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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
21 March 2013 (21.03.2013)

WIPO | PCT

(10) International Publication Number
WO 2013/040605 A2

(51) International Patent Classification:
G06Q 20/16 (2012.01) *H04B 5/00* (2006.01)
G06Q 20/40 (2012.01)

(21) International Application Number:
PCT/US2012/055951

(22) International Filing Date:
18 September 2012 (18.09.2012)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
61/536,042 18 September 2011 (18.09.2011) US
13/361,343 30 January 2012 (30.01.2012) US

(71) Applicant *(for all designated States except US)*: **GOOGLE INC.** [US/US]; 1600 Amphitheatre Parkway, Mountain View, CA 94043 (US).

(72) Inventors; and
(71) Applicants *(for US only)*: **WALL, Jonathan** [US/US]; 461 2nd Street, #130, San Francisco, CA 94107 (US). **VON BEHREN, Rob** [US/US]; 1726 Martin Luther King Jr. Way, Berkeley, CA 94709 (US). **COLLINE, Raymond Emmett, II** [US/US]; 1257 Jenevein Avenue, San Bruno, CA 94066 (US).

(74) Agent: **ISAACS, William O., II**; Johnson, Marcou & Isaacs, LLC, 317A E. Liberty Street, Savannah, GA 31401 (US).

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

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

[Continued on next page]

(54) Title: ONE-CLICK OFFLINE BUYING

(57) Abstract: Contactless payment transactions are initiated through single input activation of a mobile device's secure element and contactless communication system. Activation of the secure element and the contactless communication system is coupled to the activation status of the mobile device's screen. Activation of the secure element may be further coupled to the activation status of an electronic wallet application. Where activation of the electronic wallet application is required, one-click activation of the electronic wallet application and secure element is provided.

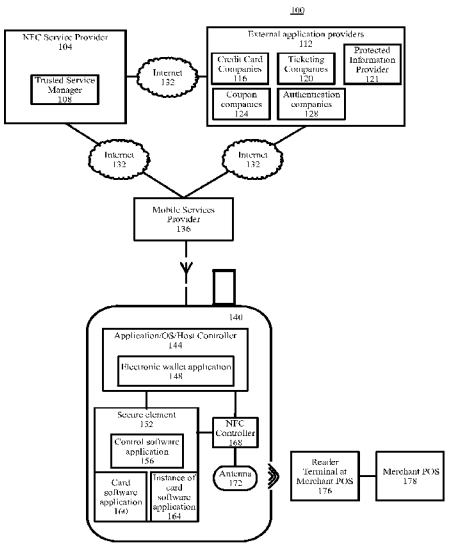

Fig. 1

WO 2013/040605 A2

Published:

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

ONE-CLICK OFFLINE BUYING

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This patent application claims priority to U.S. Patent Application No. 13/361,343, entitled, "One-Click Offline Buying" and filed January 30, 3012, which claims priority to U.S. Provisional Patent Application No. 61/536,042, entitled "One Click Offline Buying" and filed September 18, 2011. The complete disclosures of the above-identified priority applications are hereby fully incorporated herein by reference.

TECHNICAL FIELD

[0002] The invention relates generally to systems, methods, and devices for initiating a contactless payment transaction using a mobile device electronic wallet application, and, more particularly, to systems, methods, and devices whereby a user can use a single action to activate a mobile device secure element that is necessary to initiate a contactless payment transaction.

BACKGROUND

[0003] Contactless payment technology incorporates proximity communications between two devices to authenticate and enable payment for goods and services over the air (OTA) or without physical connection. Near Field Communication (NFC) is an example of a proximity communication option that can enable contactless payment technologies and that is supported by the Global System for Mobile Communications (GSM) Association. RFID is an example of a proximity communication method that can be adapted to enable NFC contactless payment technology. NFC communication distances generally range from about 3 to about 4 inches. Such short communication distances enable secure communication between close field proximity enabled devices. Proximity enabled contactless payment also can be implemented on Code Division Multiple Access (CDMA) devices with an embedded secure element within an NFC controller or a Re-usable Identification Module (R-UIM) type card.

[0004] Existing contactless payment technology is not integrated with NFC mobile device communication elements. As a result, a user must maneuver through multiple activating steps to initiate a payment transaction. For example, the mobile device must not only be turned "on" but must also be "active." A user must unlock their mobile device and

launch a contactless payment application, such as an electronic wallet application. Within the application the user must signal an intent to initiate a payment and enter security information such as a personal identification number. The user must also select a payment option, such as a particular credit card, to use in the payment transaction. The majority of these steps must be repeated for each payment transaction.

[0005] Accordingly, there is a need in the art for methods and systems that integrate contactless payment technology with the mobile device's contactless communication systems and streamline the process by which a user can securely initiate payment transactions.

SUMMARY

[0006] In certain exemplary embodiments, a computer-implemented method for initiating a contactless payment transaction using a single input activation of a mobile device's secure element comprises detecting the activation status of the mobile device's screen. The contactless communication system of the device is inactive while the device's screen is inactive. An exemplary contactless communication system may comprise an NFC controller and NFC antenna. Upon detection of screen activation, the contactless communication system is activated. In certain exemplary embodiments, the secure element may be also activated upon screen activation. In certain other exemplary embodiments, activation of the secure element may further require an active electronic wallet application. Where activation of the electronic wallet application is required, the electronic wallet application can be activated by a single-click input. The single-click input subsequently activates the secure element, identifies the default payment information, and prepares the default payment information for communication to a merchant reader terminal via the mobile device contactless communication system.

[0007] These and other aspects, objects, features, and advantages of the exemplary embodiments will become apparent to those having ordinary skill in the art upon consideration of the following detailed description of illustrated exemplary embodiments, which include the best mode of carrying out the invention as presently perceived.

BRIEF DESCRIPTION OF THE DRAWINGS

[0008] **FIG. 1** is a block diagram depicting systems for processing NFC payment transactions through single action activation of a mobile device secure element in an NFC communication system according to certain exemplary embodiments.

[0009] **FIG. 2** is a block flow diagram depicting a method for initiating a contactless payment transaction using a single input activation of a secure element in an NFC communication system according to certain exemplary embodiments.

[0010] **FIG. 3** is a block flow diagram depicting a method for initiating a contactless payment transaction through a single input activation of a secure element independent of NFC communication system activation according to certain exemplary embodiments.

