information, a merchant registration request logic is built into the Merchant application as part of the standard functionality,

Sending the registration request data in a single SMS to the platform using the merchant applet,

Receiving registration request from the interested merchant by the Platform and performing necessary validation in the system for duplicate request, generating a unique Merchant ID and merchant specific security keys for loading into the merchant mobile,

merchant registering with the acquiring bank, wherein the merchant sends the terminal request along with the acquiring bank name to the platform by SMS utilizing the merchant-acquirer registration request logic, which is built into the Merchant application as part of the standard functionality, which is then forward to the respective Acquiring banks along with the merchant contact details for further processing and Acquiring bank registering the merchant in their system,

Sending the merchant detail to the platform to subsequently load it on to the merchant,

Customer registering with the platform to perform payment transaction, where in utilizing the customer registration request logic which is built into the customer applet as part of the standard functionality, the customer sends a registration request to the platform via SMS/GPRS,

platform registering customer, where in on receiving registration request from the interested customer ,the platform performs necessary validation in the system to check for duplicate request and generates security Keys and registers the customer with ATOM loyalty scheme for availing loyalty points in the system and send the registration data in a single SMS to the customer mobile,

customer requesting for loading electronic card into the Mobile, where in Customer sends the card load request to the platform after registering with the platform to perform financial transactions, the platform receives the request from the customer and sends it to the appropriate issuing bank to process the customer request for card loading,

issuing bank loading the Electronic card load into the customer Mobile where in the Issuing bank after verifying the interested customer prepares card personalization data and transfers the electronic card data to the platform, the Issuing bank first registers with the platform and generates the required Master Key(s) into the HSM residing with the platform and the platform uses this key to encrypt the card data of the customer before loading it into the customer mobile,

Sending Confirmation of card loading back to Platform, where in the customer mobile on receiving the card load data responds with confirmation detail to the platform.

8) An invention which transacts a sale utilizing the mobile devices, this includes

Step 1: merchant choosing the terminal from the plurality of personalized terminals (merchant may have more than one terminal loaded into the same mobile) entering the customer ID or customer Mobile number and entering the amount in the merchant application and sending it to the platform, encrypting the payment request and sending it to the platform;

Step 2: platform verifying the decrypted payment request and validating the merchant then forwarding the request to customer mobile after encrypting;

Step 3: customer receiving the merchant payment request and the application loaded into the customer mobile automatically validating the decrypted payload and decrypting the data, the customer entering TIP amount (if any) and choosing the card for payment from the list of loaded cards, the customer also entering the PIN (if any) for the chosen card encrypting the payment confirmation and sending to the platform;

Step 4: the platform decrypting the customer response, validating the Cryptogram, decrypting the payload and sending it to Virtual POS to process the payment by sending the Payment authorization request to acquirer host, the Virtual POS simulating the actual hardware POS and the message format being similar to the actual POS message format (ISO 8583);

Step 5: the acquirer host validating the merchant on receiving the payment authorization request and sending the authorization request to the issuer bank, the Issuer bank then sending the authorization response back to the acquirer host with the retrieval reference number, which is then forwarded to the Virtual POS in the platform;

Step 6: the platform generating Authorization Response Cryptogram and sending the confirmation or the failure receipt based on the Authorization response Code to the merchant;

Step 7: the platform generating Authorization Response Cryptogram, calculating the loyalty points awarded and sending the confirmation or the failure receipt based on the Authorization response Code to the customer.

9) An invention which enables a financial transaction to be securely conducted via mobile phone and through the use of an ATOM transaction Platform which operates on two modes of Security viz. Transaction Security and Operational Security, by the use of Keys of the following kinds :

Master Key : is the ATOM proprietary master key used for creating card specific master keys;

Master Message Authentication Key : which is used to derive and securely transfer the ICC Message Authentication Key to the customer and merchant mobile;

Master Loyalty Master Key : which is used to derive a securely transfer the customer specific ICC Loyalty Master Key to the customer mobile;

ATOM Elliptic Curve Key Encryption Key :is used by the ATOM Platform during key exchange of Customer/Merchant Card Master and the message authentication key to the customer mobile;

Issuer Master Key : which is used to derive and securely transfer the ICC Account Master Key (IAMK) to the customer SIM;

