ONLINE PAYMENT USING AN NFC ENABLED DEVICE

Applicant: Blaze Mobile, Inc., Berkeley, CA (US)
Inventor: Michelle Fisher, Oakland, CA (US)
Assignee: Blaze Mobile, Inc., Berkeley, CA (US)
Appl. No.: 13/710,677
Filed: Dec. 11, 2012

Related U.S. Application Data
Continuation of application No. 11/948,903, filed on Nov. 30, 2007, now Pat. No. 8,352,323.

Publication Classification
Int. Cl.
G06Q 20/40 (2012.01)
G06Q 20/20 (2006.01)

US, Cl.
CPC .................. G06Q 20/4012 (2013.01); G06Q 20/20 (2013.01)
USPC .......................... 705/72; 705/65; 705/76

ABSTRACT
A method and system for conducting an online payment transaction through a point of sale device. The method includes receiving input from a user selecting an item for purchase through the point of sale device; calculating a total purchase amount for the item in response to a request from the user to purchase the item; and sending payment authorization for the total purchase amount from the point of sale device to a payment entity, in which the payment authorization is sent to the payment entity via a mobile communication device of the user. The method further includes receiving a result of the payment authorization from the payment entity through the mobile communication device; and completing the payment transaction based on the result of the payment authorization.
FIG. 1

MOBILE COMMUNICATION DEVICE 102

PAYMENT AUTHORIZATION

POINT OF SALE DEVICE 104

MANAGEMENT SERVER 106

FIG. 2

MOBILE COMMUNICATION DEVICE 102

MOBILE APPLICATION 200

SHOPPING LIST 202
302 RECEIVE USER INPUT SELECTING ONE OR MORE ITEMS FOR PURCHASE

304 IN RESPONSE TO A REQUEST FROM THE USER TO PURCHASE THE ONE OR MORE ITEMS, CALCULATING A TOTAL PURCHASE AMOUNT FOR THE ONE OR MORE ITEMS

306 SEND PAYMENT AUTHORIZATION FOR TOTAL PURCHASE AMOUNT TO PAYMENT ENTITY THROUGH MOBILE COMMUNICATION DEVICE OF USER

308 RECEIVE RESULT OF PAYMENT AUTHORIZATION FROM PAYMENT ENTITY THROUGH MOBILE COMMUNICATION DEVICE OF USER

310 COMPLETE PAYMENT TRANSACTION BASED ON RESULTS OF PAYMENT AUTHORIZATION

FIG. 3
ONLINE PAYMENT USING AN NFC ENABLED DEVICE

CROSS-REFERENCE TO RELATED APPLICATIONS

This application is a continuation of application Ser. No. 11/948,903, filed Nov. 30, 2007, titled METHOD AND SYSTEM FOR CONDUCTING AN ONLINE PAYMENT TRANSACTION USING A MOBILE COMMUNICATION DEVICE, all of which is incorporated by reference herein in its entirety.

FIELD OF INVENTION

The present invention relates to data communications and wireless devices.

BACKGROUND OF THE INVENTION

Mobile communication devices—e.g., cellular phones, personal digital assistants, and the like—are increasingly being used to conduct payment transactions as described in U.S. patent application Ser. No. 11/933,351, entitled “Method and System For Scheduling A Banking Transaction Through A Mobile Communication Device”, and U.S. patent application Ser. No. 11/467,441, entitled “Method and Apparatus For Completing A Transaction Using A Wireless Mobile Communication Channel and Another Communication Channel, both of which are incorporated herein by reference. Such payment transactions can include, for example, purchasing goods and/or services, billing payments, and transferring funds between bank accounts.

BRIEF SUMMARY OF THE INVENTION

In general, this specification describes a method and system for conducting an online payment transaction through a point of sale device. The method includes receiving input from a user selecting an item for purchase through the point of sale device; calculating the total purchase amount for the item in response to the request from the user to purchase the item; and sending payment authorization for the total purchase amount from the point of sale device to a payment entity, in which the payment authorization is sent to the payment entity via a mobile communication device of the user. The method further includes receiving a result of the payment authorization from the payment entity through the mobile communication device; and completing the payment transaction based on the result of the payment authorization.

