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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
5 April 2012 (05.04.2012)

PCT

(10) International Publication Number
WO 2012/042262 A1

(51) International Patent Classification:
G06Q 20/00 (2012.01)

(21) International Application Number:
PCT/GB2011/051839

(22) International Filing Date:
28 September 2011 (28.09.2011)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

12/891,866	28 September 2010 (28.09.2010)	US
12/905,419	15 October 2010 (15.10.2010)	US
12/955,326	29 November 2010 (29.11.2010)	US
12/955,373	29 November 2010 (29.11.2010)	US
13/100,610	4 May 2011 (04.05.2011)	US
13/225,898	6 September 2011 (06.09.2011)	US
13/247,352	28 September 2011 (28.09.2011)	US

(71) Applicant *(for all designated States except US)*: **BARCLAYS BANK PLC** [GB/GB]; 29th Floor, One Churchill Place, London, Greater London, E14 5HP (GB).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **BAUER, John** [US/US]; 1310 New Virginia Road, Downingtown, Pennsylvania 19335 (US). **MCMILLEN, Glenn Curtiss** [US/US]; 1379 Pennsridge Place, Downingtown, Pennsylvania 19335 (US). **CROZIER, Eric** [US/US]; 600 Parkridge Drive, Hockessin, Delaware 19707 (US). **SCHUETZ, Christine Ann** [US/US]; 250 Kennett Pike, Chadds Ford, Pennsylvania 19317 (US). **LLOYD, Garry** [GB/GB]; Merry Marshes, Stable Lane, Moulton Road, Pitsford, Northamptonshire NN6 9AU (GB). **CRAKE, David, A.** [US/US]; 13 Latour Lane, Newark, Delaware 19702 (US). **AKANA, Thomas, P.** [US/US]; 22 Letchworth Lane, Avondale, Pennsylvania 19311 (US). **BARTON, Loren** [GB/GB]; 67 Becmead Avenue, London, Greater London SW16 1UJ (GB). **ROMAGNOLI, Amy Sobocinski** [US/US]; 18 Lotus Circle North, Bear, Delaware 19701 (US). **STARCK, Mike** [US/US]; 228 Hansell Road, Newtown Square, Pennsylvania 19073 (US). **MESA, Patrick** [US/US]; 2436 W. Colonial Drive, Boothwyn, Pennsylvania 19061 (US). **MOORE, Leslie** [US/US]; 2102 Swinnen Drive, Wilmington, Delaware 19810 (US).

(74) Agent: **CROSS, James**; 26 Caxton Street, London, Greater London SW1H 0RJ (GB).

(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, 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,

[Continued on next page]

(54) Title: MOBILE PAYMENT SYSTEM

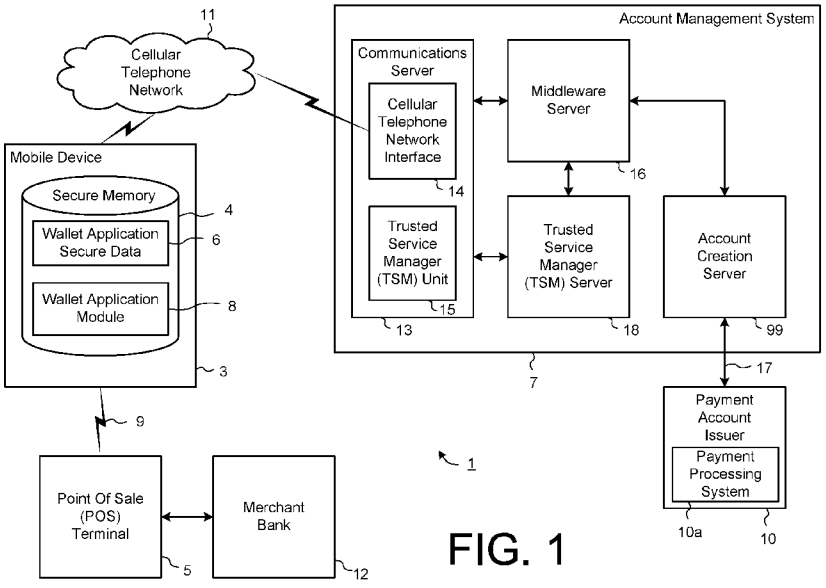


FIG. 1

(57) Abstract: A mobile payment system and methods are described for providing, validating, authorizing, activating and using a mobile payment account on a portable electronic device to enable efficient and secured contactless payment at an electronic point of sale.