Terminal Master Key : is used to decrypt the Terminal PIN Key (TPK)/Terminal Authentication Key which would encrypt the PIN/ generate MAC for the data flowing fron the terminal to acquirer;

Terminal PIN Key : is a data encrypting key which is used to encrypt pins for transmission between the terminal and the terminal data acquirer;

Terminal Authentication Key : is a data encrypting key which is used to generate and verify Message Authentication Code when data is transmitted between the terminal and the terminal data acquirer;

Customer Card Master Key : is sent to customer mobile using OTA with OTA encryption;

Customer Message Authentication Key : is used to derive Message Authentication Code for the data flowing from customer mobile to ATOM Platform and vice versa;

Customer Loyalty Master Key : is used to create session key to generate cryptogram for payment through ATOM loyalty points;

Customer Account Master Key : is an account specific key and is used to generate Application Cryptograms using its derived key;

Customer Elliptic Curve Key : is used for loading the derived Customer Master Key and the Customer Message Authentication Key to the application residing in the mobile;

Merchant Card Master Key : is used only for deriving session keys and never for data encryption;

Merchant Message Authentication Key : is used by the ATOM application residing in the merchant mobile to derive Message Authentication Code session key to create Message Authentication Code for the data flowing from Merchant mobile to ATOM Platform and vice versa;

Merchant Elliptic Curve Key : is used for loading the derived Merchant Card Master Key to the application residing in the mobile.

10) A method of doing a void transaction through mobile communicating device, when the merchant and the customer are registered with the platform and the acquiring bank as claimed in claim 1, comprising the steps of :

STEP 1:

The Merchant selecting the VOID menu and choosing the terminal from a plurality of terminals (if more than one terminal is loaded into the merchant mobile) and entering the Retrieval Reference Number (RRN),
encrypting the data and transferring it to the platform;

STEP 2:

the platform decrypting the VOID request and searching the Retrieval Reference Number in the database for validity, On successful search, platform preparing the VOID request data through Virtual POS and sending it to the respective acquiring host for processing;

STEP 3:

The acquirer then validating the merchant and forwarding the request to Issuer for processing, the Issuer on performing the operation sending the response back to the acquirer and routing to the Virtual POS of the platform;

STEP 4:

the platform preparing the success / failure receipt based on the reply from the acquirer, encrypting the receipt and sending to the merchant mobile;

STEP 5:

preparing the success / failure receipt based on the reply from the acquirer, encrypting the receipt and sending to the customer mobile.

11) A method of doing a refund transaction through mobile communicating device, when the merchant and the customer are registered with the platform and the acquiring bank as claimed in claim 1, comprising the steps of :

STEP 1:

the Merchant selecting the REFUND menu and choosing the terminal (Terminal on which the earlier sale operation is performed) from a plurality of terminals (if more than one terminal is loaded into the merchant mobile), entering the Retrieval Reference Number (RRN) and the refund amount, encrypting the data and transferring to the platform;

STEP 2:

the Platform decrypting the REFUND request and searching the Retrieval Reference Number in the database for validity, On successful search, the platform preparing the REFUND request message format through Virtual POS and sending it to the respective acquiring host for processing;

STEP 3:

the acquirer then validating the merchant and forwarding the request to Issuer for processing, the Issuer sending the response back to the acquirer and routing to the Virtual POS of the ATOM platform;

STEP 4:

platform preparing the success / failure receipt based on the reply from the acquirer, encrypting the receipt and sending to the merchant mobile;

STEP 5:

platform preparing the success / failure receipt based on the reply from the acquirer, encrypting the receipt and sending to the customer mobile;

12) A method of conducting secure transaction through mobile communicating device as described substantially here in with reference to the figures of the accompanying drawings wherein a merchant first requests for its registration with an ATOM Platform which upon receiving such request performs necessary validation and generates an unique ATOM Merchant ID and merchant specific security keys and forwards the merchant request to the acquiring bank for registration which confirmation details are loaded into the merchant mobile.

13) A method of conducting secure transaction through mobile communicating device as described substantially herein with reference to the figures of the accompanying drawings wherein a customer can perform the payment transaction by

first requesting for its registration with the ATOM Platform which upon such receipt confirms registration of a customer with it by loading an electronic card into the customer's mobile phone issued by the issuing bank. This data is forwarded to the issuing bank which then prepares an electronic card personalization data and transfers the same to the ATOM Platform and in addition thereto generates the required Master Key into the HSM residing with ATOM which in turn uses this key to encrypt the card data of the customer before loading it on the customer mobile and the customer upon receiving the card load data respond with confirmation detail to ATOM Platform thus ensuring safe transaction thereof.

