US 20130012125A1

(19) United States

(12) Patent Application Publication

(10) Pub. No.: US 2013/0012125 A1

(43) Pub. Date: Jan. 10, 2013

Fisher et al.

(54) SECURE NFC PAYMENT TRANSACTIONS

(75) Inventors: **Michelle Fisher**, Oakland, CA (US); **Rathin Guha**, Alameda, CA (US)

(73) Assignee: **BLAZE MOBILE, INC.**, Berkeley, CA (US)

(21) Appl. No.: **13/620,263**

(22) Filed: **Sep. 14, 2012**

Related U.S. Application Data

(63) Continuation of application No. 11/939,821, filed on Nov. 14, 2007, now Pat. No. 8,290,433.

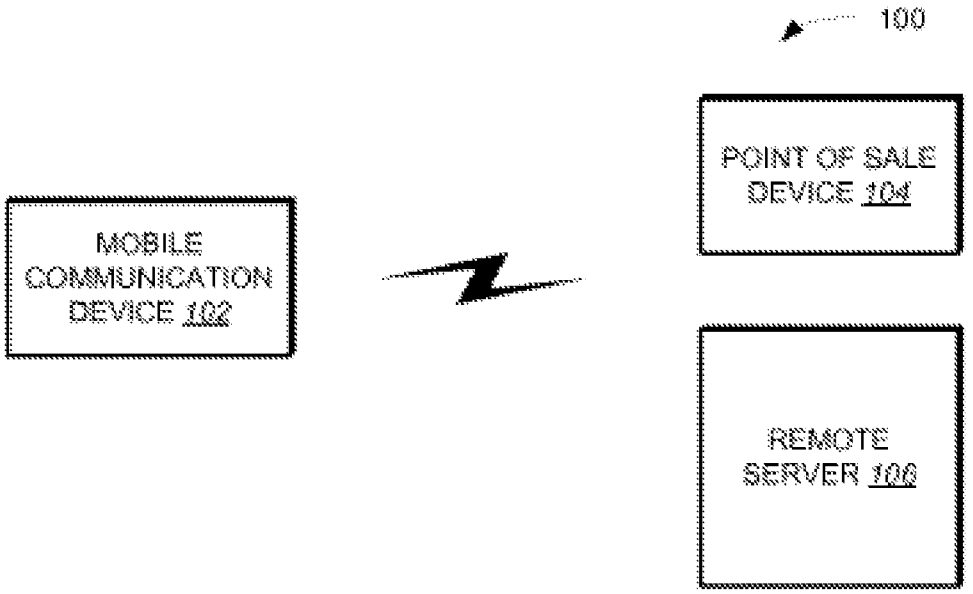
Publication Classification

(51) **Int. Cl.**
H04B 5/00 (2006.01)

(52) **U.S. Cl.** **455/41.1**

(57) **ABSTRACT**

A method for transmitting data between a mobile communication device and a server. The method includes running a mobile application on the mobile communication device. The mobile application is hosted on the mobile communication device through the server as a Software as a Service (SaaS). The method further includes transmitting data associated with the mobile application between the mobile communication device and the server, in which transmission of the data between the mobile communication device and the server is monitored through the server.