[0011] **FIG. 4** is a block flow diagram depicting a method for activating a secure element in communication with an electronic wallet application using a single-click input according to certain exemplary embodiments.

DETAILED DESCRIPTION OF EXEMPLARY EMBODIMENTS

Overview

[0012] The methods, systems and devices described herein enable a user to initiate a contactless payment transaction through a single input activation of an electronic wallet application. The present invention integrates secure element activation of a contactless payment system with the contactless communication systems of a mobile device, such as an NFC controller and antenna, to allow secure and efficient initiation of contactless payment transactions. Default payment information is specified and stored within a secure element of the mobile device. Upon activation of the mobile device screen from a sleep or powered-down state, or in combination with one-click activation of the electronic wallet application, the secure element and contactless communication systems of the device are activated. Following secure element and contactless communication system activation, the device is prepared to communicate payment information stored in the secure element to a reader terminal connected to a merchant point of sale device. In certain exemplary embodiments, the wallet application remains active even after the mobile device goes dormant. In certain other exemplary embodiments, a user may configure how long the electronic wallet application remains active before timing out. By maintaining either the contactless communication system, or secure element, or both as inactive, the present invention maintains security and prevents the initiation of payment transactions or access to payment information without the user's consent. By integrating the activation of the mobile device's contactless communication systems and secure elements, the present invention can provide that when the user is ready to initiate a payment transaction, the user can do so efficiently.

[0013] One or more aspects of the invention may comprise a computer program that embodies the functions described and illustrated herein, wherein the computer program is implemented in a computer system that comprises instructions stored in a machine-readable medium and a processor that executes the instructions. However, it should be apparent that there could be many different ways of implementing the invention in computer programming, and the invention should not be construed as limited to any one set of computer program instructions. Further, a skilled programmer would be able to write such a computer program to implement an embodiment of the disclosed invention based on the appended flow charts and associated description in the application text. Therefore, disclosure of a particular set of program code instructions is not considered necessary for an adequate understanding of how to make and use the invention. Further, those skilled in the art will appreciate that one or more aspects of the invention described herein may be performed by hardware, software, or a combination thereof, as may be embodied in one or more computing systems. Moreover, any reference to an act being performed by a computer should not be construed as being performed by a single computer as the act may be performed by more than one computer. The inventive functionality of the invention will be explained in more detail in the following description, read in conjunction with the figures illustrating the program flow.

[0014] Turning now to the drawings, in which like numerals indicate like (but not necessarily identical) elements throughout the figures, exemplary embodiments are described in detail.

System Architecture

[0015] Fig. 1 is a block diagram depicting a system 100 for enabling single input activation of a mobile device secure element to process NFC payment transactions.

[0016] An external trusted service manager (TSM) 108 controlled by a near field communications (NFC) service provider 104 hosts and transmits card software applications for installation within the secure element 152 of a contactless smart card in mobile device 140. The NFC service provider 104 provides a secure key encrypted software card application for decryption and installation in the secure element 152. The TSM 108 includes a trusted service agent, which may be an automated software distribution entity within the TSM. In certain exemplary embodiments, the TSM may be accessible to the mobile device 140 via the Internet 132 directly, without the requirement of a mobile services provider 136 for the purpose of downloading trusted card software applications to the mobile device. The mobile services provider 136 provides card software applications in one of many mobile

services protocol, such as 3G and 4G. In certain exemplary embodiments, the TSM 108 may exist as a part of the mobile services provider 136.

[0017] In certain exemplary embodiments, external application providers 112 provide card software applications to the TSM 108 for deployment to the mobile device 140. In an alternative embodiment, each of the external application providers 112 may include a TSM for providing trusted card software applications directly to the mobile device via the Internet 132 or the mobile service provider 136. Exemplary external application providers 112 include credit card companies 116 for providing credit card type payment card software applications, such as Java credit/debit/PayWave/PayPass type applets, ticketing companies 120 for providing tickets to events, travel, and other related functions, coupon companies 124 for providing coupons that are downloaded and scan-able at a point-of-sale (POS) using the contactless smart card, RFID tags, barcodes, QR 2 dimensional bar codes, and other similar optical coding methods, an authentication company 128 for providing authentication data that may be used to lock/unlock physical appliances or for virtual functions on computer software, and a protected information provider 121, such as a bank, merchant, or other financial service provider, for providing confidential or otherwise protected information (for example, account information), which may be used to instantiate a particular card.

[0018] In certain exemplary embodiments, an application host OS 144 on the mobile device 140 provides the user of the mobile device with the capability to manage multiple card software application instances 160-164 using a wallet software application 148, where the wallet software application does not need TSM 108 permission to perform certain functions on each of the card software application instances 160-164. The management of the card software applications may be performed via a control software application 156, which communicates with the wallet software application 148 using APDUs, transmitted and received, through a secure and encrypted communication channel. The control software application 156 may freely communicate with the multiple card software application instances 160-164 because each of the card instances 160-164 and the control software application 156 are resident within the same secure element 152. Alternatively, multiple secure elements providing secure communication channels can provide the same functionality as disclosed herein. The user may engage the control software application 156 using commands to activate, deactivate, prioritize, delete, and install card software applications 160-164 within the secure element.

[0019] When the default card software application has been activated according to the methods of the present invention, the NFC controller 168 is notified of the state of readiness of the mobile device 140 for an NFC transaction. The NFC controller polls, through the antenna 172, a radio signal, or listens for radio signals from a reader terminal device 176. On establishing a channel between the devices 172 and 176, the reader requests to see the list of available card software applications within the secure element 156. Default payment information is then transmitted from the application 160-164 set as the default payment option to the reader terminal and the transaction is initiated.

System Process

[0020] Fig. 2 is a block flow diagram depicting a method 200 for using a single input activation of a mobile device screen to activate a secure element and NFC antenna to process a contactless payment transaction. The method 200 is described with reference to the components illustrated in Figure 1.

[0021] At block 205, the electronic wallet application 148 receives input of default payment information from a user of the mobile device via a user interface generated by the electronic wallet application 148, and communicates the input to the control software application 156 on the secure element 152. The control software application 156 prioritizes the card software applications 160-164 according to the input received from the electronic wallet application 148. Alternatively, default payment information may be communicated to the device via the Internet 132, mobile services provider 136, or other suitable communication network.

[0022] In an exemplary embodiment, the wallet application 148 can operate continuously after being activated.