WO 2012/042262 A1

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, 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, MD, 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).

Published:

— *with international search report (Art. 21(3))*

Mobile Payment System

Field of the Invention

[0001] This invention relates to a mobile payment account system, and more particularly to aspects of the system including providing, validating, authorizing, activating and using a mobile payment account on a mobile device to enable efficient and secured contactless payment at an electronic point of sale.

Background of the Invention

[0002] Mobile payment account systems are generally known, in which portable electronic devices are configured to provide payment from an electronic wallet. Typically, these portable electronic devices are configured to enable a contactless communication with a merchant Point Of Sale (POS) terminal to carry out a payment transaction, for example using near field communication (NFC) technology.

[0003] Such conventional mobile payment systems typically involve a complicated process for provisioning a mobile payment account on the portable electronic device. Customers expect a certain degree of security and peace of mind that their sensitive identification and account details are protected from theft, and therefore known account provisioning systems involve a time consuming activation process which often requires the customer to, for example, post in a copy of documents to verify their identity, telephone the account issuer to provide verbal confirmation of their identity, or login to a website to complete a lengthy authentication process. This results in significant delays between a customer requesting a new mobile payment account and the time when the mobile account is actually provisioned and ready for use to carry out payment transactions.

[0004] Conventional mobile payment systems typically involve a complicated process in order for a user to effect a secured payment transaction from an electronic wallet. For example, US 7,707,113 to Sprint Communications Company L.P. discusses a method of a portable electronic device providing payment from an electronic wallet with different levels of security. In a first level of security, the method prompts for input of a personal identification number (PIN) after the wallet has been opened and

providing payment from the wallet after receiving the PIN. However, in another level of security, no PIN is required thus enabling efficient but unsecured payment transactions to be made from the electronic wallet.

[0005] Additionally, when customers use such a payment product to conduct low dollar transactions over contactless interfaces, a signature may not be required at the point of sale, nor a challenge for a numeric passcode (PIN) or a password. In the United States for example, customers are able to wave their payment device and authorize the payment transaction without further interaction. For any theft of payment devices, the liability for these low dollar swipe transactions is placed upon the issuing bank, not the customer and not the merchant.

[0006] For payment accounts residing on mobile devices such as contactless payment capable mobile phones, the theft of a phone now becomes immediately available for low dollar purchases without consumer verification prior to a purchase. The perpetrator can make as many low dollar transactions without being challenged for authentication and access the payment account. All of these low dollar transactions will be the responsibility of the issuing bank under current payment association dispute rules. Customers may elect to always require a numeric passcode challenge for a purchase transaction regardless of the value, but this is not required.

[0007] On another issue, issuing banks have generally issued paper terms and conditions (T&C) and cardmember agreements (CMA) to support traditional credit card programs. In the case of an instant credit offer, (e.g. retail) the customer is presented the CMA in paper form as part of the paper application. In a non-instant credit offer (e.g. mail channels), the CMA is delivered to the customer in paper format, via US Mail as part of their new cardmember fulfillment kit. In a web apply channel, the disclosure is generally provided digitally, allowing the customer to simply print out the disclosure, and a follow up hard copy is delivered by post in the fulfillment kit. Mobile payment systems present an unusual problem in that "instant credit" for a mobile user assumes not only traditional instant credit (such as the retail scenario above), but that it provides the customer with the ability to immediately provision and activate the mobile payment account on the mobile device, thus providing the customer with the ability to

immediately begin making purchases. This mobile instant credit availability requires the issuer to consider a new, digital disclosure solution.

[0008] As another issue, application logic, applets, modules or the like in the portable electronic device for handling electronic wallet transactions typically require user validation by requesting the user to first enter a correct passcode to ensure the user really wants the transaction to be executed. This prevents "virtual pickpocketing" by the application controlling the response to the POS terminal only when the user has successfully authenticated the transaction.

[0009] As the use of mobile payment systems becomes more prevalent, payment account issuers are seeking to expand the products and services that are provided in a mobile electronic wallet. For example, an electronic wallet could be used for a plurality of different forms of transactions, such as payments, ticketing, coupons or other activities, and payments could be made from one of a plurality of payment accounts from the same issuer. Each additional product or service from an issuer may require one or more separate application logic or modules in the portable electronic device for handling control, user verification and access to that particular product or service over contactless transaction communication protocols using a respective security mechanism. Therefore, as additional products and services are added to the mobile electronic wallet, the user is burdened with an increasingly complex system, particularly if each of the plurality of security mechanisms involves different user verification passcodes or personal identification numbers (PIN).