Particular implementations can include one or more of the following features. The point of sale device can be a desktop computer, a laptop computer, or a terminal. The mobile communication device can be a cellular phone, a wireless personal digital assistant (PDA), or a laptop computer. The cellular phone can be an NFC-enabled phone. Sending payment authorization for the total purchase amount from the point of sale device to a payment entity can include sending the payment authorization securely to the payment entity. The payment entity can be a person, a computer system, or a bank. The method can further include maintaining a shopping list on the mobile communication device of the user, in which the shopping list includes a listing of one or more items to be purchased by the user. The payment authorization can be an authorization for payment with a credit card, a debit card, or a prepaid card.

The details of one or more implementations are set forth in the accompanying drawings and the description below. Other features and advantages will be apparent from the description and drawings, and from the claims.

BRIEF DESCRIPTION OF THE DRAWINGS

The details of one or more implementations are set forth in the accompanying drawings and the description below. Other features and advantages will be apparent from the description and drawings, and from the claims.

FIG. 1 illustrates a block diagram of a communication system including a wireless mobile communication device and a management server in accordance with one implementation.

FIG. 2 illustrates one implementation of the wireless mobile communication device of FIG. 1.

FIG. 3 is a method for conducting a payment transaction using a point of sale device in accordance with one implementation.

FIG. 4 illustrates a block diagram of a communication system including a wireless mobile communication device and an online store in accordance with one implementation.

FIG. 5 is a block diagram of a data processing system suitable for storing and/or executing program code in accordance with one implementation.

Like reference symbols in the various drawings indicate like elements.

DETAILED DESCRIPTION OF THE INVENTION

FIG. 1 illustrates one implementation of a communication system 100. The communication system 100 includes a hand-held, wireless mobile communication device 102 a point-of-sale device 104 and a management server 106. In one implementation, the mobile communication device 102 includes a mobile application (discussed in greater detail below) that permits a user of the mobile communication device 102 to conduct payment transactions. Payment transactions can include, for example, using contactless payment technology at a retail merchant point of sale (e.g., through point of sale device 104), using mobile/internet commerce (e.g., purchase tickets and products, etc.), storage of payment information and other digital artifacts (e.g., receipts, tickets, coupons, etc.), storage of banking information (payment account numbers, security codes, PIN’s, etc.), and accessing banking service (account balance, payment history, bill pay, fund transfer, etc.), and so on. The mobile communication device 102 can be a cellular phone, a wireless personal digital assistant (PDA), a laptop computer, or other wireless communication device. The point of sale device 104 can be a desktop computer, laptop computer, terminal, or other device that is configured to receive user input selecting items for purchase or other transaction.

In one implementation, authorizations for payment transactions that are made through the point of sale device 104 are sent from the point of sale device 104 to an issuer authorization (e.g., management server 106) through the mobile communication device 102 (as shown in FIG. 1). In one implementation, an issuer authorization is a payment entity that either approves or disapproves a payment transaction. An issuer authorization can be, e.g., a person, computer system, bank (or other third party). One potential benefit of having payment authorizations flow through the mobile communication device 102 is that sensitive user information (e.g. account numbers, pin numbers, and/or identity information) need only be sent from the mobile communication device 102 directly to an issuer authorization. Such operation reduces the
potential for identity theft and/or fraudulent purchases made through a point of sale device. For example, (in one implementation) payment authorizations cannot be sent to an issuer authorization if the mobile communication device 102 is turned off.

FIG. 2 illustrates one implementation of the mobile communication device 102. The mobile communication device 102 includes a mobile application 200 that (in one implementation) is provided to the mobile communication device 102 through a remote server (e.g., management server 106). In one implementation, the mobile application is a Mobile Wallet application available from Mobile Candy Dish, Inc., of Alameda, Calif. In one implementation, the mobile application is a hosted service, as described in U.S. patent application Ser. No. 11/939,821, entitled “Method and System For Securing Transactions Made Through a Mobile Communication Device”, which is incorporated herein by reference. In one implementation, the mobile application 200 is configured to send requests to the management server for artifacts based on user input, e.g., received through a keypad (not shown) of the mobile communication device 102. Requests to the management server 106 can also be automated, via proximity-based services, e.g., consumer tapping (or in close proximity) an LBS/contactless/RFID enabled phone against a smart poster (RFID/Bluetooth/LBS enabled, etc.), kiosk, or other device.

