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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
22 September 2005 (22.09.2005)

PCT

(10) International Publication Number
WO 2005/086593 A2

(51) International Patent Classification: Not classified

(21) International Application Number:
PCT/IN2005/000038

(22) International Filing Date: 4 February 2005 (04.02.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
165/DEL/2004 5 February 2004 (05.02.2004) IN

(71) Applicant *(for all designated States except US)*: **A LITTLE WORLD PRIVATE LIMITED** [IN/IN]; 403, Alpha, Hiranandani Business Park, Powai, Mumbai 400 0076 (IN).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **GUPTA, Anurag** [IN/IN]; 403, Alpha, Hiranandani Business Park, Powai, Mumbai 400 0076 (IN). **PANDA, Lokanath** [IN/IN]; Flat No. : 103, Srinivasa Residency, 7th Cross, N. R. Colony, Bangalore 560 017 (IN).

(74) Agent: **VAIDYANATHAN, Alamelu**; 451, 2nd Cross, 3rd Block, 3rd Stage, Basaveshwaranagar, Bangalore 560 079 (IN).

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

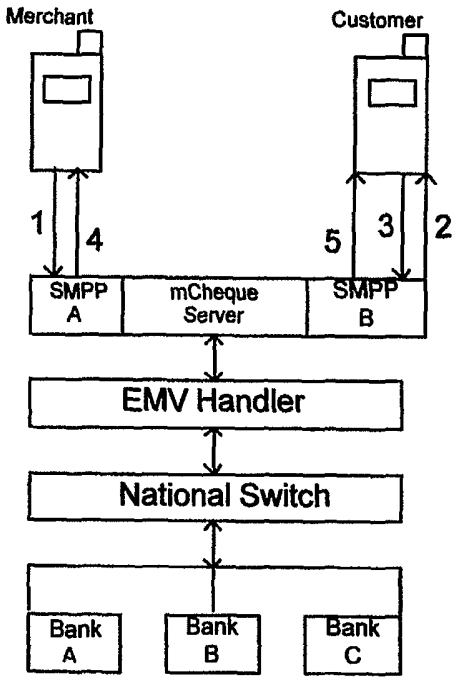
(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, 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 the identity of the inventor (Rule 4.17(i)) for the following designations AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK,*

[Continued on next page]

(54) Title: INTER-OPERABLE, MULTI-OPERATOR, MULTI-BANK, MULTI-MERCHANT MOBILE PAYMENT METHOD AND A SYSTEM THEREFOR



(57) Abstract: This invention relates to an inter-operable Multi-operator, Multi-bank, Multi-merchant Mobile Payment System. This invention makes the mobile phone a debit/credit instrument for payment as well as an instrument to carry out payment terminal functions. The debit/credit card(s) on the mobile phone could be used to carry out payment transactions with another mobile phone, a regular Point-of-Sale terminal, an ATM, a Vending Machine or Internet.

WO 2005/086593 A2

LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW, ARIPO patent (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)

— *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii)) for all designations*
— *of inventorship (Rule 4.17(iv)) for US only*

Published:
— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

AN INTER-OPERABLE MULTI-OPERATOR, MULTI-BANK, MULTI-MERCHANT MOBILE PAYMENT METHOD AND A SYSTEM THEREFOR.

This invention relates to an Inter-operable Multi-operator, Multi-bank, Multi-merchant Mobile Payment System. This invention makes the mobile phone, a debit/credit instrument for payment as well as an instrument to carry out payment terminal functions. The debit/credit card(s) on the mobile phone could be used to carry out payment transactions with another mobile phone, a regular Point-of-Sale terminal, an ATM, a Vending Machine or Internet.

Introduction:

The existing financial transaction systems involve use of physical currency, debit and credit cards based on Magnetic Stripe technology. The Magnetic Stripe debit/credit card based transactions are inherently prone to security violations given to the fact that Magnetic Stripes can be easily read and duplicated. Also, there are disadvantages in terms of physical damage to the Magnetic Stripe after some swipes on a physical merchant terminal. The existing smartcard based transaction systems are secure, but mandate use of an expensive Point-of-Sale Terminal to carry out a financial transaction, be it a stored value transaction or an online/offline debit/credit transaction.