[0010] What is desired is an improved mobile payment system and method which addresses the above issues.

[0011] It is also desired to provide a facility for expedient and secured management of users authorized to use the mobile payment account associated with an electronic wallet, directly, entirely and exclusively from the portable electronic device.

[0012] Systems for online banking via the Internet are also generally known that provide the user with an online account for access to the user's bank account information and account related functions, such as transferring funds from the user's bank account to another bank account, using a web browser on a computing device in communication with a suitably configured web server at the financial institution.

[0013] It is a further object of the invention to provide a system that integrates a mobile payment account sub-system and an online banking sub-system in a secure manner.

Statements of the Invention

[0014] In one aspect of the present invention, a mobile payment account activation system and method are provided for facilitating the automated activation of a mobile payment account stored on a portable electronic device, comprising an account activation unit for automatically authenticating a user associated with the mobile payment account by transmitting validation data to the portable electronic device and for activating the provisioned mobile payment account after the user has been authenticated based on the transmitted validation data.

[0015] In another aspect, the present invention provides a mobile payment account activation system for facilitating the automated activation of a mobile payment account stored on a portable electronic device, comprising an account activation unit for automatically authenticating a user associated with the mobile payment account by transmitting validation data to the portable electronic device and for activating the provisioned mobile payment account after the user has been authenticated based on the validation data.

[0016] In another aspect, a mobile device for use in a mobile payment system is provided, comprising a communication network interface, a secure memory for storing data associated with at least one inactive mobile payment account data, and an account activation module operable to receive validation data from the account provisioning system to facilitate automatic authentication of the user and automatically activation of the mobile payment account.

[0017] Preferably, the validation data does not facilitate payment from the activated mobile payment account. Preferably, the validation data used in the automated activation process comprises one or more identification and validation questions that are answered by the user via the portable electronic device to authenticate the user's identity. According to another aspect, enhanced out of band questions may be presented

to the user via the portable electronic device depending for example on predetermined levels of security.

[0018] In another aspect of the invention, a mobile payment account activation system and method are provided for facilitating the automatic activation of a mobile payment account in a mobile payment system, the mobile payment account activation system arranged to store a plurality of mobile payment accounts associated with a user and comprising an account activation unit for receiving a user selection of an inactive mobile payment account and automatically activating the selected mobile payment account after the user has been authenticated.

[0019] In yet another aspect, the present invention provides a method of facilitating secured payment from an electronic wallet on a portable device, comprising storing, on the portable device, an electronic wallet comprising data for completing a payment transaction, wherein said data includes a passcode for enabling access to the electronic wallet and a flag indicating whether input of the passcode is required to access the electronic wallet; receiving a command from a device remote from the portable device to set the flag to indicate that input of the passcode is required to access the electronic wallet; and responsive to a request to conduct a payment transaction from the electronic wallet, prompting for input of a passcode if the flag indicates that input of the passcode is required, verifying the input passcode, and providing payment information to authorize the payment transaction.

[0020] In another aspect, the present invention provides a method is provided of facilitating payment from an electronic wallet on a portable device, comprising storing, on the portable device, wallet application software for accessing the electronic wallet, including executable code for facilitating access to data defining one or more mobile payment accounts in the electronic wallet and executable code for facilitating activation of a secure payment from a mobile payment account; storing, on the portable device, a further payment application software associated with the executable code in the wallet application software for facilitating activation; and receiving a user input selection of the second application software and in response, directly executing the associated executable code in the first application software to facilitate activation of a secure payment from the mobile payment account.

[0021] In yet another aspect, the present invention provides a method for facilitating secured payment from an electronic wallet on a mobile device. The method is achieved by storing an electronic wallet comprising data for authorizing a payment transaction, wherein the data includes a passcode for enabling access to the electronic wallet. The method also includes generating a transaction request message including a value identifying one of a plurality of passcode entry related states and transmitting the generated transaction request message to a remote apparatus.

[0022] Preferably, the remote apparatus can determine that the transaction request is declined based at least on the received value identifying a passcode entry related state. Responsive to determining that the transaction request is declined for a passcode related reason, the remote apparatus transmits a transaction decline response to the mobile device identifying the passcode related reason for decline.

