

**METHOD AND APPARATUS TO MANAGE  
MOBILE PAYMENT ACCOUNT  
SETTLEMENT**

**CROSS-REFERENCE TO RELATED  
APPLICATIONS**

**[0001]** The present application claims the benefit of U.S. Provisional Application No. 60/915,377, filed 1 May 2007 and U.S. Provisional Application No. 60/883,747 filed 5 Jan. 2007, which are incorporated by reference.

**BACKGROUND**

**[0002]** 1. Field of the Invention

**[0003]** The present invention relates to mobile commerce, and more particularly electronic payment systems for portable communication devices that act as smart cards.

**[0004]** 2. Description of Related Art

**[0005]** Because of the widespread adoption of mobile telephones and of the benefits attributed to the emerging smart card technology for use as stored value devices, there is considerable interest in adapting mobile telephones using smart card technology for use as stored value devices. United States Patent Publication No. 2006/0097037A1, entitled Electronic Value Transfer Device Equipped with Non-Contact IC Interface, by Sakamura, et al. describes one system taking advantage of the smart card technology combined with mobile terminals such as cell phones.

**[0006]** The use of portable electronic devices as smart cards that store value creates a new class of security problem, because of inability to control access to and tampering with the smart cards. Computer-based security technology, including encryption and authentication systems can limit the exposure to tampering. However, consumer trust in such computer-based security technology is low. Also, the incentives for breaking through the computer-based protection grow as the value stored on the device increases.

**[0007]** In addition, the financial transaction networks used for mobile commerce architectures have been dominated by the banking system and communication system providers. This reliance on existing banking and telecommunication provider networks limits the flexibility and has impeded widespread development and use of the technology.

**[0008]** It is desirable to provide an architecture for mobile commerce that reduces the exposure to tampering with mobile communication devices and fraudulent use of the electronically stored money, while also reducing the dependence on access to the banking and telecommunication provider system networks.

**SUMMARY OF THE INVENTION**

**[0009]** A system architecture is described for managing transactions that use a mobile communication device, like a cellular telephone or another similar device. Mobile communication devices used in the architecture described herein are characterized by secure memory usable for storing value and a controller which manages the secure memory. The controller on the mobile communication device supports communication links for the purposes of managing data in the secure memory by at least two independent media, including a protocol executed via a telecommunication provider network and a secure protocol preferably via a short range medium using a wireless proximity coupling device or other type communication link, with a transaction terminal in proximity with

the mobile communication device. In one example, the protocol executed via the telecommunication provider network may be compliant with an industry standard data communication protocol like an email protocol or a Short Message Service SMS protocol defined in GSM recommendation 03.40. Also, in one example, the secure protocol executed for communication with a wireless proximity coupling device at the transaction terminal may be a contactless protocol as contemplated by industry standard ISO 14443. The stored value device may be implemented for example like a smart card as contemplated by industry standard ISO7816 or other similar technologies

**[0010]** According to the system architecture described herein, a transaction operation server communicates with both a transaction terminal and a telecom interface terminal. A telecom interface terminal in the system described herein manages communication channels through the telecommunication provider network between the transaction operation server and the mobile communication devices utilizing the system. The transaction terminal, which may be a stand-alone computer, point of sale device or network, or another mobile communication device, is configured using secure memory technology to prevent tampering with programs or data by the merchants or other people having access to the terminals. The transaction operations server is configured to execute specific application programs which can be tailor-made for individual transaction terminals particularly at merchant sites, utilizing a highly secure and trusted communication environment, such communications based on the public key infrastructure PKI. Also, for any transaction that involves changes to application programs or data that affects the use of the transaction terminal or contents in the stored value device, highly secure authentication/approval/ciphering techniques can be executed over the communication links between the transaction operation server and the transaction terminals. Transactions for value, or for changing programs or data stored on the mobile communication device, are secured by a protocol between the transaction terminal and the mobile communication device using the secure protocol for communication with the reader.

**[0011]** Transactions for value executed according to the architecture described herein include purchasing goods from merchants, purchasing electronic (virtual) coupons or tickets to entertainment events that can be stored on the communication device, purchasing services, transferring funds in the form of electronic checks, electronic coupons and electronic tickets to other mobile communication devices, redeeming electronic checks, coupons or tickets to entertainment events, and so on.

**[0012]** The controller on the mobile communication device is configured to deliver transaction records or other records for the purposes of accounting and verification to the transactions operation server, at the time of transactions and/or periodically independent of actual transaction times, using a communication channel through the telecommunication provider network. Data delivered via the communication channel through the telecommunication provider network is used as a second source of validation of actual transactions executed using transaction terminals, and to provide information that can be used to detect tampering with the secure memory on the mobile communication device.

**[0013]** Interfaces with the banking network are managed by the operations server, which includes an account registration service to establish user accounts, and maintains the neces-