The secure and more reliable alternative lies in use of a mobile phone, which offers computational capabilities and guarantees security with cryptographic support in the phone/SIM operating system.

Europay Mastercard Visa (EMV) and Common Electronic Purse Scheme (CEPS) standards provide means for development of interoperabe payment scheme. In this context A.Little.World is implementing a new interoperable payment brand in India and abroad known as mCheque. mCheque platform provides a secure all-purpose debit/credit payment system on mobile phones.

The proposed solution enables the consumer (hereby referred to as 'payer' or 'customer') to carry out financial transactions from his/her Mobile Phone with debit/credit cards configured on the Mobile Phone and helps the merchant (hereby referred to as 'payee' or 'merchant') to use a hosted Virtual Terminal service, while the mobile phone of the merchant is used as the payment terminal. However the payer can use the debit/credit card(s) configured on the Mobile Phone to engage in a payment transaction with the payee application on the regular Point-of-Sale Terminal, Vending Machine, Internet or ATM.

Large-scale use of mobile-to-mobile payment between customers and merchants - using any mobile phone as an EMV debit/credit payment instrument issued by a Bank, to pay any merchant who has another mobile phone. No additional terminal infrastructure apart from mobile phone is required by Bank or by merchants. No compromises made on transaction security.

Funds flow will be handled entirely through the banks, using proven EMV security with the added layer of mobile network security for secure communications. The EMV handler will provide an effective intermediary solution to the Bank without need for the Bank having to upgrade its back-end infrastructure to EMV.

Public Key Infrastructure (PKI) will be used for non-repudiation in specific application areas. Mobile Phones will have the capability of a universally usable digital ID (to be issued as an X.509 certificate by a Certification Authority) for digitally signing transactions for non-repudiation. RSA is the preferred standard for security implementation for PKI applications of mCheque.

The application download and personalization of the mobile phone can be done both over-the-counter (OTC) and over-the-air (OTA). The complete application functionality for the customer's payment card will be provided on the phone. The application functionality for the merchant's terminal will be provided at the back-end as a Virtual Terminal, with the phone used for confirmation of the transaction (transaction receipt).

The ready availability of communications network; the display screen; and the large memory on the phone to store and view transaction records helps enhance the Bank's product value for the customer and makes this the most user friendly and versatile payment instrument the customer will ever use. The mobile phone can be used both as a credit and debit cards at the same time multiple debit/credit accounts from different banks can be configured on the same mobile phone without any security compromise. A single PIN for all accounts will simplify banking and payment for the customer.

PRIOR ART:

There are known instances of various forms of payment mechanisms using mobile devices, such as Singapore Patent Publication No. 86428 using a payment center backend without use of real debit/credit card and involving a bank in the transaction.

US Patent No. 6,612,488 describes a method of payment using credit cards using a portable communication terminal such as a cellular phone. However, this method does not avoid the use of the credit card or debit card. The portable communication terminal is used to only identify the purchaser to avoid fraudulent use of the cards.

US Patent No. 6, 678, 664 issued to CheckFree Corporation suggests cashless transactions, e.g. purchases of goods and services without making cash payments at the time of purchase, by transmitting, preferably from a point of purchase, information identifying the purchaser of a product without identifying a payment account for the purchaser, the point of purchase being, for example, a register within a retail store or a server at an internet site.

Though the aforesaid US patent suggests the use of personal identification information such as purchaser's name, address and drivers license or passport number or any other identification code, this process of identification is little cumbersome and yet requires some document to be carried by the purchaser. Further, the transaction cannot be completed by using a wireless communication device and also it does not offer a virtual terminal to the seller. In other words, the seller is required to have a terminal, a scanner or other similar means to transmit the personal identification details to the bank or to the payment operator.

Objects of The Invention:

- The primary object of the present invention is to provide an inter-operable, multi-operator, multi-bank, multi-merchant, mobile payment method and system.