[0023] In yet another aspect, the present invention provides a system and method of facilitating mobile payment account management from an electronic wallet on a first portable device. The method comprises, on the first portable device, storing an electronic wallet comprising data for authorizing a payment transaction from a primary payment account and receiving user input of an additional user authorized to use the primary payment account. An activation code is generated for an additional authorized user, in response to receipt of user input of an additional authorized user. A second portable device stores an electronic wallet comprising data for authorizing a payment transaction from the primary payment account. The method enables payment transactions from the primary payment account to be authorized from the second portable device after receiving user input of the activation code at the second portable device.

[0024] In yet a further aspect, the present invention provides a system and computer-implemented method for tracking a process of provisioning, by a middleware server to a portable device in a mobile payment system, electronic wallet data for authorizing a payment transaction. Preferably, the method comprises transmitting, by the portable device to the middleware server, a user request for a payment account product; initiating, by the middleware server responsive to the received user request, a provisioning process for the requested payment account product, including storing

status data indicative of an initiated state of the provisioning process; transmitting, by the middleware server to the portable device, a digital document including information that must be viewed by the user and updating the stored status data indicative of a digital document transmitted state (that is, the transmitted state of the digital document); receiving, by the middleware server from the portable device, an indication that the digital document has been viewed by the user, and in response updating the stored status data indicative of a digital document viewed state; and provisioning, by the middleware server to the portable device, electronic wallet data for the requested payment account product.

[0025] Generally, the digital document is a terms and conditions (T&C) digital document or a cardmember agreement (CMA). In a further aspect, the T&C digital document is delivered to the portable device as a pre-application disclosure and the CMA is delivered to the portable device as a post-application disclosure.

[0026] In another aspect, the process of delivering the CMA is integrated within the payment product activation process which occurs on the handset. Once the customer has been given the option to view their CMA and elects to continue the account activation process, the payment account can then be fully activated and made available for immediate use.

[0027] In yet another aspect of the present invention, a mobile payment account system and computer-implemented method are provided comprising a mobile device configured for contactless payment operations from a mobile payment account. Preferably, the mobile device is associated with a unique identifier and includes a secure element storing a wallet application module, data defining an encryption key, and data associated with the mobile payment account. The mobile device also includes a mobile-side passcode generator adapted to generate a first passcode based at least on the encryption key and the unique identifier. The system also comprises an online account server including a memory storing online account data defining a user account associated with the mobile device. The online account data comprises data defining a corresponding encryption key. The system further includes a communication interface adapted to receive user input data identifying the unique identifier associated with the mobile device and user input data identifying the first passcode generated by the mobile

device. A server-side passcode generator is adapted to generate a second passcode based at least on the encryption key stored in the online account server and the received unique identifier. The system also includes a user validator adapted to compare the first and second passcodes for a match in a registration process to register the user account.

[0028] In another aspect of the present invention, a system and computer implemented method are provided for registering an online account associated with a mobile device configured for contactless payment operations in a mobile payment account system. Preferably, the method comprises a online account server performing computer-implemented step of storing online account data defining a user account associated the mobile device. The online account data comprises data defining the same encryption key. The method further includes employing the online account server in the performance of receiving user input data identifying a unique identifier associated with the mobile device; receiving user input data identifying a first passcode generated by the mobile device based at least on an encryption key stored in the mobile device and a unique identifier associated with the mobile device; generating a second passcode based at least on an encryption key stored in the online account server and the received unique identifier; comparing the first passcode to the second passcode to determine a match; and registering the online account when a match is determined.

[0029] In another aspect, the present invention provides a system and computer implemented method for registering an online account associated with a mobile device configured for contactless payment operations in a mobile payment account system. The method comprises a computing device performing the computer-implemented step of initiating a registration process to register an online account associated with a mobile device; receiving user input data identifying the unique identifier associated with the mobile device; receiving user input data identifying a first passcode generated by the mobile device; and transmitting the received unique identifier and the first passcode to a online account server for registering the online account when the online account server determines that the first passcode matches a second passcode generated by the online account server based at least on an encryption key stored in the online account server and the received unique identifier.