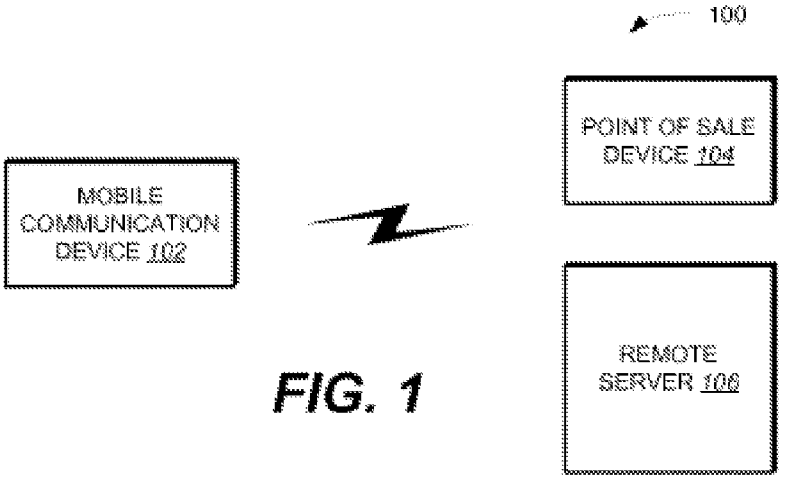


FIG. 1

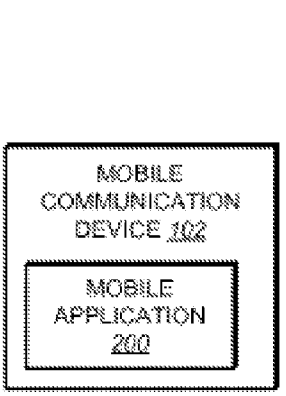


FIG. 2

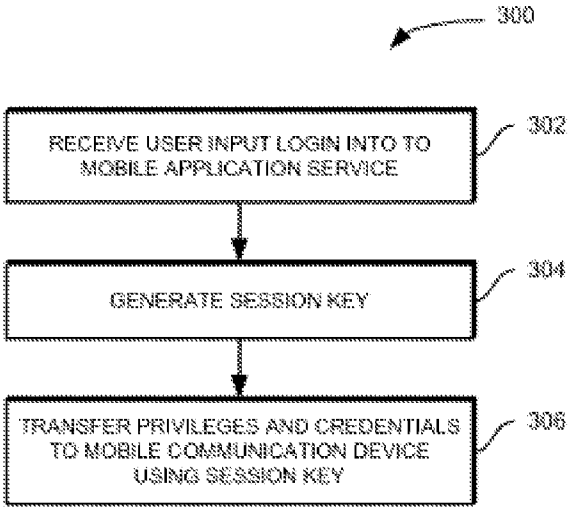


FIG. 3

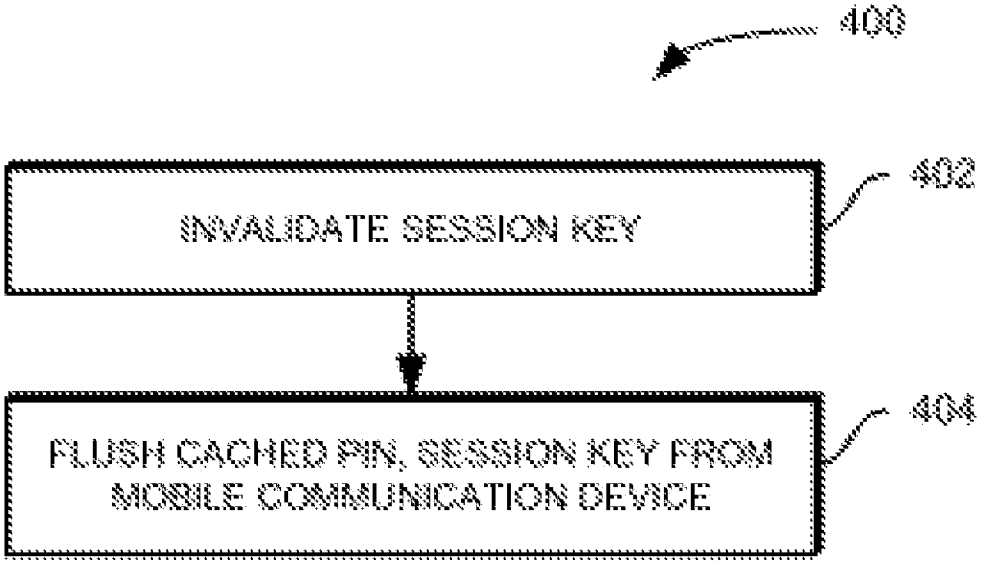

400
INVALIDATE SESSION KEY
402
FLUSH CACHED PIN, SESSION KEY FROM MOBILE COMMUNICATION DEVICE
404

FIG. 4

SECURE NFC PAYMENT TRANSACTIONS

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application is a continuation of application Ser. No. 11/939,821, filed Nov. 14, 2007, titled METHOD AND SYSTEM FOR SECURING TRANSACTIONS MADE THROUGH A MOBILE COMMUNICATION DEVICE, all of which is incorporated by reference herein in its entirety.

FIELD OF INVENTION

[0002] The present invention relates to data communications and wireless devices.

BACKGROUND OF THE INVENTION

[0003] 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, bill payments, and transferring funds between bank accounts. Given the sensitive nature of personal money or banking data that may be stored on a mobile communication device as a result of the ability to transact payments, it is critical to protect a user from fraudulent usage due to, e.g., loss or theft of a mobile communication device.

BRIEF SUMMARY OF THE INVENTION

[0004] In general, in one aspect, this specification describes a method for transmitting data between a mobile communication device and a server. The method includes running a mobile application on the mobile communication device. The mobile application is hosted on the mobile communication device through a management server. The method further includes transmitting data associated with the mobile application between the mobile communication device and the server, in which transmission of the data between the mobile communication device and the management server is monitored through the management server.

[0005] Implementations can include one or more of the following features. Transmitting data can include generating a session key that is only valid for a given communication session between the mobile communication device and the server. The method can further include disabling use of the mobile application running on the mobile communication device through the management server by invalidating the session key. The method can further include timing out a given communication session between the mobile communication device and the management server after a pre-determined amount of time to prevent theft of data that is accessible through the mobile application. Transmitting data associated with the mobile application between the mobile communication device and the management server can include prompting a user to enter a payment limit PIN in response to a pending purchase exceeding a pre-determined amount. The payment limit PIN