[0023] At block 210, the method 200 determines whether the screen of the device 140 is active. In this embodiment, the secure element 152 is inactive if the mobile device screen is inactive. In an inactive state, the secure element 152 can neither receive nor communicate payment information through the mobile device contactless communication system, such as the NFC controller 168 and antenna 172. Upon screen activation, the host controller 144 detects a change in the screen activation status and communicates the change in screen status to the control software application 156 of the secure element 152 and the NFC controller 168. In an exemplary embodiment, the host controller 144 communicates the screen activation status to the wallet application 148, which communicates the screen activation status to the control software application 156 of the secure element 152.

[0024] A mobile device screen is "active" or "activated" when powered on and displaying a default home user interface. A screen may become active, for example, by response to direct user input, from the detection of movements that would indicate the user is preparing to use the device, or from the detection of voice commands.

[0025] If the screen is active, the method 200 proceeds to block 215.

[0026] At block 215, the secure element 152 and the NFC controller 168 receive the communication indicating a change in the mobile device screen's activation status. The NFC controller 168 is configured so that the antenna 172 is inactive when the screen is inactive. Accordingly, the antenna 172 will become active and inactive in sync with subsequent communications to the NFC controller 168 indicating the mobile device screen's activation status.

[0027] The secure element 152 can neither receive nor transmit data until activated. In an exemplary embodiment, the wallet application 148 can operate continuously after being activated by the user, even when the screen is not active. In this state, the wallet application 148 remains active in the background, awaiting the screen activation status. After receiving the screen activation status from the host controller 144, the wallet application 148 can activate the secure element 152 for an NFC payment transaction. Accordingly, the secure element 152 will become active and inactive in sync with subsequent communications indicating the mobile device screen's activation status.

[0028] At block 220, the NFC controller 168 polls, through the antenna 172, a radio signal, or listens for radio signals from a point of sale reader terminal device 176. If a radio signal is not detected, the method 200 returns to block 210 and continues to monitor. If the screen remains active, there is no change in status communicated to the NFC controller 168 or the secure element 152 at block 215. Once the screen goes inactive, the change in screen status is communicated to the NFC controller 168 and the secure element 152 following the same procedure discussed in block 215, and the antenna 172 and the secure element 152 are deactivated.

[0029] Referring back to step 220, while active, if the antenna 172 detects a reader terminal communication field, the method proceeds to block 225.

[0030] At block 225, data received from the reader terminal 176 at the antenna 172 is communicated to the control software application 156. The control software application 156 accesses the default payment information stored on the secure element 152 and prepares the payment information for communication to the reader terminal 176. Multiple forms of

payment information can be stored in the secure element 152. The control software application 156 will select the payment information identified in block 205 as the default payment information for processing the transaction. The user can change or modify the default payment information at their discretion using the electronic wallet application 148.

[0031] At block 230, the control software application 156 communicates the default payment information to the reader terminal 176 via the NFC antenna 172. The default payment information is received at the reader terminal 176 and further processed by the merchant POS device 178.

[0032] At block 235 the mobile device 140 waits to receive payment confirmation via the terminal reader 176 from the merchant POS device 178. The payment confirmation may be monitored by the secure element 152. Upon receipt of payment confirmation from the merchant POS 178, the secure element 152 communicates the payment confirmation to the electronic wallet application 148. The electronic wallet application 148 then notifies the user of the payment confirmation via the user interface generated by the wallet application (see block 245).

[0033] Alternatively, the payment confirmation may be monitored directly by the electronic wallet application 148. The control software application 156 can notify the electronic wallet application 148 of the communication of payment information to the merchant POS 178, prompting the electronic wallet application 148 to monitor for receipt of the payment confirmation from the merchant POS 178.

[0034] If the payment is not confirmed at block 235, the method proceeds to block 240. At block 240, the wallet application 148 generates a notification indicating the payment transaction was not completed and communicates the notice to the user via the user interface generated by the electronic wallet application 148. In certain exemplary embodiments, the electronic wallet application 148 may present to the user the option of selecting an existing account or entering new payment account information to use as the default payment information. The process then returns to block 210 to repeat the method 200 as necessary.

[0035] Referring back to block 235, if the payment is confirmed, the method 200 proceeds to block 245. At block 245, the electronic wallet application 148 generates a payment confirmation notice and communicates the notice to the user via the user interface generated by the wallet application 148. A payment notification may include transaction details such as the details included on standard paper receipts. In an exemplary embodiment,

the payment notification may be a replication of a receipt or receipt information received from the merchant POS system 178.

[0036] The payment notifications may be stored by the wallet software application 148 on the mobile device 140, and/or communicated to a separate device, such as a personal cloud server or other central server or a personal computer of the user. For example, the user may review receipt information via the user interface generated by the wallet application 148, and/or receipt information may be used by another system to identify user preferences.

[0037] From block 245, the method 200 returns to block 210 to determine whether the screen is still active. If the screen is inactive, the NFC antenna 172 is deactivated by the NFC controller 168. If the screen is still active, the NFC antenna 172 remains active and ready to detect additional reader terminal 176 radio signals and to initiate subsequent payment transactions.

[0038] Figure 3 is a block flow diagram depicting a method 300 for using a one-click input to activate a secure element 152 to process a payment transaction where activation of the secure element is independent of NFC communication system activation. The method 300 is described with reference to the components illustrated in Figure 1.

[0039] In certain exemplary embodiments, the NFC antenna 172 is activated prior to activation of the secure element 152.

[0040] The first two blocks of method 300 proceed as described previously with reference to blocks 205 and 210 of Figure 2.

[0041] At block 315, the NFC controller 168 receives the communication indicating a change in the screen activation status and changes the activation status of the antenna 172 accordingly. The NFC controller 168 is configured so that the antenna 172 is inactive when the screen is inactive. Accordingly, the antenna 172 will become active and inactive in sync with subsequent communications to the NFC controller 168 indicating the mobile device screen's activation status.

[0042] At block 320, the secure element 152 is activated and the default payment information is configured for a contactless payment transaction via a single click command. Block 320 will be described in further detail hereinafter with reference to Figure 4.

[0043] Figure 4 is a block flow diagram depicting the method 320 for activating, using a one-click input, the secure element 152 to access the default payment information for a contactless payment transaction. Thus, Figure 4 describes the process 320 by which a one-

click input is utilized to activate the secure element 152 to allow processing of an NFC payment transaction according to an exemplary embodiment.