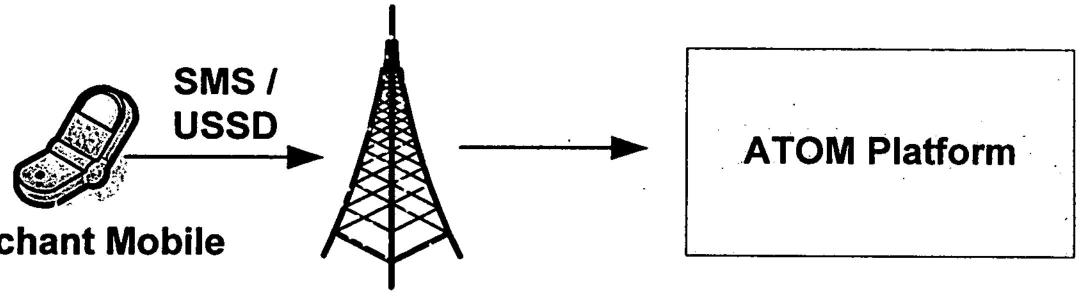


Fig 1: merchant requesting for re੍gistration with the Platform

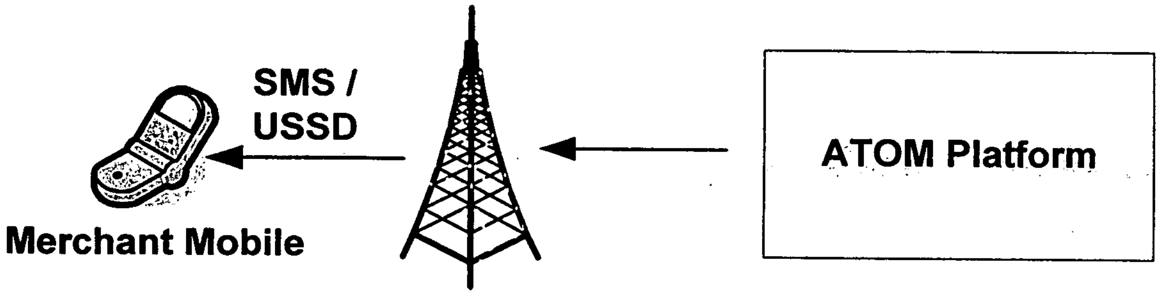


Fig 2: Platform Registering the Merchant