In one implementation, the mobile application 200 running on the mobile communication device 102 is configured to receive artifacts (e.g., advertisements, receipts, tickets, coupons, media, content, and so on) from the management server 106. In one implementation, the management server 106 sends artifacts to the mobile application based on user profile information and/or transaction history (or payment trends) associated with a user of the mobile communication device 102 as described in U.S. patent application Ser. No. 11/944,267, entitled “Method and System For Delivering Information To a Mobile Communication Device Based On Consumer Transactions”, which is incorporated herein by reference.

In one implementation, the mobile communication device 102 is an NFC-enabled phone. The mobile communication device 102 can be NFC-enabled, for example, through an embedded chip or a sticker that is affixed to the cellular phone, as described in U.S. application Ser. No. 11/933,321, entitled “Method and System For Adapting a Wireless Mobile Communication Device For Wireless Transactions”, which is incorporated herein by reference. In one implementation, the NFC chip (or sticker) on the cellular phone can be used in conjunction with a merchant’s point of sale device as described in greater detail below.

For example, with reference to FIG. 4, in one implementation, the NFC chip (or sticker) on the cellular phone can communicate with NFC chips that are installed on the front of PC’s (TV’s, Kiosks, or any other device) and serve as scanners/readers. In this implementation a mobile candy dish applet (e.g., MCD POS plugin 414) is installed on the consumer’s computer (e.g., PC 404) which interfaces with the NFC chip on the PC. When a consumer (or user) is shopping online and they are ready to pay for their products, the consumer opens his mobile wallet and selects one of the payment methods (e.g., credit card, debit card, prepaid card, etc.) from their mobile wallet. If a default card has been selected already, this step is not necessary. The consumer then waves their phone over the NFC reader present on the PC 404. The consumer’s payment credentials are transferred from the phone to the merchant website (e.g., online store application 410) using a communication protocol between the chip in the phone and the chip in the PC, which can be radio frequency for example. If the consumer has coupons in their mobile wallet the consumer can either elect to manually apply the coupon, save the coupon for a future use (against a larger purchase for example), or have the coupon automatically applied during the transaction and the transaction amount is updated. After the consumer enters any necessary validation information (e.g., pin) to provide a multi-factor authentication and confirms the transaction, the online purchase is processed as normal by the merchant’s online processor. The mobile wallet can retrieve transaction data, account balance from the management server 408.

In one implementation, the mobile communication device 102 is a non NFC-enabled phone. In this implementation, the consumer connects his phone to the PC 404 via some non radio frequency method (e.g., IR, Bluetooth, USB cable, etc.). When a consumer is shopping online and they are ready to pay for their products, the consumer opens his mobile wallet and selects one of the payment methods (e.g., credit card, debit card, prepaid card, etc.) from their mobile wallet. If a default card has been selected already, this step is not necessary. The consumer then pushes, e.g., a “Buy now” button and the consumer’s payment credentials are transferred from the phone to the merchant website (e.g., online store application 410) using the protocol between the phone and the PC 404 which can be radio frequency, for example. If the consumer has coupons in their mobile wallet the consumer can either elect to manually apply the coupon, save the coupon for a future use, or have the coupon automatically applied during the transaction and the transaction amount is updated. After the consumer enters any necessary validation information (e.g., PIN) to provide multi-factor authentication and confirms the transaction, the online purchase is processed as normal by the merchant’s online processor. The mobile wallet can retrieve transaction data and account balance from the management server 408.