can be applied to all purchases globally or on a per-payment basis. The method can include use of biometrics to authenticate the user before authorizing the transacation. The mobile application can comprise a payment transaction application that permits a user to perform one or more of the following services including bill payment, fund transfers, or purchases through the mobile communication device. The mobile application can permit a user to subscribe to each of the services separately.

[0006] 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

[0007] FIG. **1** illustrates one implementation of a block diagram of a communication system including a wireless mobile communication device.

[0008] FIG. **2** illustrates one implementation of the wireless mobile communication device of FIG. **1**.

[0009] FIG. **3** illustrates one implementation of a method for authenticating a user.

[0010] FIG. **4** illustrates one implementation of a method for remotely locking use of a mobile application on a mobile communication device.

[0011] Like reference symbols in the various drawings indicate like elements.

DETAILED DESCRIPTION OF THE INVENTION

[0012] 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 remote 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 (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.

[0013] In one implementation, the mobile application running on the mobile communication device **102** implements one or more of the following tools to secure data that may be stored and presented on the mobile communication device **102** as a result of a payment transaction. The mobile application can implemented one the mobile communication device **102** through a management server which hosts and operates (either independently or through a third-party) the application for use by its customers over the Internet, or other wireless network (e.g., a private network), or a wired network . In one implementation, customers do not pay for owning the software itself but rather for using the software. In one implementation, the mobile application is accessible through an API accessible over the Web (or other network). The mobile application can include a multi-factored PIN-based login and authentication, and include session keys and have command-level authentication. In one implementation, the mobile application running on the mobile communication device **102**

can be remotely locked through a remote server (e.g., remote server **106**). In one implementation, a PIN request can be implemented to limit the amount of purchases that can be made. Further, security codes for different payment methods can be implemented to protect a user. Each of these tools is discussed in greater detail below.