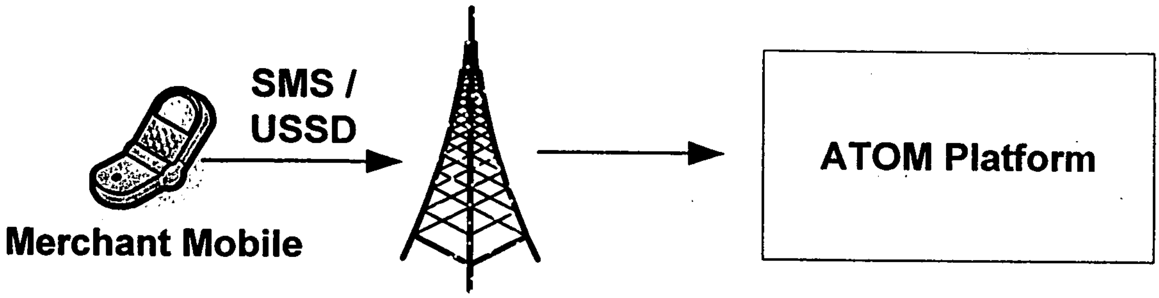


Fig 3: merchant confirming registration

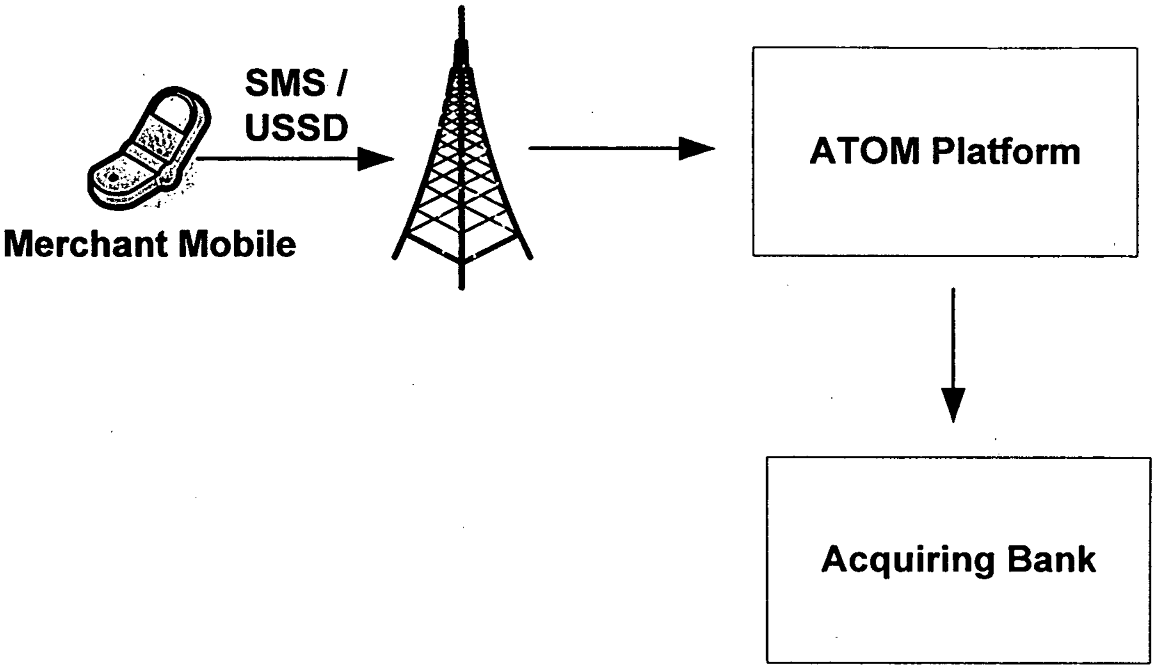


Fig 4: Merchant - Terminal Load Request

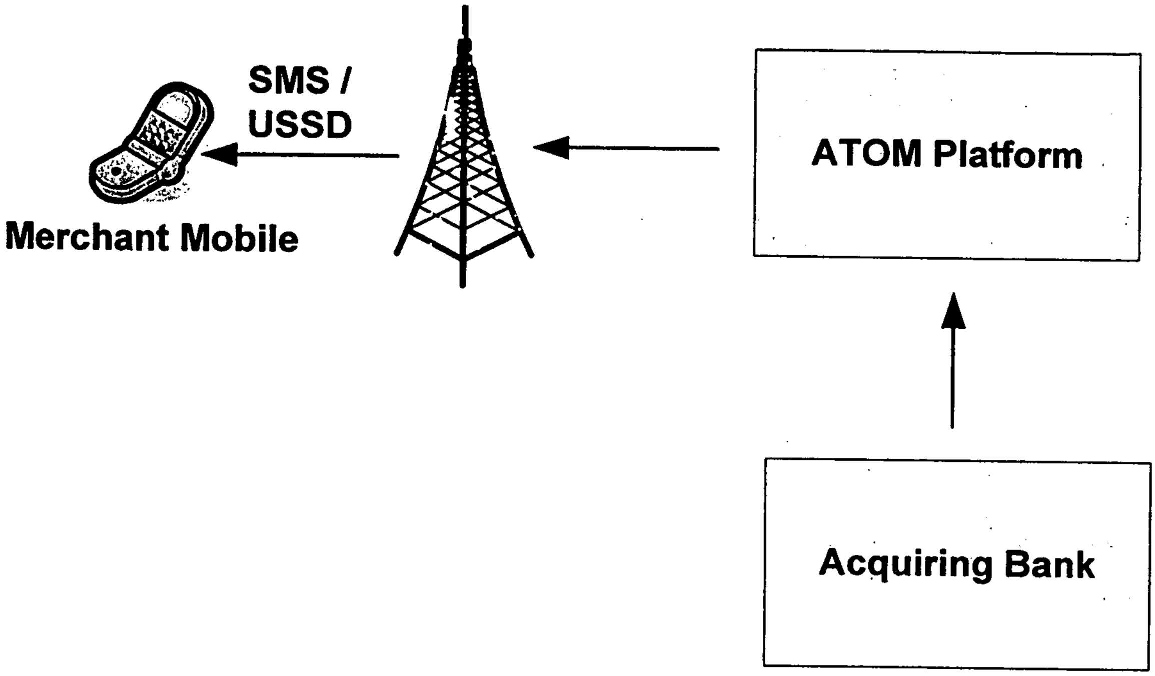