In one implementation, the management server 408 and merchant portal (e.g., online store 408) are maintained by trusted parties and use an encrypted tunnel to transfer financial data. When the consumer is ready to pay for their online product, they enter their cell phone number on the merchant portal. The merchant portal (which has an MCD applet (e.g., MCD POS plugin 414) installed on its server) securely connects to the management server 408 (that in one implementation is maintained by Mobile Candy Dish (MCD)). In one implementation, the management server 408 identifies the consumer through their cell phone number, and verifies the consumer’s authenticity by sending a unique transaction code to the consumer mobile wallet on their cell phone. The consumer then enters this unique transaction code onto the merchant’s web portal. The merchant portal sends this transaction number to the management server 408 for authentication. Upon authentication, the consumer’s virtual wallet and payment methods (e.g., credit card, debit card, prepaid card, etc.) are securely retrieved from the management server 408 and are displayed to the consumer in a window on a website associated with the merchant portal. The consumer selects one of these payment methods to pay for their transaction. If a default card has been selected already, this step is not necessary. If the consumer has coupons in their mobile wallet the consumer can either elect to manually apply the coupon, save
the coupon for a future use, or have the coupon automatically applied during the transaction and the transaction amount is updated. After the consumer enters any necessary validation information to provide a multi-factor authentication and confirms the transaction, the online purchase is processed as normal by the merchant’s online processor. The mobile wallet can retrieve transaction data, account balance from the management server 408.

Referring to FIG. 2, in one implementation, the mobile application 200 maintains a shopping list 202 for a consumer. Accordingly, consumers have the ability to store their shopping list in their mobile wallet and add, delete, or change items on their shopping list either in offline or online mode. In one implementation, consumers are sent coupons based on items on their shopping list, preferences, previous shopping history, proximity to the physical retail store, or a combination of these parameters, as discussed in application Ser. No. 11/944,267, which is incorporated by reference above. If the consumer has coupons in their mobile wallet the consumer can either elect to manually apply the coupon, save the coupon for a future use, or have the coupon automatically applied during the transaction and the transaction amount is updated. When a consumer wants to order the items on their shopping list via an online merchant (in contrast to a physical retail store), the consumer can logon to the merchant portal and electronically transmit their shopping list to the merchant portal either by waving their phone over NFC enabled phone’s or some other connection such as IR, Bluetooth, USB, or the like.

FIG. 3 illustrates a method 300 for conducting a payment transaction using a point of sale device (e.g., point of sale device 104). User input is received selecting one or more items for purchase (e.g., at the point of sale device) (step 302). In general, the transaction being made at the point of sale device can be any type of transaction that involves the exchange or transfer of funds—e.g., the transaction can be a payment transaction, a fund transfer, or other type of transaction. In response to a request from the user to purchase the one or more items, a total purchase amount for the one or more items is calculated (e.g., by the point of sale device) (step 304). If the user has coupons in their mobile wallet the user can either manually apply the coupon or have the coupon automatically applied during the transaction and the transaction amount is updated. The user request to purchase an item can be received, e.g., by a user clicking on a “buy now” icon that is displayed on a graphical user interface of the point of sale device. Payment authorization for the total purchase amount is sent to a payment gateway through a mobile communication device of the user (step 306). A result of the payment authorization is received at the point of sale device from the payment gateway through the mobile communication device (step 308). The payment transaction is completed based on the result of the payment authorization (step 310). If the payment transaction was authorized by the payment gateway, then the sale of the items through the point of sale device is completed. Otherwise, if the payment transaction was not authorized by the payment gateway, then the point of sale device terminates the payment transaction.

FIG. 4 illustrates an example payment transaction being made in a communication system 400 in accordance with one implementation. The communication system 400 includes a mobile communication device 402, a personal computer (PC) 404, an online store 406, and a core (or datastore) 408. As indicated by interaction (1), a user (or customer), using a phone (e.g., mobile communication device 402 or personal computer 404), browses an online store website (online store application 410) and finds an item that the customer wishes to purchase. This could also be a purchase made through a midlet application (POS midlet 412) residing on the mobile communication device 402. The user then goes to, e.g., a checkout of the online store 406 and makes a purchase. If the user has coupons in their mobile wallet the user can either manually apply the coupon or have the coupon automatically applied during the transaction and the transaction amount is updated. When it comes time to authorize the purchase, (in one implementation) the user is given an option to purchase with the mobile communication device 402. In one implementation, the mobile communication device 402 is an NFC-equipped phone (or NFC phone).