[0014] 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., remote server **106**). In one implementation, the mobile application is a Mobile Wallet application available from Mobile Candy Dish, Inc., of Berkeley, Calif. Providing the mobile application as a hosted service enables central monitoring and management of all security aspects of the service at the remote server. In addition, data (corresponding to a payment transaction) can be stored on the remote server (e.g., remote server **106** (FIG. **1**)) in a secure manner. In one implementation, the remote server is a management server that is can be maintained by Mobile Candy Dish or a trusted third party, as described in U.S. patent application Ser. No. 11/933,351. For example, the data can be securely stored on the remote server using conventional PCI guidelines. Hence, in the event the mobile communication device **102** is lost (or stolen), no confidential data can be recovered as no data is stored on the mobile communication device **102**. In addition, an added benefit is that a user can recover seamlessly by syncing new mobile communication device (via new installation of the mobile application) with the service. Thus, in one implementation, sensitive information (e.g., banking account numbers, credit card account numbers, expiry dates, and so on) are never stored on the mobile communication device. This reduces risk and exposure of the user's private information and data.

Client Login and Authentication

[0015] In general, while effort is made to minimize storage of sensitive user information and data in a memory of a mobile communication device, in one implementation, some data is stored in the memory of a mobile communication device due to reasons of performance, usability and user experience. For example, data may need to be stored on a mobile communication device in the following circumstances. Payment credentials, coupons, tickets, and so on may have to be stored on the secure element of an NFC phone. Account balance, banking payment history, etc., may be locally cached on a mobile communication device. In one implementation, a user can opt-in to save payment method security codes in the client (or mobile application) for convenience. Tickets and/or coupons may be locally cached so that a user can redeem the tickets and/or coupons in an offline mode. For example, a mobile communication device may be offline in a situation in which network connectivity inside a building is degraded, and storing a ticket and/or coupon in a local cache of the mobile communication device permits the user to access the ticket or coupon.

[0016] In addition to data partitioning, in one implementation, users have an ability to subscribe to different services. For example, User A may subscribe to "Mobile Payments" and "Mobile Banking" services, while User B may only subscribe to "Mobile Banking" and "What's Nearby" services. Hence, in one implementation, the mobile application includes a mechanism to enable/disable different services on the Client based on particular services to which users are subscribed. Table 1 below illustrates example services that are enabled/disabled based on user subscriptions.

TABLE 1

USER	SERVICE	SUBSCRIPTION STATUS
User A	Money Manager	Disabled
User B	Money Manager	Transaction Only
User C	Money Manager	Transaction, Payment
User D	Money Manager	Transaction, Payment, BillPay, FundTransfer

The above example control access to the Money Manager service and what privileges within the service a given user can perform. This will be used by the Client (mobile application) to enable/disable available features on the Client.

[0017] In one implementation, when a user subscribes to a mobile wallet the user is assigned credentials that include a unique WalletID, SiteKey, a user-defined PIN, as well as tokens that specify access and privileges for the different services. FIG. **3** illustrates one implementation of a method **300** for authenticating a user. User input is received (through a mobile communication device) logging into the mobile application service (step **302**). In one implementation, when a user attempts to login with the client, the user is prompted to enter login credentials (e.g., mobile phone number, 1-time activation code, Wallet PIN, etc.). A session key is generated (step **304**). In one implementation, the session key is a unique server-generated session key that is valid only for the duration of a given session. In one implementation, the session key is used to ensure the server can identify the client and ensure that the client has been previously authenticated. Upon a successful login, the server will transfer credentials, service access and privileges (step **306**), which are locally cached on the mobile communication device. The service access and privileges control the behavior of the client. In one implementation, to prevent command spoofing, the session key is passed in every API server call. The server will validate (every time) the session key is valid. If valid, the API server call is processed. Failure to validate the session key will cause a failure. In such a case, the client will flush the cached PIN and force the user to re-authenticate (or re-login).