[0044] At block 405, the electronic wallet application 148 receives a one-click input and communicates the input to the secure element 152. In certain exemplary embodiments, the one-click input comprises a physical tap, a voice command, selection by the user of a defined control on the user interface generated by the electronic wallet application 148, activation of a defined button on the contactless device 140, activated of a motion gesture that is detected by a gyroscope or other motion-detecting mechanism of the contactless device 140 (for example, a shake, double shake, "fishing," or other motion of the contactless device 140). The wallet application 148 detects the user input of the command to ready the secure element 152 for a contactless payment transaction and communicates the command to the secure element 152.

[0045] At block 410, the control software application 156 of the secure element 152 receives the one-click input communication from the electronic wallet application 148 and activates the secure element 152 to make the default payment information accessible. In this case, activation means that the secure element 152 is able to communicate with a reader terminal for a contactless payment transaction.

[0046] At block 415, the control software application 156 identifies the default payment information stored in the secure element 152. Multiple forms of payment information can be stored in the secure element 152. The control software application 156 will select the payment information identified in block 205 of Figure 3 as the default payment information for processing the transaction. The user can change or modify the default payment information at their discretion using the electronic wallet application 148.

[0047] At block 420, the control software application 156 prepares the default payment information for communication to the NFC antenna 172. Preparation of the default payment information can comprise the identification of the default payment information that can be communicated in the payment transaction. Alternatively or additionally, preparation of the default payment information can include encrypting the payment information for secure transmission to a reader terminal. The control software communication module 156 will not communicate the payment information to the NFC antenna 172 until the NFC controller 168 indicates the NFC antenna 172 has detected a reader terminal 176 radio signal.

[0048] The method 320 then proceeds to block 325 of Figure 3.

[0049] Returning to Figure 3, at block 325, the NFC controller 168 polls, through the antenna 172, a radio signal, or listens for radio signals from a reader terminal device 176. If no radio signal is detected, the method 300 proceeds to block 330 to determine if an time-out period for activation of the secure element has expired. In certain exemplary embodiments, the time-out period could be based on a time-out period for the wallet application 148. In certain exemplary embodiments, when the electronic wallet application times-out period expires, a personal identification number, password, or other authentication must be entered to unlock the application. The electronic wallet application time-out period can be configured through settings of the electronic wallet application 148. If the time-out period has not expired, the NFC controller 168 will maintain the NFC antenna 172 in an active state. If no reader terminal 176 radio signal is detected within the time-out period, the method 300 returns to block 320 and reactivation of the secure element 152 is required.

[0050] Referring back to block 325, if a radio signal is detected at block 325, the subsequent steps of communicating the default payment information to a merchant point of sale device via the NFC antenna 172, confirming payment, notifying user payment transaction is complete or not complete, and generating a payment confirmation and displaying the confirmation via the wallet software application 148 interface, proceeds as described previously with reference to blocks 230-245 of Figure 2, respectively.

[0051] The wallet application 146 in conjunction with the secure element 152 can accommodate multiple payment methods. Within the secure element 152, multiple credit cards, debit cards, and/or other forms of secure payment can be stored. The user can select a particular one of the payment forms as the default payment method. Additionally, the wallet application 148 can store and process unsecure payment forms, such as coupons, loyalty cards, check-ins, membership cards, gift cards, and other forms of value-added services. The wallet application 148 can communicate these payment forms to the reader terminal 176 via the antenna 172 for application during the payment transaction.

[0052] In exemplary embodiments, a payment transaction can comprise one or more payment or other value transactions, all conducted within a single tap of the contactless payment device 140 with the reader terminal 176.

[0053] Exemplary value added services can be embodied in one or more value added applications residing on the device 140 and/or within the secure element 126. Value added applications can perform functionality to redeem the value added services.

[0054] For example, a value added coupon application can automatically redeem coupons stored in the value added coupon application. More specifically, a user may save one or more coupons (or other "offers") to the value added service coupon application on the contactless device 140. When the default payment information communication is performed in block 230, the value added coupon can be applied to the transaction. For example, the value added coupon application can search stored coupons that can be applied to the current transaction. This determination can be based on an identity of the merchant operating the POS system 178 and products being purchased, as provided by the device reader 176 to the device 140. Alternatively, or additionally, merchant information can be determined by the value added coupon application based on geocode information available to the device 140 by comparing the geocode information for the current location of the device 140 with known merchant locations. After identifying coupons that can apply to the merchant or products, the value added coupon application communicates the coupon(s) to the device reader 176 via the antenna 172. Thereafter, the POS system 178 processes the coupon for the transaction. If multiple coupons apply to the transaction, the value added service application can determine which coupon offers the greatest value and/or which combination of coupons offers the greatest value and can automatically apply the greatest value choice.

[0055] As another example, a value added loyalty application can automatically collect and redeem loyalty rewards. More specifically, a user may install a loyalty application for a particular merchant (or a loyalty application that operates for multiple merchants). Each time a transaction is conducted with the merchant, the value added loyalty application collects loyalty rewards (for example, points, number of visits, number of items purchased, or other suitable reward). Then, when sufficient loyalty rewards have been collected to redeem for value, the value added loyalty application can automatically apply the redemption. For example, when default payment information communication is performed in block 230, the value added loyalty rewards can be accumulated and/or applied to the transaction. For example, the value added loyalty application can search accumulated rewards that can be applied to the current transaction. This determination can be based on an identity of the merchant and products being purchased, as provided by the device reader 176 to the device 140. Alternatively, or additionally, merchant information can be determined by the value added loyalty application based on geocode information available to the contactless device 140 by comparing the geocode information for the current location of the device 140 with known merchant locations. After identifying loyalty rewards that can be redeemed for the

merchant or products, the value added loyalty application communicates the loyalty reward(s) to the device reader 176 via the antenna 172. Thereafter, the POS system 178 processes the loyalty rewards for the transaction. If loyalty rewards are not available for redemption, the value added loyalty application communicates a request to accumulate loyalty rewards to the device reader 176 via the antenna 172. Thereafter, the POS system 178 processes the transaction and communicates the loyalty rewards for the transaction from the device reader 176 to the contactless device 140. The value added loyalty application increments the stored loyalty rewards accordingly for future redemption.

[0056] Other value added applications can be implemented in a similar manner, for example, check-ins, membership cards, gift cards, and other forms of value-added services. Corresponding value added service applications can function to determine whether the particular service applies to the transaction (for example, to the merchant or the product) and to apply the service to the transaction if appropriate. For instance, a gift card having value stored thereon can be applied to the transaction.