Fig 5: Merchant – Acquirer confirmation detail loading into the Merchant Mobile

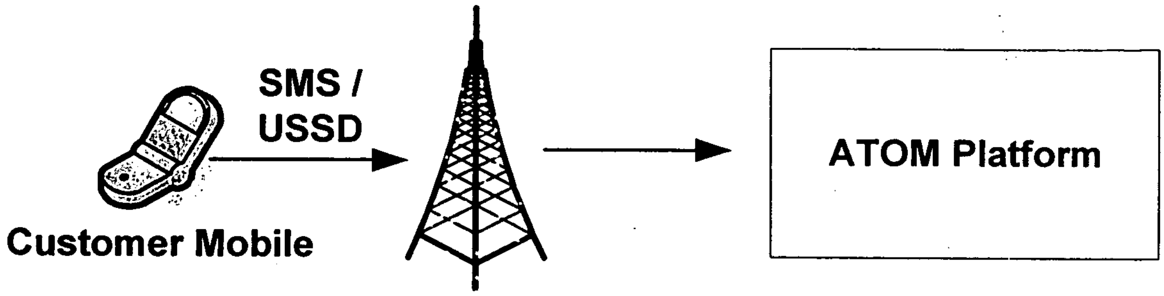


Fig 6: Customer requesting for registration with the Platform