- In the proposed payment method/system, a regular mobile phone is used as a bank-account linked debit/credit payment instrument to pay any merchant with a regular mobile phone, without customisation of phone hardware. The merchant does not need a regular payment terminal. However, the merchant terminal can be a regular Point-of-Sale terminal, vending machine, Internet or ATM.

- Genuine 'card present' transactions using debit/credit cards configured on the mobile phone.

- EMV Handler solution enabling banks to participate in the secure debit/credit card based transactions without having to migrate to EMV.

The following is the scope of the mCheque payment method/system:

Use a regular mobile phone as an EMV-based payment instrument linked to a debit or credit account in a Bank, to pay any merchant who has a mobile phone or an on-line EMV capable terminal. The merchant does not need a regular payment terminal. EMV security is fully implemented for this product.

The ready availability of a communications network; the display screen on the mobile; and the large memory on the phone to store and view transaction records helps enhance the product value for the customer and makes this the most user friendly and versatile payment instrument the customer will ever use. The mobile phone can be used both as a credit and debit cards at the same time. Multiple debit/credit accounts from different banks can be configured on the same mobile phone without any security compromise. A single PIN for all accounts will simplify banking and payment for the customer.

In case of availability of a Subscriber Identification Chip module on the phone (SIM for GSM and R-UIM for CDMA), the application is developed without need to customize either the phone hardware or software. The only change is made to the SIM/R-UIM software through the use of the SIM Application Toolkit or a script using existing SIM/R-UIM browsing environment. In case of phones without having a Subscriber Identification Chip module, the application is developed on the phone. As a result, nearly the entire base of mobile phones can be used as cards and terminals without extra investment required in cards or terminals. The payment application for debit/credit card on payer's mobile phone and the merchant terminal on payee's mobile phone use security mechanisms prescribed by EMV.

The application download and personalization of the mobile phone will be done both over-the-counter (OTC) and over-the-air (OTA). The complete application functionality for the customer's payment card will be provided on the phone. The application functionality for the merchant's terminal will be provided at the back-end, with the phone or a connected PoS terminal being used for confirmation of the transaction (transaction receipt).

The EMV handler solution will be used to provide an effective intermediary solution to banks that have not yet upgraded their back-end infrastructure to EMV. This applies both to the debit/credit card issuance, transaction authorization and merchant acquiring systems of the bank.

The transactions will be cleared and settled domestically through the inter-bank switch for domestic transactions or an international settlement agency for cross-border transactions. Security Key management will be provided by the scheme operator or the domestic banking regulator for both Symmetric Keys based on 3-DES or AES and Asymmetric Keys based on RSA.

Multiple mobile operators and multiple issuer and acquiring banks can be part of the system. Funds flow is handled entirely through the banking system, using proven EMV security with the added layer of GSM/CDMA security for secure communications.

The mCheque Platform in its true sense of 'Interoperability' is intended to support existing systems and technologies used by mobile operators, mobile phones, transaction systems and banks.

The following are the unique features of the present invention:

a. Use of mobile phone as a debit/credit card.
b. Use of mobile phone as a merchant terminal.
c. Use of mobile phone to have multiple debit/credit cards
d. Use of mobile phone to store Track-2 data of a debit/credit card.
e. Responsibility of Authentication of mobile debit/credit card transaction lies with the bank and not with mobile operator.
f. Provisioning of debit/credit card on mobile phone without a contact interface using OTA interface.
g. Provisioning of digital certificate on mobile phone without a contact interface using OTA interface.
h. EMV Handler: Authorization of transaction security on behalf of banks. Ability to handle EMV Transactions in a multibank interoperable environment without enforcing the banks to change their existing infrastructure.

i. Providing printed payment receipt using a mobile phone, wherever possible without making any change on the mobile phone hardware using an external receipt printer.

j. Payment over Internet using debit/credit card on mobile phone.

k. ATM cash-withdrawal using bank card on mobile phone.

l. Person-to-person transfer of payment or funds transfer using mobile phone both domestic and international.

m. Use of Public Key Infrastructure on mobile phones for transactions requiring non-repudiation.

n. Maintaining and managing loyalty pools and coupons on mobile phone.