In interaction (2), when the user chooses to purchase with the mobile communication device 402, the online store application 410 sends the transaction information for authorization to the POS vendor plugin (e.g., MCD POS plugin 414). In one implementation, the POS vendor plugin is installed in the merchant’s online store and enables the merchant to accept MCD Blaze payments as an alternative form of payment, similar to accepting credit cards for payment. As shown by interaction (3), the POS vendor plugin formats, encrypts, and cryptographically signs the purchase authorization request which is sent via a secure SSL link (e.g., HTTPS, Bluetooth, IR, USB, or other suitable protocol) established by the browser/web application 416 back to the mobile communication device 402. As with the first scenario, all communication is over secure channels. (It may be required that the mobile wallet application be opened prior to beginning a phone online purchase.) The POS midlet 412 is a component of the mobile wallet application that executes PayPass or other payment authorization protocol between itself and the SE payment applications on the mobile communication device 402 (interaction (4)). The results of the request are sent back to the POS vendor plugin.

As shown by interaction (5), the POS midlet 412 then forwards the properly formatted authorization request to a payment entity (e.g., issuer authorization 418) for authorization. The results of the request are then sent back to the POS component of the mobile wallet. Through interaction (6), the POS midlet 412 then forwards the results back to the MCD POS plugin 414 to complete the purchase. The MCD POS plugin 414 then forwards the purchase transaction information to the management server 408 (or intercustomer viewing (interaction (7)). As indicated by interaction (8), users (or customers) will then be able to query the management server 408 and immediately obtain purchase information, either by phone or PC.

One or more of method steps described above can be performed by one or more programmable processors executing a computer program to perform functions by operating on input data and generating output. Generally, the invention can take the form of an entirely hardware embodiment, an entirely software embodiment or an embodiment containing both hardware and software elements. In one implementation, the invention is implemented in software, which includes but is not limited to firmware, resident software, microcode, etc. Furthermore, the invention can take the form of a computer program product accessible from a computer-readable medium providing program code for use by or in connection with a computer or any instruction execution system. For the purposes of this description, a computer-
usable or computer readable medium can be any apparatus that can contain, store, communicate, propagate, or transport the program for use by or in connection with the instruction execution system, apparatus, or device. The medium can be an electronic, magnetic, optical, electromagnetic, infrared, or semiconductor system (or apparatus or device) or a propagation medium. Examples of a computer-readable medium include a semiconductor or solid state memory, magnetic tape, a removable computer diskette, a random access memory (RAM), a read-only memory (ROM), a rigid magnetic disk and an optical disk. Current examples of optical disks include compact disk—read only memory (CD-ROM), compact disk—read/write (CD-R/W) and DVD.

[0027] FIG. 5 illustrates a data processing system 500 suitable for storing and/or executing program code. Data processing system 500 includes a processor 502 coupled to memory elements 504A-B through a system bus 506. In other implementations, data processing system 500 may include more than one processor and each processor may be coupled directly or indirectly to one or more memory elements through a system bus. Memory elements 504A-B can include local memory employed during actual execution of the program code, bulk storage, and cache memories that provide temporary storage of at least some program code in order to reduce the number of times the code must be retrieved from bulk storage during execution. As shown, input/output or I/O devices 508A-B (including, but not limited to, keyboards, displays, pointing devices, etc.) are coupled to data processing system 500. I/O devices 508A-B may be coupled to data processing system 500 directly or indirectly through intervening I/O controllers (not shown).

[0028] In one implementation, a network adapter 510 is coupled to data processing system 500 to enable data processing system 500 to become coupled to other data processing systems or remote printers or storage devices through communication link 512. Communication link 512 can be a private or public network. Modems, cable modems, and Ethernet cards are just a few of the currently available types of network adapters.

[0029] Although the present invention has been particularly described with reference to implementations discussed above, various changes, modifications and substitutes are can be made. Accordingly, it will be appreciated that in numerous instances some features of the invention can be employed without a corresponding use of other features. Further, variations can be made in the number and arrangement of components illustrated in the figures discussed above.