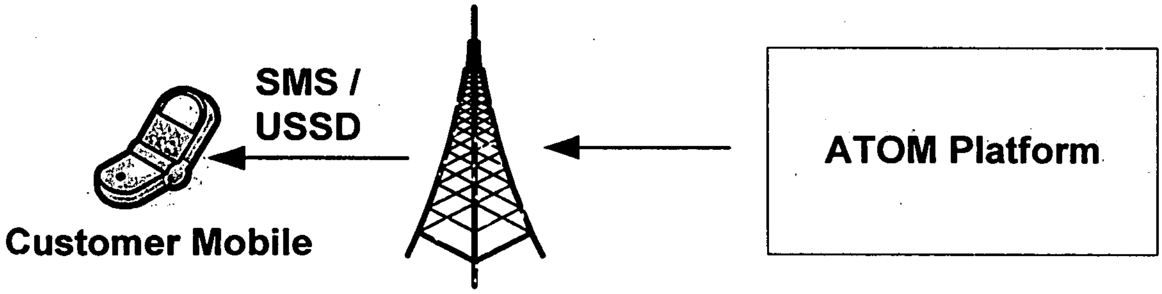


Fig 7: Platform Registering Customer

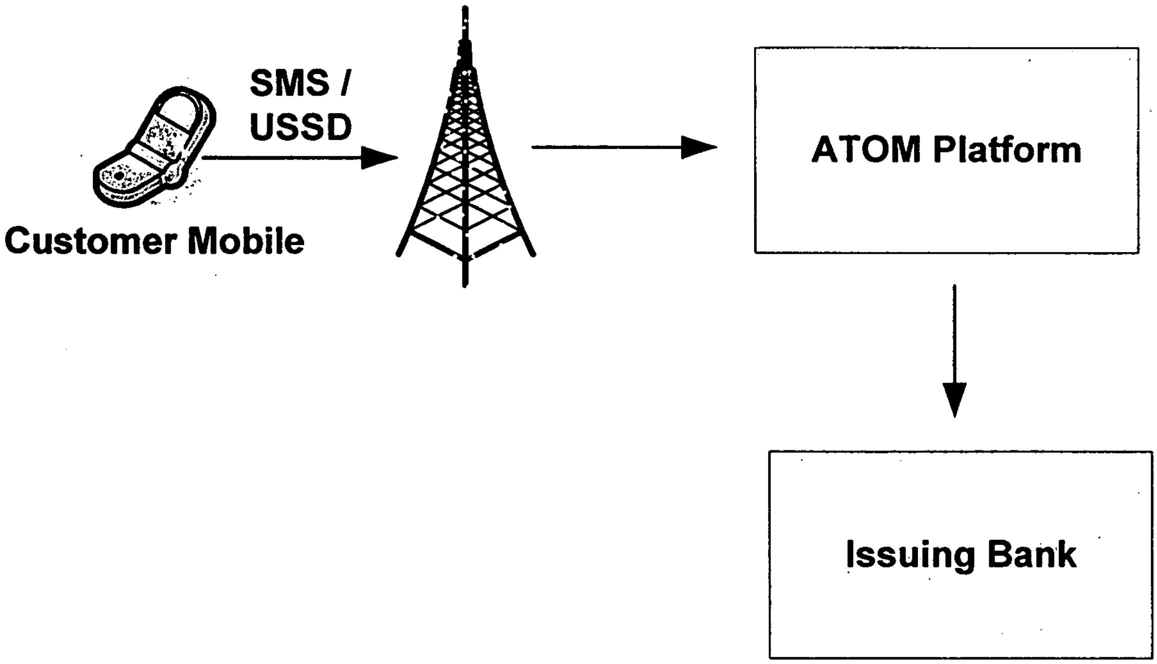


Fig 8: Electronic card Load request from customer Mobile

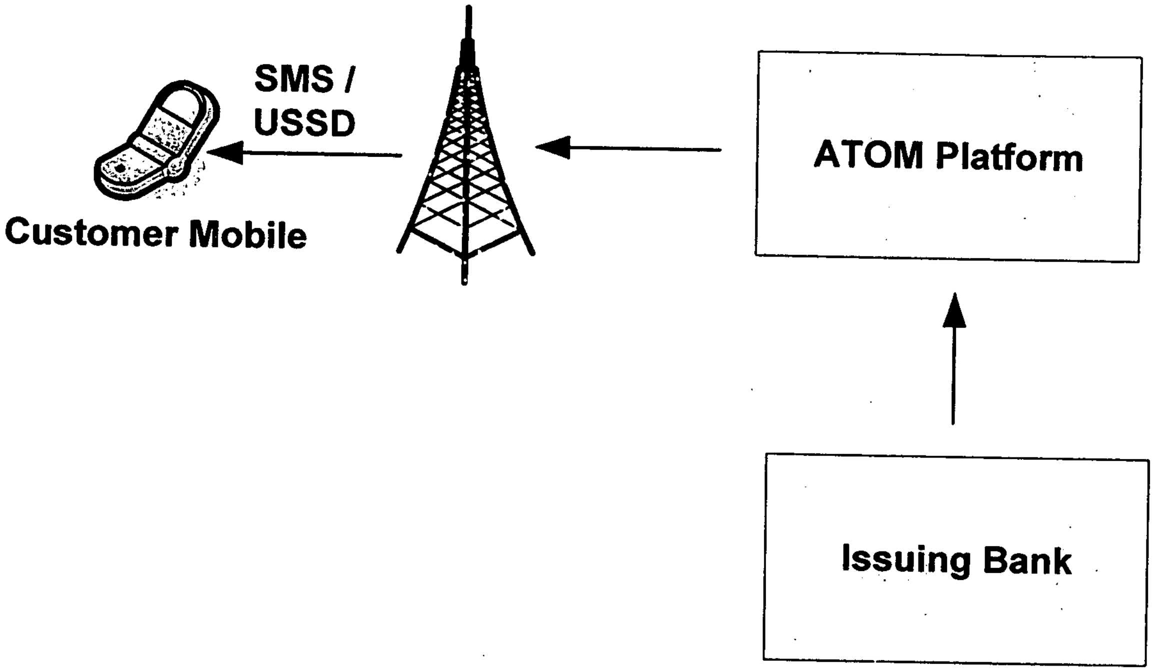