This invention thus provides a multi-bank interoperable payment system using mobile phone as debit/credit card which comprises the steps of:

(i) establishing connectivity with multiple mobile operators, issuing banks and acquiring banks participating in the "interoperable mCheque system" and inter-bank clearing & settlement systems, both domestic and international, via the mCheque back-end system/issuance system;

(ii) establishing a link with mutual authentication and trust using standard security mechanism between mCheque issuance system, participating bank and the mobile operator. A third party Certification Authority can provide certificates to establish mutual authentication and trust between different systems.

(iii) providing transaction security which is dependent on the bank's security domain defined on the mobile phone. The mobile network is used as a transport and the system does not necessarily depend on the security provided by the mobile network to guarantee transaction security. However, the security provided by the mobile network is treated as a complementary measure.

(iv) Application Provisioning Step-1: loading of payment application containing the basic menus, transaction logic, application security keys

and application configuration data; on the target mobile phone of payer/payee using the over-the-air system of the mobile operator;

(v) Application Provisioning Step-2: loading of a conventional Track-2 data provided by the participating bank with EMV security keys and risk management parameters on the target mobile phone of payer using the over-the-air system of the mobile operator; and

(vi) Application Provisioning Step-3 (optional): loading of a digital certificate on the target mobile phone of payer/payee using the over-the-air system of the mobile operator requiring non-repudiation; and

(vii) establishing a link between the PIN number allotted to the customer and a common mCheque PIN.

The system takes care of post-issuance activities including blocking/unblocking of debit/credit card, creation/deletion of debit/credit cards, update loyalty pool, loyalty redemption, offering of loyalty coupons, blocking/unblocking/resetting of PIN, key version control, application version control, restoration of debit/credit accounts and loyalty details for a lost/stolen mobile phone.

This invention will now be described with reference to the accompanying drawings, wherein:

Fig. 1 illustrates the mCheque transaction flow;

Fig. 2 illustrates the mCheque transaction system;

Fig. 3 illustrates the mCheque Card Issuance/Merchant Configuration System; and

Fig. 4 illustrates the mCheque Digital Certificate System.

The use of mobile phone as a debit or credit card involves the following five steps, which is illustrated in Fig. 1.

1. Payee Mobile sends a message through mobile network to mCheque back-end with Payer Mobile Number, Transaction Amount and a Random Number.

2. mCheque back-end sends a message through mobile network to Payer Mobile with Random Number, Request for Payment and Merchant Details.
3. Payer Mobile sends a message to mCheque back-end through mobile network with EMV Cryptogram.
4. mCheque back-end through mobile network sends a message to Payee Mobile with Transaction Receipt.
5. mCheque back-end through mobile network sends a message to Payer Mobile with Transaction Receipt.

Message-1: Payment Request Message Originating from Merchant

1. Merchant enters the Amount of Transaction, Customer's ID (generally customer's mobile number or a proxy number similar to the mobile number assigned by mCheque) and Merchant PIN using mCheque menus.
2. mCheque Application on Merchant device generates a Random Number (to be used as the seed for the Application Request Cryptogram to be generated on Customer's Mobile Phone for EMV transaction) and signs the transaction data.
3. The Merchant Mobile Phone initiates a session with the mCheque Server and sends the signed data.

Message-2: Confirmation Request Message Terminating on Customer Mobile

1. The signed message from Merchant reaches mCheque Virtual Terminal Application Server (VTAS), which verifies the signature and adds EMV specific terminal risk management parameters and Merchant's Name to the original transaction attributes provided by the merchant.
2. mCheque VTAS initiates a session with Customer Mobile Phone.

Message-3: Confirmation Response Message Originating from Customer Mobile

1. Customer Mobile Phone receives the message-2 and displays a confirmation message consisting of Merchant Name, Transaction Amount and Merchant Id. Up on confirmation by the customer, a PIN entry is requested.
2. Up on successful PIN entry, the Customer Mobile Phone generates an Application Request Cryptogram (ARQC) as per EMV specifications using the Card Risk Management Parameters, Random Number, Card Master Key (of the key index assigned for the application in the card security domain).
3. Customer Mobile Phone sends the transaction data with the ARQC to mCheque VTAS.