Remote Lock

[0018] In one implementation, a mobile application running on a mobile communication device can be remotely locked (or disabled) by invalidating a session key. Users, via calling a Customer Care, a personal web portal, or some other mechanism, can implement changes (e.g., change PIN, etc.) that causes the server to invalidate the session key. In real-time, the next attempt by the client to issue an API server call, validation of the session key will fail, which (in one implementation) causes the client to automatically flush the cached PIN and session key, and force the user to re-authenticate. In addition, the client can perform additional actions, in addition to flushing the cached PIN and session key. This includes, but is not limited to, one or more of the following: changing the secure element mode to effective temporarily or permanently disable the secure element—i.e., a user can remotely alter the state of the smart chip to lock it remotely; and deleting all cached data stored in the memory (or disk) of the mobile communication device.

Session Time Out

[0019] In one implementation, while a client is open, a user has access to transaction data. In such an implementation, users who may misplace a mobile communication device while the client is open may expose the user to risk of information theft. Therefore, in one implementation, mobile application (or client) shuts down after a period of inactivity. Additional tasks that can be associated with the shutdown procedure can include, but is not limited to, temporarily shutting down a secure element (of the mobile communication device) to prevent NFC payments, NFC coupon redemption, and NFC ticket redemption.

Payment Limit PIN

[0020] For payments (mobile commerce ticket purchase, etc.), in one implementation a user can prevent either fraudulent purchases or accidental purchases by forcing a PIN prompt when a purchase amount exceed a user-specified value. In one implementation, a user can control this behavior globally (e.g., across all users' payment methods) or on a per-payment-method basis. Thus, when a user purchases ticket and selects a payment method (to pay for purchase), if the transaction amount exceeds a specified payment method's limit, the client will trigger and prompt for the PIN. In order to proceed with purchase, the user has to enter the correct PIN. The user's input is validated against the cached PIN on the client. The payment transaction will proceed if validated. Otherwise, an appropriate response is generated to the user. Effectively, this is a mechanism for the user (not the Merchant or Issuing Bank) to throttle/control the dollar amount that can be authorized for various payments and transactions. In the event of a contactless purchase, the client controls the smart chip. In the event of an electronic purchase (ticketing, etc.), a server can manages the controls.

Local Storage of Payment Security Codes

[0021] As a convenience to users, a user can opt-in and have only the security codes (CVV, etc.) associated to each of their payment methods locally stores on the client. In one implementation, management tools are provided to add/delete/edit these security codes. In one implementation, the security codes are encrypted (Key Management of encryption key performed by a server) and then only stored in the client on the mobile communication device. In one implementation, security codes are not stored in any form on the server. The encryption key and security codes can be kept separately to prevent fraudulent usage.

[0022] 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 for conducting a near field communication contactless payment transaction, the method comprising:

determining that a data exchange between a mobile application running on a mobile communication device and a management server has occurred, wherein the management server permits a user associated with the mobile application running on the mobile communication device to conduct a near field communication contactless payment transaction as a result of the data exchange, wherein the mobile communication device includes a mobile communication device processor, a mobile communication device memory, and a mobile communication device wireless transceiver configured to support a first communication channel;

maintaining a payment application and payment credentials in a secure element memory of a secure element, wherein execution of the payment application facilitates transfer of payment credentials to a point-of-sale terminal;

executing the payment application stored in the secure element memory of the secure element by using a secure element processor in the secure element, wherein the payment application is executed in response to detection of a near field communication induction-based trigger by the point-of-sale terminal;

transmitting transaction data by using a secure element wireless transceiver included in the secure element, the secure element wireless transceiver configured for near field communications, wherein transaction data is sent through a second communication channel to the point-of-sale terminal, wherein the second communication channel is different from the first communication channel.

2. The method of claim **1**, wherein the data exchange includes exchanging an identification code

3. The method of claim **2**, wherein the identification code is a personal identification number (PIN).

4. The method of claim **1**, wherein the data exchange includes using a session key that is only valid for a given communication session between the mobile communication device and the management server.