Fig 9: Electronic card loading into the customer Mobile

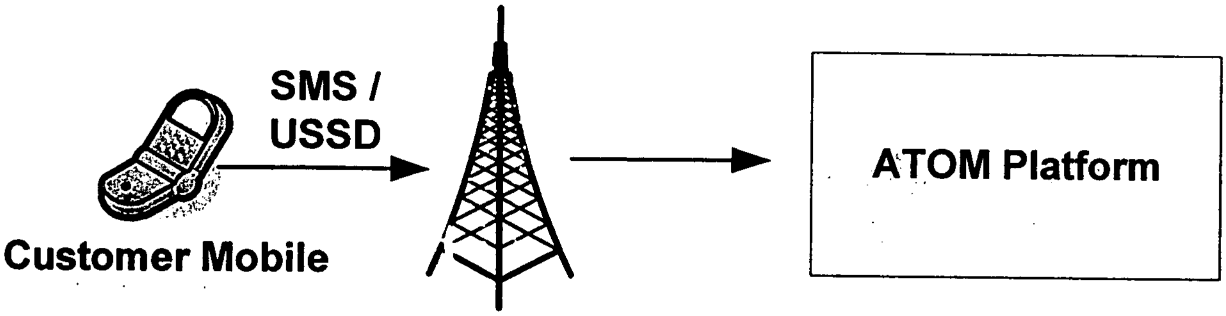


Fig 10: Electronic card load Confirmation sent back to the Platform