What is claimed is:
1. A method comprising:
   receiving an input request from a user selecting an item for purchase from a merchant portal, the input request received at a mobile device, the mobile device comprising a mobile device display, a mobile device processor, a mobile device radio interface configured to use a first communication channel for voice and data interactions, and a mobile device memory;
   sending a transaction request to the merchant portal, the merchant portal configured to determine a total purchase amount and encrypt and cryptographically sign a payment authorization for the total purchase amount;
   receiving the encrypted and cryptographically signed payment authorization for the total purchase amount;
   executing a POS midlet payment authorization protocol between a POS midlet and a secure element payment application in response to a near field communication interaction between the POS midlet and the secure element payment application configured to run on a secure element, the secure element coupled to the mobile device;
   wirelessly transmitting a purchase authorization request from the POS midlet to a financial institution;
   receiving a payment authorization from the financial institution at the POS midlet for purchase of the item through the first communication channel; and
   transmitting the purchase authorization from the POS midlet to a vendor POS plugin at the merchant portal to complete the purchase.
2. The method of claim 1, wherein the secure element comprises a secure element memory configured to maintain the secure element payment application and payment credentials, a secure element processor configured to execute the secure element payment application to transfer data including payment credentials to the POS midlet, a secure element wireless transceiver configured to transfer data to the POS midlet using a second communication channel different from the first communication channel.
3. The method of claim 2, wherein a digital artifact is received at the secure element from the POS midlet through the second communication channel.
4. The method of claim 3, wherein the digital artifact is presented on the mobile device display.
5. The method of claim 1, wherein the POS midlet is a desktop computer, a laptop computer, or a thin client, and wherein the point of sale terminal includes an NFC chip configured as an NFC scanner and an NFC reader.
6. The method of claim 1, further comprising automatically applying a coupon during the near field communication transaction.
7. The method of claim 1, further comprising automatically applying a default payment method during the near field communication transaction.
8. The method of claim 6, wherein a receipt, ticket, or coupon is sent to the mobile device after the transaction.
9. The method of claim 8, wherein the item is included in a virtual shopping list received at the mobile device through a near field communication interaction.
10. The method of claim 1, wherein the item is included in a virtual shopping list received at the mobile device through a near field communication interaction.
11. The method of claim 1, wherein the secure element is physically coupled to the mobile device and electrically coupled to electrical interior components of the mobile device.
12. The method of claim 1, wherein the secure element is included within a body of a memory card configured for placement in a memory card slot in the mobile device.
13. The method of claim 1, wherein the secure element is embedded within a body of the mobile device.
14. The method of claim 1, wherein a security tool is implemented at the mobile device, and wherein implementation of the security tool comprises prompting the user to login to the mobile device, using biometrics to authenticate the user before authorizing a transaction, disabling use of the mobile device, prompting the user to enter a payment limit PIN in response to a pending purchase exceeding a pre-determined amount, temporarily disabling the secure element, permanently disabling the secure element, deleting all cached data stored in the mobile device memory, and/or storing encrypted
security codes on the mobile device, wherein disabling the secure element prevents near field communication payments, coupon redemption, and ticket redemption.

15. A mobile device comprising:
   a mobile device input interface configured to receive an input request from a user selecting an item for purchase from a merchant portal;
   a mobile device output interface configured send a transaction request to the merchant portal, the merchant portal configured to determine a total purchase amount and encrypt and cryptographically sign a payment authorization for the total purchase amount, wherein the encrypted and cryptographically signed payment authorization is received for the total purchase amount;
   a mobile device processor configured to execute a POS midlet payment authorization protocol between a POS midlet and a secure element payment application in response to a near field communication interaction between the POS midlet and the secure element payment application configured to run on a secure element, the secure element coupled to the mobile device;
   a wireless transceiver configured to transmit a purchase authorization request from the POS midlet to a financial institution and receive a payment authorization from the financial institution at the POS midlet for purchase of the item through the first communication channel, wherein the purchase authorization is transmitted from the POS midlet to a vendor POS plugin at the merchant portal to complete the purchase.

16. The mobile device of claim 15, wherein the secure element comprises a secure element memory configured to maintain the secure element payment application and payment credentials, a secure element processor configured to execute the secure element payment application to transfer data including payment credentials to the POS midlet, a secure element wireless transceiver configured to transfer data to the POS midlet using a second communication channel different from the first communication channel.

17. The mobile device of claim 16, wherein a digital artifact is received at the secure element from the POS midlet through the second communication channel.

18. The mobile device of claim 17, wherein the digital artifact is presented on the mobile device display.

19. The mobile device of claim 15, wherein the POS midlet is a desktop computer, a laptop computer, or a thin client, and wherein the point of sale terminal includes an NFC chip configured as an NFC scanner and an NFC reader.

20. The mobile device of claim 15, further comprising automatically applying a coupon during the near field communication transaction.

* * * * *