[0030] According to yet another aspect of the present invention, a system is provided for management of a plurality of application logic or modules in a mobile device secure element to be controlled via a single authentication (or authorization) mechanism. The system facilitates secure authentication of a user using a single controlling passcode or PIN to subsequently allow action by the plurality of application logic or modules within the issuer's control. The application logic or modules are preferably transaction applets that interact with another device (for example, a POS terminal) over communication protocols and could be used for a variety of applications such as payment, ticketing, coupons, or other activities.

[0031] An advantage of such a system is that customers authenticate to the issuer for a variety of products and services using the same passcode as an authentication value. This allows customers to not have to remember a separate passcode for each payment product from the same issuer, and to use the same passcode to obtain servicing of the accounts from the mobile device. This single passcode is intended to apply to all items within the security domain of the same issuer who is primarily liable for the applications used. Since the issuer is responsible for ensuring the payment credentials are validated for accessing the payment, it is their general responsibility to ensure the entered passcode is the customer's correct passcode.

[0032] In another aspect of the present invention is a method of handling a mobile transaction operation whereby the single controlling passcode is entered by a user to the mobile application. This passcode information is transmitted to the central issuer authentication applet inside the secure element for verification. The passcode is verified against local rules and counters inside an authentication applet to ensure the applets are not locked out or otherwise unusable. A subordinate applet is then available for use with a mobile transaction. Execution is then directed to the subordinate applet where it will have the PIN verified state set and the transaction will be allowed over the associated communication interface.

[0033] In an implementation, the authentication applet controls the passcode verification from the subordinate applet. In an alternative implementation, the passcode verification process has the authentication applet directly calling the subordinate applet for simulating passcode entry to manage multiple passcodes to multiple applets.

Advantageously, one controlling passcode is used in an authentication applet to dictate usage to a series of subordinate applets all within the ownership rights of the security domain of the entire collection of applets.

[0034] The controlling passcode could be implemented using any number of methods including a word, phrase, numeric PIN, on-screen path gesture, or facial recognition. The passcode entered by the customer and held by the subordinate applets could be the actual passcode entered by the user or it could optionally be mapped to a passcode held by the authentication applet. This provides greater flexibility in the mobile device allowing for pass phrases or gesture based interactions and translating into something a subordinate applet requires such as a four digit PIN for instance.

[0035] In other aspects, there are provided computer programs arranged to carry out the above methods when executed by a suitable computer, portable device or system.

Brief Description of the Drawings

[0036] There now follows, by way of example only, a detailed description of embodiments of the present invention, with references to the figures identified below.

Figure 1 is a block diagram showing the main components of a mobile payment system according to a first embodiment of the invention.

Figure 2 is a block diagram showing the main elements of a mobile device shown in Figure 1.

Figure 3, which comprises Figures 3a and 3b, is a flow diagram illustrating the main processing steps performed by the components in Figure 1 in provisioning a mobile payment account.

Figure 4, which comprises Figures 4a and 4b, is a flow diagram illustrating the main processing steps performed by the components in Figure 1 in activating a provisioned mobile payment account.

Figure 5, which comprises Figures 5a to 5f, illustrates a sequence of screens displayed by the mobile device to the user during the mobile payment account activation processing illustrated in Figure 4.

Figure 6 is a block diagram showing the main components of a mobile payment system according to a second embodiment of the invention.

Figure 7a is a block diagram showing the main hardware and/or software elements of a mobile device shown in Figure 6 according to the second embodiment.

Figure 7b is a block diagram showing the main functional elements of the mobile device shown in Figure 7a according to the second embodiment.

Figure 8 is a flow diagram illustrating the main processing steps performed by the mobile device of Figures 6 and 7 in a mobile payment process according to the second embodiment.

Figure 9, which comprises Figures 9a to 9d, is a flow diagram illustrating the main processing steps performed by the main components of the mobile payment system of Figure 6 in the step of processing user inputs to activate a payment feature on the mobile device as illustrated in Figure 7.

Figure 10, which comprises Figures 10a to 10f, illustrates a sequence of screens displayed by the mobile device to the user during a mobile payment process according to the second embodiment.

Figure 11, which comprises Figures 11a to 11d, illustrates a sequence of screens displayed by the mobile device to the user during a process for setting a default mobile payment account on the mobile device.

Figure 12 is a block diagram showing the main components of a mobile payment system according to a third embodiment of the invention.

Figure 13 is a block diagram showing the main hardware and/or software elements of a mobile device shown in Figure 12 according to the third embodiment.