[0057] In this manner, multiple value added services can be applied in blocks 230 and 235. The wallet application 148 can process each available value added service application to thereby apply all available value added services to the transaction. Additionally, if multiple value added services apply to the transaction, the application 148 can determine which service offers the greatest value and/or which combination of services offers the greatest value and can automatically apply the greatest value choice. Furthermore, after application of all value added services, the POS system 178 charges the remaining balance to the default payment method through a secure payment transaction with the secure element 152. All of the transactions can be processed via a single tap of the device 140 to the reader terminal 176.

[0058] The payment confirmation generated in block 245 can identify all items applied to the transaction. For example, the payment confirmation can identify each coupon, loyalty redemption, stored value card, other value added service, and all secure payment forms applied to the transaction, and may also show items included in the transaction (for example, ticket numbers for tickets purchased). In an exemplary embodiment, a single payment confirmation may show all items applied to the transaction. Alternatively, multiple payment confirmations may be provided, wherein each receipt is for a particular one of the items applied to the transaction.

General

[0059] The exemplary systems, methods, and blocks described in the embodiments presented previously are illustrative, and, in alternative embodiments, certain blocks can be performed in a different order, in parallel with one another, omitted entirely, and/or combined between different exemplary methods, and/or certain additional blocks can be performed, without departing from the scope and spirit of the invention. Accordingly, such alternative embodiments are included in the invention described herein.

[0060] The invention can be used with computer hardware and software that performs the methods and processing functions described herein. As will be appreciated by those having ordinary skill in the art, the systems, methods, and procedures described herein can be embodied in a programmable computer, computer executable software, or digital circuitry. The software can be stored on computer readable media. For example, computer readable media can include a floppy disk, RAM, ROM, hard disk, removable media, flash memory, memory stick, optical media, magneto-optical media, CD-ROM, etc. Digital circuitry can include integrated circuits, gate arrays, building block logic, field programmable gate arrays ("FPGA"), etc.

[0061] Although specific embodiments have been described above in detail, the description is merely for purposes of illustration. It should be appreciated, therefore, that many aspects described above are not intended as required or essential elements unless explicitly stated otherwise. Various modifications of, and equivalent acts corresponding to, the disclosed aspects of the exemplary embodiments, in addition to those described above, can be made by a person of ordinary skill in the art, having the benefit of the present disclosure, without departing from the spirit and scope of the invention defined in the following claims, the scope of which is to be accorded the broadest interpretation so as to encompass such modifications and equivalent structures.

CLAIMS

What is claimed is:

1. A computer-implemented method for initiating a mobile computing device contactless payment transaction, comprising:

detecting, by the mobile device, a screen activation status of the mobile device;

activating, by the mobile device, a contactless communication system of the mobile device and a secure element of the mobile device in response to detecting that the screen activation status is active;

detecting, by the mobile device, a contactless communication reader terminal signal;

establishing, by the mobile device, a contactless communication session with the reader terminal in response to detecting the contactless communication reader terminal signal;

receiving, by the mobile device, information to conduct the payment transaction from the reader terminal; and

communicating, by the contactless communication system of the mobile device, default payment information stored in the secure element of the mobile device to the reader terminal in response to receiving the information to conduct the payment transaction.

2. The method of claim 1, wherein the contactless communication system of the mobile device comprises a near field communication (NFC) controller and antenna.

3. The method of claim 1, wherein the screen activation status of the mobile device is active when powered on and displaying a default home user interface.

4. The method of claim 1, wherein detecting a screen activation status comprises detecting at least one of a direct user input, a movement indicating a user is preparing to use the device, and a voice command.

5. The method of claim 1, wherein detecting the reader terminal signal comprises one of actively or passively detecting the reader terminal radio signal.

6. The method of claim 1, wherein communicating the default payment information is controlled by a control software application module of the secure element.

7. The method of claim 1, further comprising:

receiving, by the mobile device, a one-click input;

activating, by the mobile device, the secure element, wherein activation of the secure element provides access to payment information stored in the secure element;

identifying, by the mobile device, the default payment information stored in the secure element; and

preparing, by the mobile device, the default payment information for communication to the reader terminal.

8. A computer-implemented method for initiating a mobile device contactless payment transaction, comprising:

detecting, by the mobile device, a screen activation status of the mobile device;

detecting, by the mobile device, a contactless communication system activation status of the mobile device;

activating, by the mobile device, a secure element of the mobile device in response to detecting that the mobile device screen and the contactless communication system is active, wherein default payment information is stored in the secure element;

detecting, by the contactless communication system of the mobile device, a signal from a reader terminal; and

communicating, by contactless communication system of the mobile device, the default payment information stored in the secure element of the mobile device to the reader terminal in response to detecting the reader terminal signal.

9. The method of claim 8, wherein activating the secure element comprises:

receiving, by the mobile device, a one-click input;

activating, by the mobile device, the secure element, wherein activation of the secure element provides access to payment information stored in the secure element;

identifying, by the mobile device, the default payment information stored in the secure element; and

preparing, by the mobile device, the default payment information for communication to the reader terminal.

10. The method of claim 9, wherein the one-click input comprises a physical tap, a voice command, selection of a user interface control, selection of a control of the mobile device, or a movement gesture of the mobile device.

11. The method of claim 9, wherein identifying and preparing the default payment information is controlled by a control software application module of the secure element.

12. The method of claim 8, wherein the contactless communication system comprises a near field communication (NFC) controller and antenna.

13. The method of claim 8, wherein the screen activation status of the mobile device is active when powered on and displaying a default home user interface.

14. The method of claim 8, wherein detecting a screen activation status comprises detecting at least one of a direct user input, a movement indicating a user is preparing to use the device, and a voice command.

15. The method of claim 8, wherein detecting the reader terminal radio signal comprises one of actively or passively detecting the reader terminal radio signal.

16. A computer program product, comprising:

a non-transitory computer readable medium having computer-readable program code embodied therein for activating a secure element of a mobile device, the computer-readable medium comprising:

computer-readable program code for receiving a one-click input, wherein the one-click input initiates a contactless payment transaction using default payment information stored in the secure element of the mobile device;

computer-readable program code for communicating the one-click input to the secure element, wherein receipt of the communication by a control software application of the secure element activates the secure element;

computer-readable program code for identifying the default payment information stored in the secure element; and

computer-readable program code for preparing the default payment information for communication by the mobile device to a terminal reader.