5. The method of claim **1**, wherein the data exchange between the mobile communication device and the management server includes prompting a user to enter a payment limit personal identification number (PIN) in response to a purchase exceeding a pre-determined amount.

6. The method of claim **1**, wherein access to data associated with the data exchange is controlled.

7. The method of claim **6**, wherein access to the data is controlled by deleting cached data from the mobile communication device memory of the mobile communication device and from the secure element memory of the secure element.

8. The method of claim **6**, wherein access to the data is controlled by disabling the secure element.

9. The method of claim **1**, wherein the user is prompted for a personal identification number (PIN) by the mobile application before allowing the user to conduct the payment transaction.

10. The method of claim **1**, wherein the user is prompted for biometric data before allowing the user to conduct the payment transaction.

11. The method of claim **1**, wherein the user is prompted for multifactor authentication before allowing the user to conduct the payment transaction.

12. The method of claim **1**, wherein the secure element is permanently embedded within the body of the mobile communication device.

13. The method of claim **1**, wherein the secure element is affixed externally to the mobile communication device.

14. The method of claim **1**, wherein the secure element is removably embedded in a slot of the mobile communication device.

15. The method of claim **1**, wherein the mobile communication device wireless transceiver in the mobile communication device communicates wirelessly with the secure element wireless transceiver in the secure element.

16. The method of claim **1**, wherein the mobile communication device processor in the mobile communication device communicates through a wired connection to the secure element processor in the secure element.

17. A secure element for conducting a near field communication contactless payment transaction, the secure element comprising:

a secure element processor configured to determine that a data exchange between a mobile application running on a mobile communication device and a management server has occurred, wherein the management server permits a user associated with the mobile application running on the mobile communication device to conduct a near field communication contactless payment transaction as a result of the data exchange, wherein the mobile communication device includes a mobile communication device processor, a mobile communication device memory, and a mobile communication device wireless transceiver configured to support a first communication channel;

a secure element memory configured to maintain a payment application and payment credentials, wherein execution of the payment application occurs in response to detection of a near field communication induction-based trigger by a point-of-sale terminal and execution of the payment application facilitates transfer of payment credentials with the point-of-sale terminal; and

a secure element wireless transceiver configured to transmit transaction data, the secure element wireless transceiver configured for near field communications, wherein transaction data is sent through a second communication channel to the point-of-sale terminal, wherein the second communication channel is different from the first communication channel.

18. The secure element of claim **17**, wherein the data exchange includes exchanging an identification code.

19. The secure element of claim **18**, wherein the identification code is a personal identification number (PIN).

20. The secure element of claim **17**, wherein the data exchange includes using a session key that is only valid for a given communication session between the mobile communication device and the management server.

21. The secure element of claim **17**, wherein the data exchange between the mobile communication device and the management server includes prompting a user to enter a payment limit personal identification number (PIN) in response to a purchase exceeding a pre-determined amount.

22. The secure element of claim **17**, wherein access to data associated with the data exchange is controlled.

23. The secure element of claim **22**, wherein access to the data is controlled by deleting cached data from the mobile communication device memory of the mobile communication device and from the secure element memory of the secure element.

24. The secure element of claim **22**, wherein access to the data is controlled by disabling the secure element.

25. The secure element of claim **17**, wherein the user is prompted for a personal identification number (PIN) by the mobile application before allowing the user to conduct a payment transaction.

26. The secure element of claim **17**, wherein the user is prompted for biometric data before allowing the user to conduct a payment transaction.

27. The secure element of claim **17**, wherein the user is prompted for multifactor authentication before allowing the user to conduct a payment transaction.

28. The secure element of claim **17**, wherein the secure element is permanently embedded within the body of the mobile communication device.

29. The secure element of claim **17**, wherein the secure element is affixed externally to the mobile communication device.

30. The secure element of claim **17**, wherein the secure element is removably embedded in a slot of the mobile communication device.

* * * * *