Message-4: Transaction Receipt Message Terminating on Merchant

1. mCheque VTAS sends the transaction online for authorization of funds
2. After receiving transaction authorization from the Issuing Bank of the Debit/Credit Card on Customer's Mobile Phone, mCheque VTAS sends a Payment Receipt to the Merchant.
3. After confirmation of Receipt delivery, mCheque VTAS issues a Transaction Certificate to the online authorization system of Issuing Bank (denoting completion of transaction).

Message-5: Transaction Receipt Message Terminating on Customer Mobile Phone

1. After receiving transaction authorization from the Issuing Bank of the Debit/Credit Card on Customer's Mobile Phone, mCheque VTAS sends a Payment Receipt to the Customer Mobile Phone.

To achieve the above, the present invention provides a transaction system (refer Fig. 2 and 3) which comprises of an unique mCheque virtual terminal capable of handling communications from mobile phones of the payer and payee and also ensure security of the transaction, said server having means for customer database and merchant data base, means for providing hardware security, means for storing the digital certificates and application software for life cycle management of payer/payee application.

The process of obtaining a Digital certificate is illustrated in Fig. 4. The mobile phone of the user or purchaser through the personalization system of mCheque issuance system will send in the necessary request to the certification authority and after processing the request, the certification authority will forward the required certificate through to the personalization system of mCheque issuance system back to the mobile phone of the payer/payee.

The following middleware and application systems constitute the mCheque technology platform:

Backend and Middleware Modules:

- **Virtual Terminal Application Server (VTAS):**

VTAS is a secure cluster of virtual EMV terminals, security systems, loyalty systems, bank/operator interfaces running on a High-Availability platform. All mCheque messages originating from the merchant as well as the customer mobile are routed to the VTAS Server. VTAS spawns one instance of Virtual Terminal Application per Merchant Terminal registered in the mCheque system.

- **USAT Interpreter:**

Application Gateway to interpret and perform application codec (encoding/decoding) functions for data flow between VTAS and Mobile phone.

- **EMV Handler:**

The mCheque EMV Handler performs secure authorization of EMV Application Request Cryptogram (ARQC) generated by the chip card EMV application (debit/credit card) on the customer's mobile phone and generates an EMV Application Response Cryptogram (ARPC). The EMV Handler filters EMV specific data from the financial transaction message and the transaction is sent to the Issuing Bank for funds authorization as if it were a regular magnetic stripe transaction authorization request. The EMV Handler therefore provides an effective intermediary Issuing and Acquiring solution for Banks to work with chip cards based on EMV security without having to upgrade their back-end systems to EMV. In case an Issuing Bank is capable of handing EMV transactions directly, the transactions will be directly passed through for authorization by the Bank's EMV Switch. The EMV handler system uses a Hardware Security Module compliant to FIPS-140-2 and PKCS#11 standards to carry out all security operations.

- **Remote Personalization System:**

The mCheque Remote Personalization System provides secure personalization of EMV based secure Debit/Credit cards, Loyalty Pools, Coupons on Mobile phone of mobile phones Over-the-Air (OTA). The Remote Personalization System also uses the OTA bridge for personalization as well as application updates (such as update of EMV risk parameters). Multiple accounts can be handled on a single Mobile phone by this system. The remote personalization system uses a Hardware Security Module to carry out security operations.

- **OTA Bridge:**

Application system providing a secure transport of personalization and transaction data between the mCheque Application Backend (VTAS) and the Network Gateway of mobile operators (USSD Center/SMS Center) for all Over-the-Air application operations on payer/payee mobile phones. The OTA Bridge also takes care of security requirements of the mobile operator.

- **USSD-IP Gateway:**

Network gateway providing exchange of Unstructured Supplementary Service Data (USSD) messages between the Mobile Station and the IP-based backend of mCheque Payment Platform. The mCheque USSD-IP Gateway is co-located with the Master Switching Centre (MSC) of the Mobile Operator through an SS7 (Signaling System 7) link.

- **Transaction Switch:**

Host system to switch financial transactions between Switches of participating banks in ISO 8583/XML formats. This system is also used to log the clearing data provided as input to the central Clearing and Settlement Host.