17. The computer program product of claim 16, further comprising computer-readable program code for communicating the default payment information from the secure element to a contactless communication system of the mobile device.

18. The computer program product of claim 17, wherein the contactless communication system of the mobile device comprises a near field communication (NFC) controller and antenna.

19. The computer program product of claim 16, wherein the one-click input is a physical tap, a voice command, selection of a user interface control, selection of a control of the mobile device, or a movement gesture of the mobile device.

20. The computer program product of claim 16, wherein the secure element comprises the control software application and at least one card software application, wherein the default payment information is stored in the at least one card software application, and wherein the control software application identifies the default payment information in the at least one card software application.

21. A system for processing mobile device contactless payment transactions, comprising:

a mobile device comprising an electronic wallet application, a secure element, and a contactless communication system; and

a processor communicatively coupled to the electronic wallet application, the secure element, and the mobile device controller, wherein the processor executes application code instructions that are stored in the mobile device controller to

detect a screen activation status of the mobile device screen;

activate the contactless communication system when the screen activation status is active;

activate the secure element when the screen activation status is active;

detect a contactless communication signal of a reader terminal;

access default payment information stored in the secure element; and

communicate, via the contactless communication system, the default payment information to the reader terminal.

22. The system of claim 21, wherein activating the secure element comprises receiving a one-click electronic wallet application input.

23. The system of claim 21, wherein the contactless communication system comprises a near field communication (NFC) controller and antenna.

24. The system of claim 21, wherein detecting the reader terminal signal comprises actively or passively detecting the reader terminal radio signal.

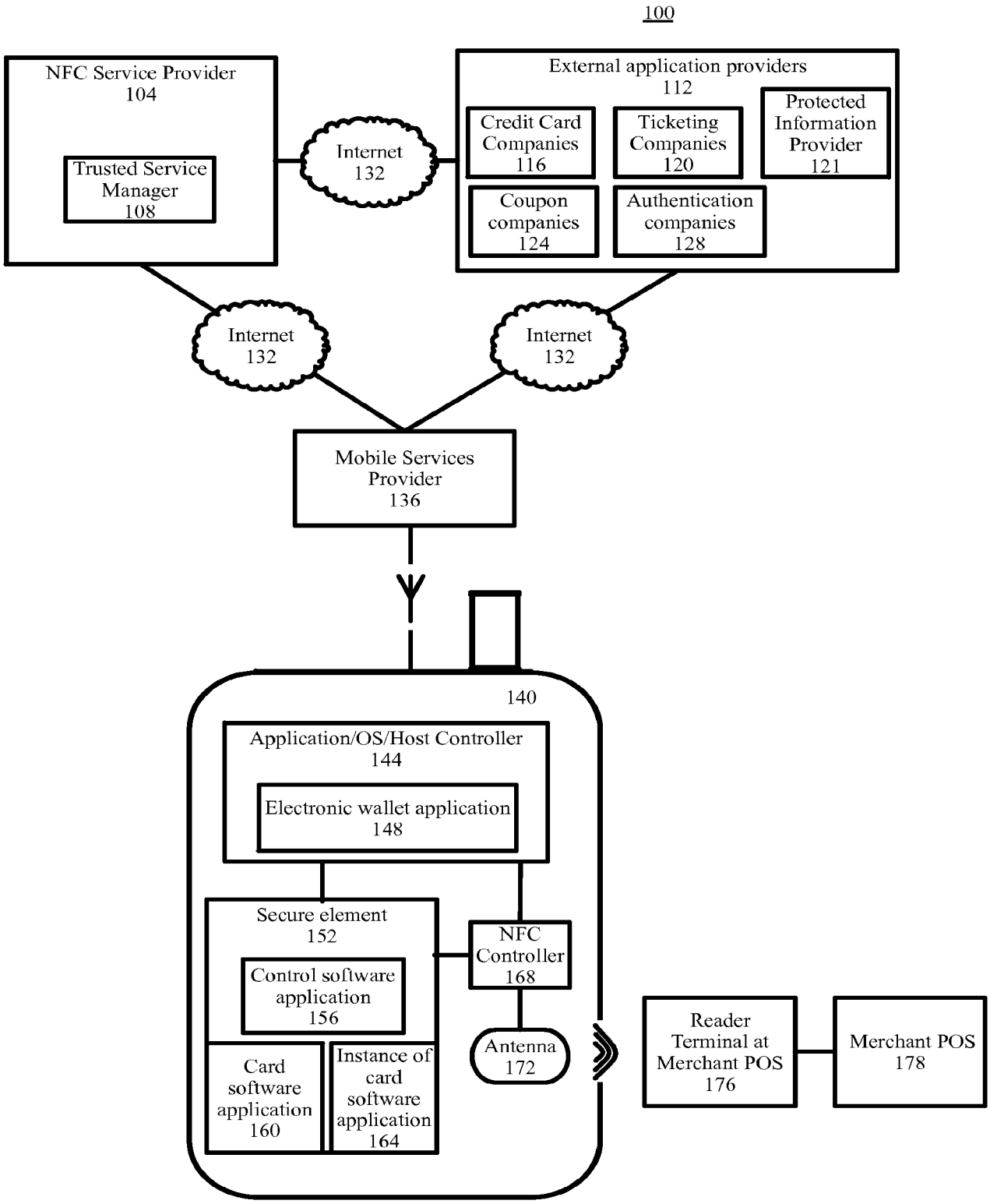
100
NFC Service Provider
104
Trusted Service Manager
108
Internet
132
External application providers
112
Credit Card Companies
116
Ticketing Companies
120
Protected Information Provider
121
Coupon companies
124
Authentication companies
128
Internet
132
Internet
132
Mobile Services Provider
136
140
Application/OS/Host Controller
144
Electronic wallet application
148
Secure element
152
Control software application
156
Card software application
160
Instance of card software application
164
NFC Controller
168
Antenna
172
Reader Terminal at Merchant POS
176
Merchant POS
178