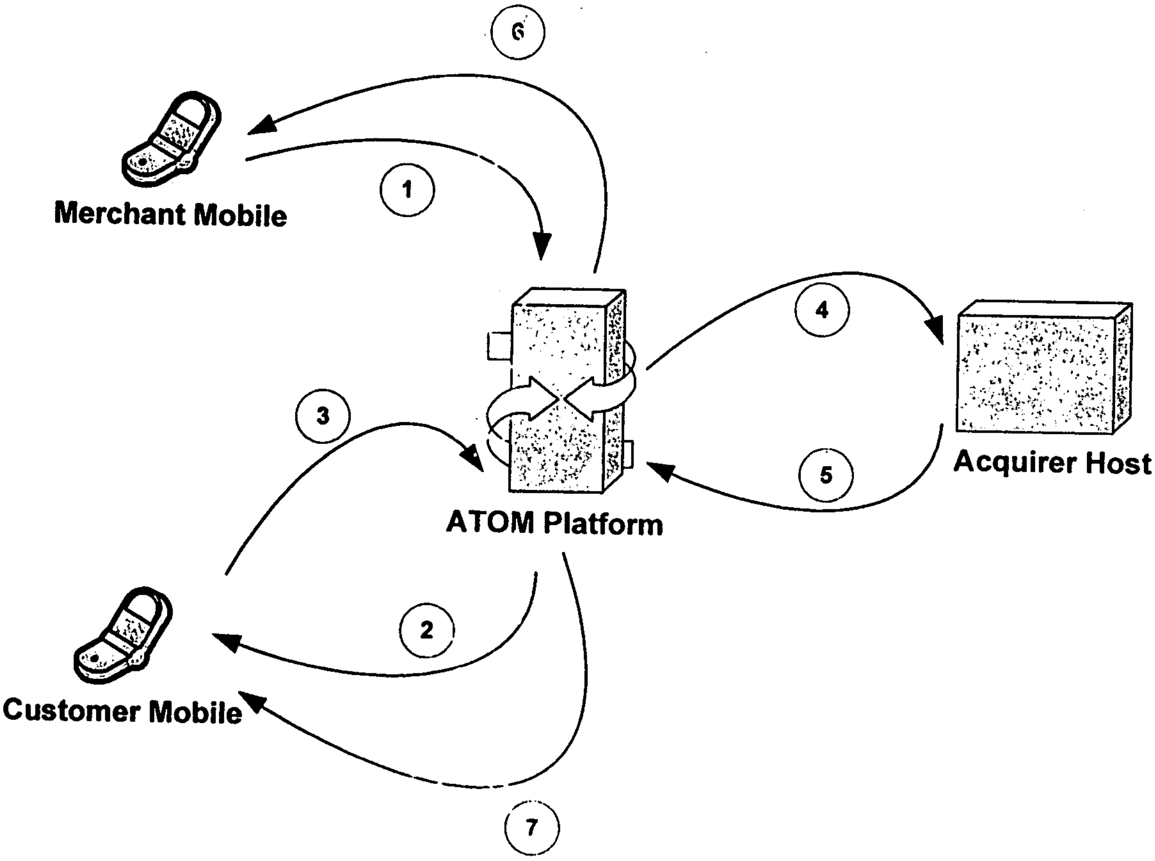


Fig 11: Sale Transaction - Remote

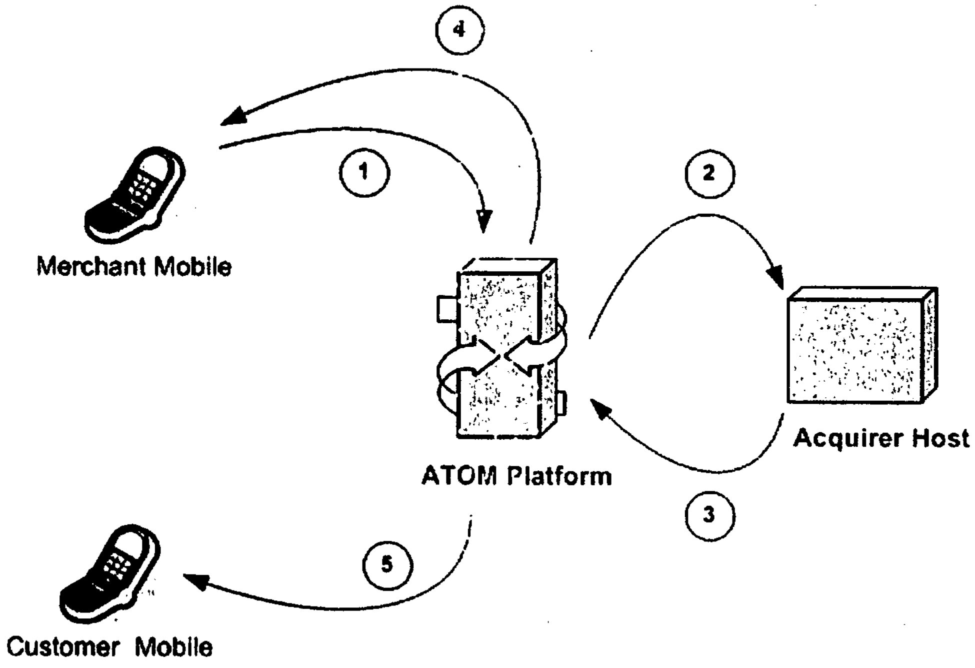


Fig 12: Void Transaction

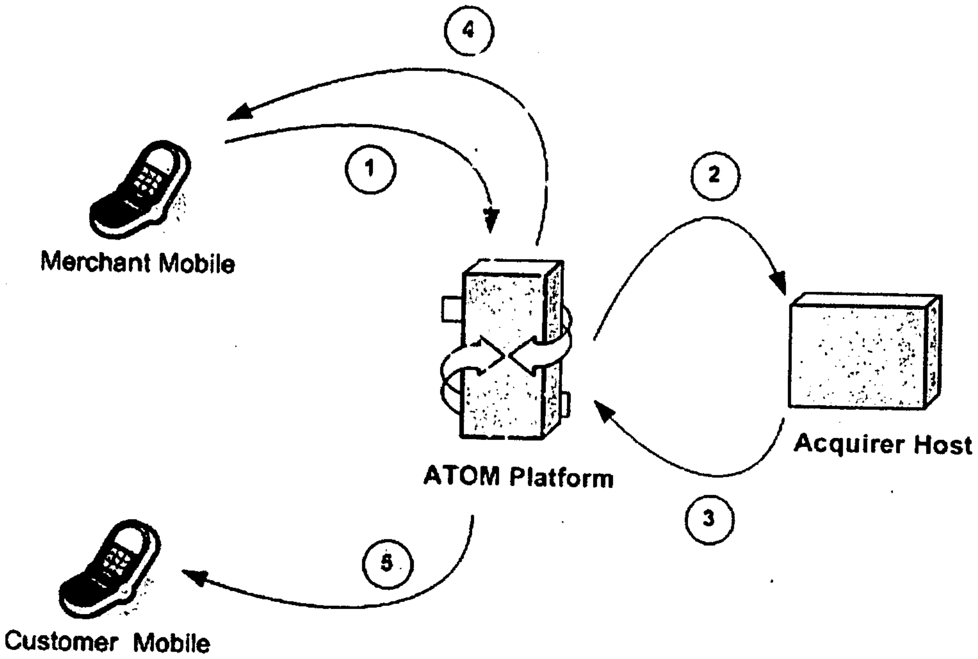


Fig 13: Refund Transaction