- **Clearing and Settlements Host:**

This system is used process the data that passes through the Transaction Switch to create logs for daily reconciliation to be performed either through a Clearing and Settlements Bank or an automated system. The Clearing and Settlement Institution will be given summaries for net settlements between participating Banks and each participating bank will be given detailed logs of all transactions performed by its customers.

- **MIS and Reporting Tools:**

Management Information System of mCheque Payment Platform includes reporting, logging and audit trail of transactional and operational data for all participating entities in the system, including merchants, customers, issuing banks, acquiring banks, mobile operators and personalization system.

- **ATM Module:**

An application specification will be provided for enhancement of the ATM customer screen to be able to accept ATM cash withdrawal transactions using mCheque. This requires collaboration with ATM vendors and the respective Banks.

Applications

- Over-the-counter debit/credit payment for small, large and very large amounts. PIN based debit/credit using secure EMV based technology on any mobile phone.
- More versatile than debit/credit cards.
- Display screen, PIN pad and storage add tremendously to usability, convenience and control.
- Multiple cards/accounts can be issued by multiple banks on one mobile.
- Only one PIN to remember - common PIN for all cards/accounts.
- Transaction amount limits and daily limits can be managed on mobile phone.
- Common rewards points pool across all cards/accounts.
- Small value transactions feasible in both credit and debit mode.
- Transaction details stored on mobile phone.
- Balance enquiry.
- Full audit and traceability.
- Unique new method to receive payments: eliminates need of cheque-book.
- PKI based non-repudiable digital-ID and signatures on mobile phone. Ideal for all kind of Government payments and transactions.
- Secure and convenient payment for Internet purchases (unique new method with highest level of security and convenience).
- Instant, anywhere, anytime payment of utility bills; insurance premiums; mobile phone bills; pre-paid top-ups.
- Payment to vending machines (snacks, beverages, etc.).
- Cash withdrawal at ATM machines with subscription based access to large number of ATMs in arrangement with banks.
- Loyalty points-pool-on-mobile phone for accumulating rewards from different merchants. Instant over-the-counter redemption.

The applications are developed without need to customize either the mobile phone hardware. As a result, the entire base of mobile phones available can be used as debit/credit cards and payment terminals without any significant extra investment.

CLAIMS:

1. An inter-operable, multi-operator, multi-bank, multi-merchant mobile payment method using mobile phone as debit/credit card comprising the steps of:
   a. establishing connectivity with each mobile operator, issuing bank and acquiring bank participating in the "interoperable mCheque system" and in any inter-bank clearing & settlement systems, via the mCheque back-end system/issuance system;
   b. establishing a link with mutual authentication and trust using standard security mechanism between mCheque issuance system, participating bank and the mobile operator;
   c. providing transaction security which is dependent on the bank's security domain defined on the mobile phone;
   d. loading of payment application containing the basic menus, transaction logic, application security elements and application configuration data;
   e. loading of at least one conventional Track-2 data provided by the participating bank of the payer, EMV security elements and risk management parameters on the target mobile phone using the over-the-air system of the mobile operator; and
   f. optional loading of digital certificate on the target mobile phone using the over-the-air system of the mobile operator to support applications requiring non-repudiation; and
   g. establishing a link between the PIN number allotted to the customer and the common mCheque PIN.

2. An inter-operable mobile payment method as claimed in claim 1, wherein the loading of payment application is carried out using application provisioning step- 1.

3. An inter-operable mobile payment method as claimed in claim 1, wherein the loading of Track-2 data provided by the participating bank is carried out using application provisioning step-2.

4. An inter-operable mobile payment method as claimed in claim 1, wherein the optional loading of the digital certificate on the target mobile phone using the over-the-air system of the mobile operator to support applications requiring non-repudiation is carried out using application provisioning step-3.

5. An inter-operable mobile payment method as claimed in claim 1, wherein multiple debit/credit card Track-2 data are loaded on the mobile phone.

6. An inter-operable mobile payment method as claimed in claim 1, including an EMV handler for handling EMV Transactions in a multi-bank interoperable environment.