Fig. 1

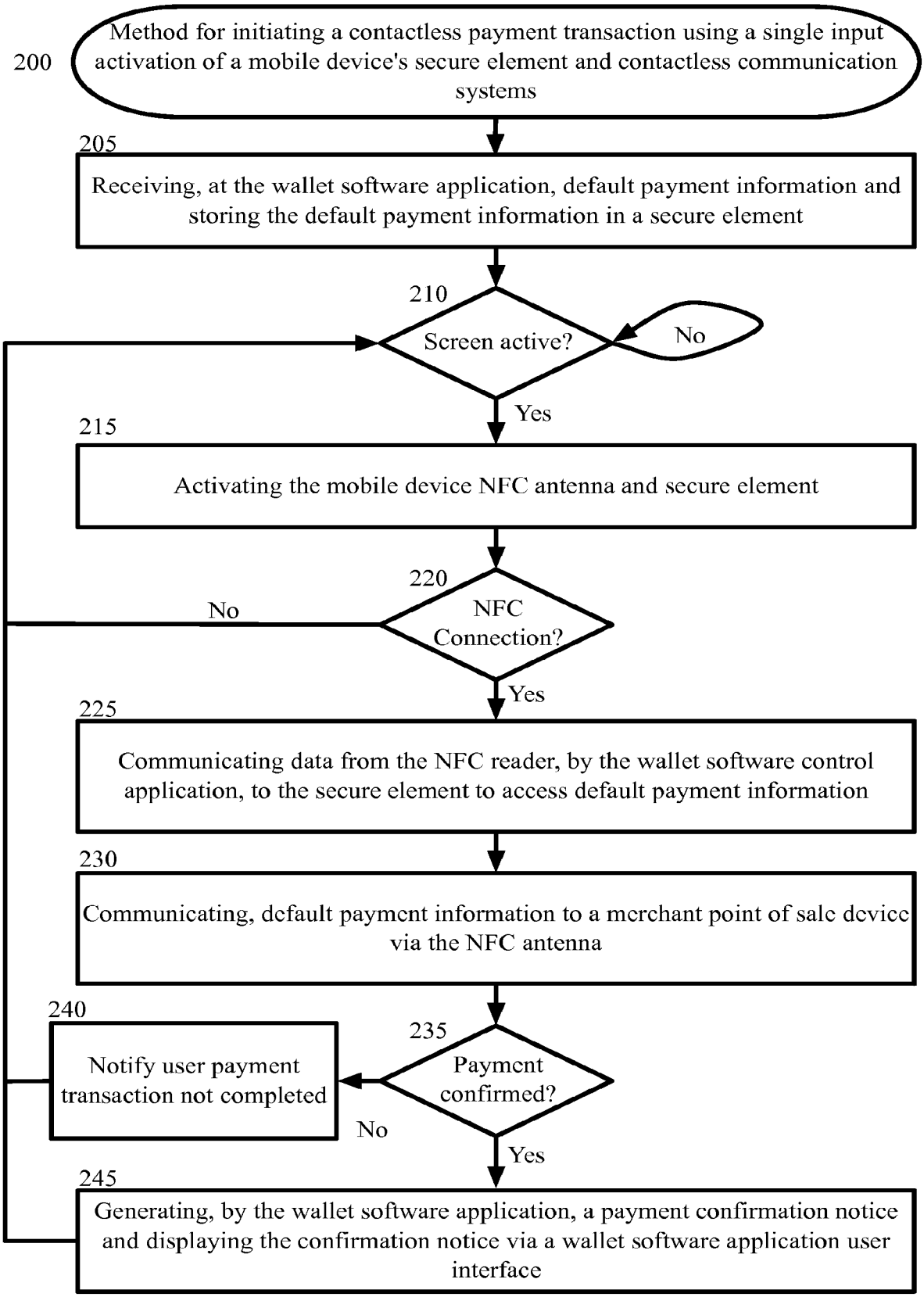
200
Method for initiating a contactless payment transaction using a single input activation of a mobile device's secure element and contactless communication systems
205
Receiving, at the wallet software application, default payment information and storing the default payment information in a secure element
210
Screen active?
No
Yes
215
Activating the mobile device NFC antenna and secure element
220
NFC Connection?
No
Yes
225
Communicating data from the NFC reader, by the wallet software control application, to the secure element to access default payment information
230
Communicating, default payment information to a merchant point of sale device via the NFC antenna
235
Payment confirmed?
No
Yes
240
Notify user payment transaction not completed
245
Generating, by the wallet software application, a payment confirmation notice and displaying the confirmation notice via a wallet software application user interface