7. An inter-operable mobile payment method as claimed in claim 1, including software for maintaining and managing loyalty pools and coupons on mobile phone.

8. An inter-operable, multi-operator, multi-bank, multi-merchant mobile payment system using mobile phone as debit/credit card comprising of;
   a. mCheque back-end system/issuance system comprising means for establishing connectivity with each mobile operator and issuing bank participating in the "interoperable mCheque system" and in any inter-bank clearing and settlement systems;
   b. Means for establishing a link with mutual authentication and trust using standard security mechanism between mCheque issuance system, participating bank and the mobile operator;
   c. Means for providing transaction security which is dependent on the bank's security domain defined on the mobile phone;
   d. Application provisioning software I to enable loading of payment application containing the basic menus, transaction logic and application configuration data;
   e. Application provisioning software II to enable loading of at least one conventional Track-2 data provided by the participating bank on the target mobile phone using the over-the-air system of the mobile operator;

f. Application provisioning software III for optional loading of digital certificate on the target mobile phone using the over-the-air system of the mobile operator to support applications requiring non-repudiation; and

g. Means for establishing a link between the PIN number allotted to the payer and the common mCheque PIN.

9. An inter-operable mobile payment system as claimed in claim 7, wherein multiple debit/credit Card Track-2 data are loaded in the mobile phone.

10. An inter-operable mobile payment system as claimed in claim 7, including an EMV handler for handling EMV Transactions in a multi-bank interoperable environment.

11. An inter-operable mobile payment system as claimed in claim 7, including software for maintaining and managing loyalty pools and coupons on mobile phone.

12. An inter-operable mobile payment system as claimed in claim 7, wherein the mobile phone of user is used as debit/credit card.

13. An inter-operable mobile payment system as claimed in claim 7, wherein the mobile phone of the merchant is used as merchant terminal.

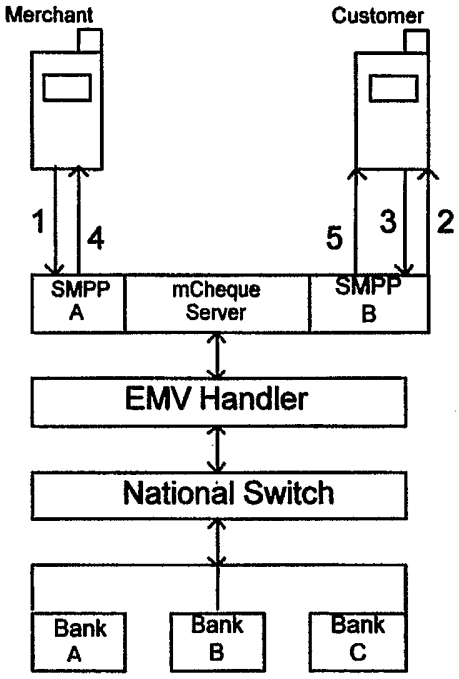

Merchant
Customer
1
4
5
3
2
SMPP A
mCheque Server
SMPP B
EMV Handler
National Switch
Bank A
Bank B
Bank C

Fig. 1.