Fig. 2

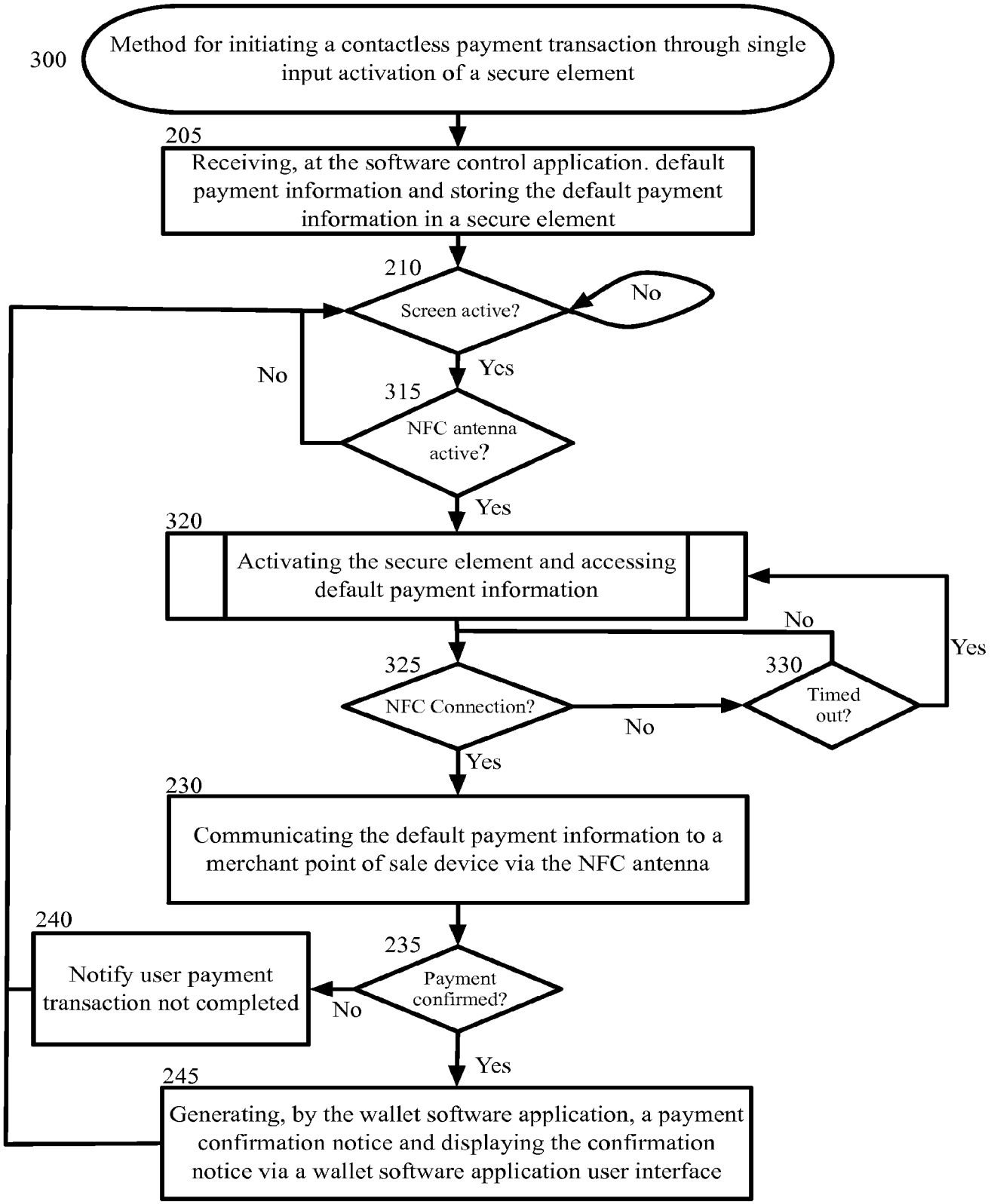
300
Method for initiating a contactless payment transaction through single input activation of a secure element
205
Receiving, at the software control application. default payment information and storing the default payment information in a secure element
210
Screen active?
No
Yes
No
315
NFC antenna active?
Yes
320
Activating the secure element and accessing default payment information
No
Yes
325
NFC Connection?
No
330
Timed out?
Yes
230
Communicating the default payment information to a merchant point of sale device via the NFC antenna
240
Notify user payment transaction not completed
235
Payment confirmed?
No
Yes
245
Generating, by the wallet software application, a payment confirmation notice and displaying the confirmation notice via a wallet software application user interface

Fig. 3

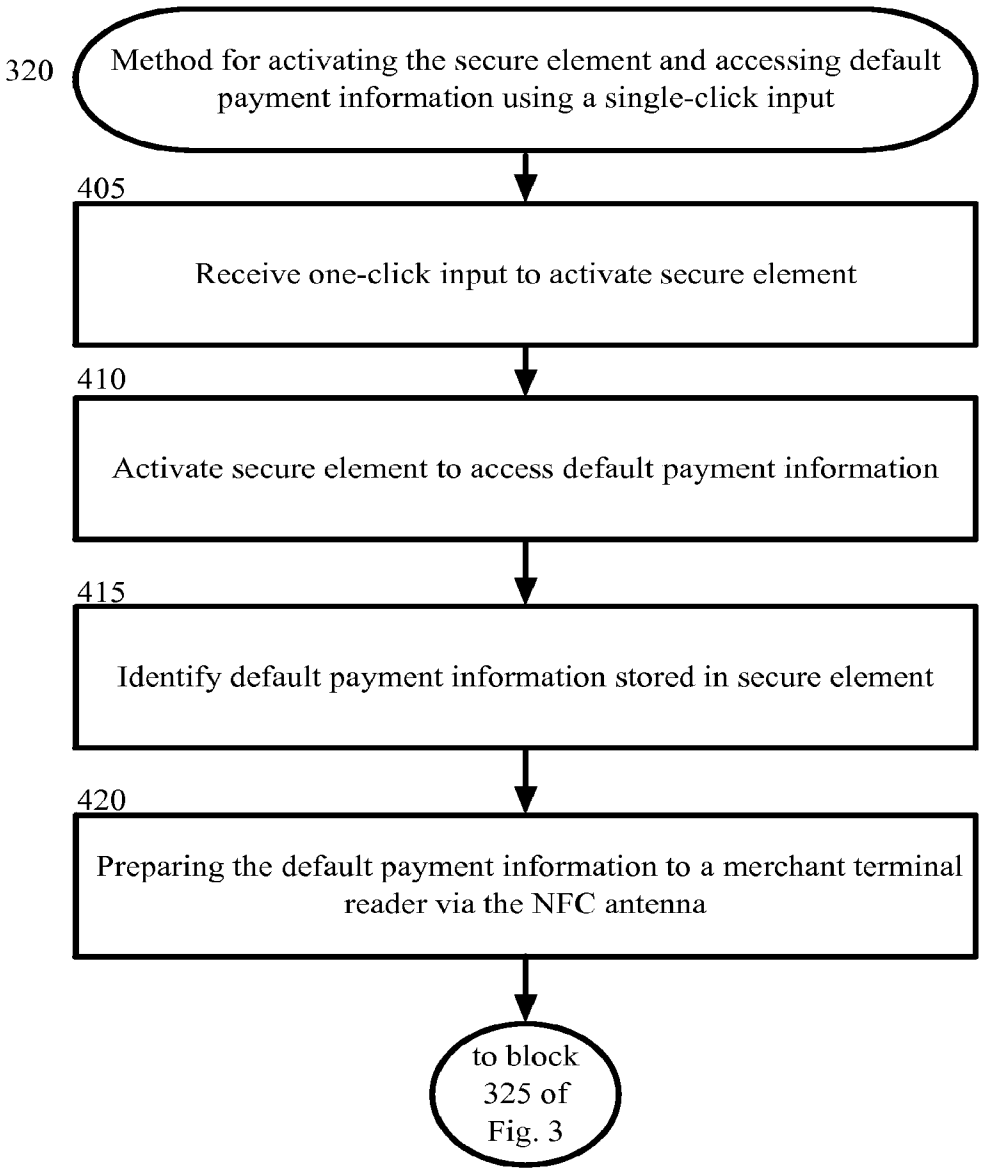
320
Method for activating the secure element and accessing default payment information using a single-click input
405
Receive one-click input to activate secure element
410
Activate secure element to access default payment information
415
Identify default payment information stored in secure element
420
Preparing the default payment information to a merchant terminal reader via the NFC antenna
to block 325 of Fig. 3

Fig. 4