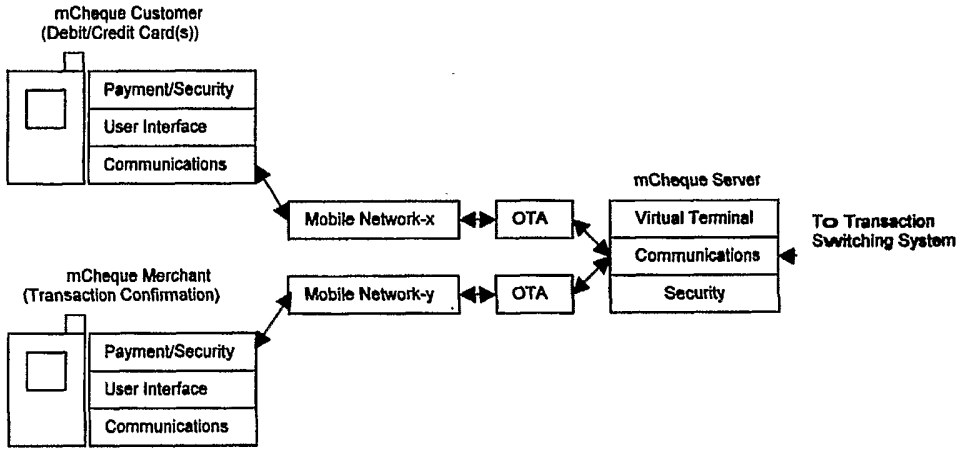

mCheque Customer
(Debit/Credit Card(s))
Payment/Security
User Interface
Communications
Mobile Network-x
OTA
mCheque Server
Virtual Terminal
Communications
Security
To Transaction
Switching System
mCheque Merchant
(Transaction Confirmation)
Mobile Network-y
OTA
Payment/Security
User Interface
Communications

Fig. 2

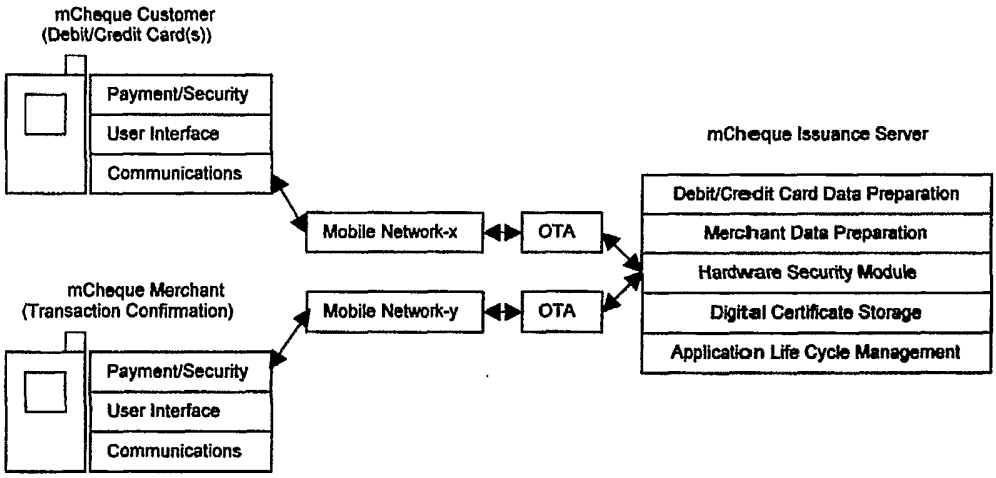

mCheque Customer
(Debit/Credit Card(s))
Payment/Security
User Interface
Communications
Mobile Network-x
OTA
mCheque Issuance Server
Debit/Credit Card Data Preparation
Merchant Data Preparation
Hardware Security Module
Digital Certificate Storage
Application Life Cycle Management
mCheque Merchant
(Transaction Confirmation)
Mobile Network-y
OTA
Payment/Security
User Interface
Communications

Fig. 3

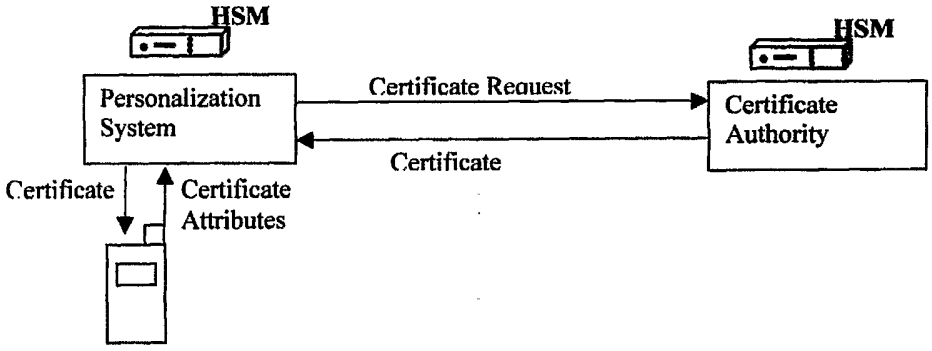

HSM
HSM
Personalization System
Certificate Request
Certificate
Certificate Authority
Certificate
Certificate Attributes

Fig. 4.