Figure 14, which comprises Figures 14a to 14d, is a flow diagram illustrating the main processing steps performed by the mobile device of Figures 12 and 13 in a process for adding an authorized user according to the third embodiment.

Figure 15, which comprises Figures 15a to 15g, illustrates a sequence of screens displayed by the mobile device to the user during the process of adding an authorized user according to the third embodiment.

Figure 16, which comprises Figures 16a to 16e, illustrates a sequence of screens displayed by the mobile device to the user during a process of activating a mobile

payment account linked to an authorizing user's primary payment account according to the third embodiment.

Figure 17, which comprises Figures 17a to 17d, illustrates a sequence of screens displayed by a portable device to the user during a process of adding an authorized user using a web interface according to an alternative embodiment.

Figure 18 is a block diagram showing the main components of a mobile payment system according to a fourth embodiment of the invention.

Figure 19 is a block diagram showing the main hardware and/or software elements of a mobile device shown in Figure 18 according to the fourth embodiment.

Figure 20 is a flow diagram illustrating the main processing steps performed by the mobile device of Figures 18 and 19 in a process for applying for a new mobile payment account product according to the fourth embodiment.

Figure 21, which comprises Figures 21a to 21f, illustrates a sequence of screens displayed by the mobile device to the user during the process of applying for a new mobile payment account product; and

Figure 22 schematically illustrates a digital document structure for facilitating enhanced monitoring and tracking of user navigation through the document, according to an alternate embodiment of the present invention.

Figure 23 is a block diagram showing the main components of a mobile payment system according to a fifth embodiment of the invention.

Figure 24 is a block diagram showing the main hardware and/or software elements of a mobile device shown in Figure 23 according to the fifth embodiment.

Figure 25 is a flow diagram illustrating the main processing steps performed by the system of Figure 23 in a process for provisioning and activating a mobile payment account, and for creating, activating and securely registering an associated online account.

Figure 26 is a flow diagram illustrating the main processing steps performed by the system of Figure 23 in the process for registering a user online account according to an embodiment.

Figure 27, which comprises Figures 27a to 27d, illustrates a sequence of screens displayed by the computing device to the user during the process of registering a user online account.

Figure 28, which comprises Figures 28a to 28d, illustrates a sequence of screens displayed by the mobile device to the user during the process of registering a user online account.

Figure 29, which comprises Figures 29a to 29d, illustrates a sequence of screens displayed by the computing device to the user during the process of registering a user online account according to an alternative embodiment.

Figure 30 is a block diagram showing the main components of a mobile transaction system according to a sixth embodiment of the invention.

Figure 31 is a block diagram showing the main hardware and/or software elements of a mobile device shown in Figure 30 according to the sixth embodiment.

Figure 32 is a block diagram showing the main functional elements of the mobile device shown in Figure 31 according to the sixth embodiment.

Figure 33 is a flow diagram illustrating the main processing steps performed by the mobile device of Figure 32 in a mobile transaction process according to the sixth embodiment.

Figure 34 is a block diagram showing the main functional elements of the mobile device shown in Figure 31 according to a seventh embodiment of the invention.

Figure 35 is a flow diagram illustrating the main processing steps performed by the mobile device of Figure 34 in a mobile transaction process according to the seventh embodiment.

Figure 36 is a block diagram of an example of a computer system on which one or more of the functions of the account management system shown in Figure 1, 6, 12, 18, 23 or 30 may be implemented.

Detailed Description of Embodiments of the Invention

First Embodiment

[0037] A first embodiment of the invention will now be described for a process involving a mobile payment system activating the mobile payment account for use on a user mobile device at a merchant's electronic point of sale terminal. In this embodiment, the process includes steps for securely provisioning the mobile payment account for a user but as those skilled in the art will appreciate, the activation process may be a separate process operating on mobile payment account data pre-provisioned on the mobile device.

[0038] Referring to Figure 1, the mobile payment system 1 of the present embodiment comprises a mobile device 3, a merchant's electronic Point Of Sale (POS) terminal 5 as commonly known in the field, and an account management system 7 associated with a payment account issuer 10. The mobile device 3, merchant's electronic POS terminal 5, and the account management system 7 associated with the payment account issuer 10 communicate electronically with one another.

[0039] As will be described below in greater detail, the account management system 7 includes a communications server 13 and a Trusted Service Manager (TSM) server 18 for facilitating communication between the middleware server 16 and the mobile device 3. The payment account issuer 10 includes a payment processing (authorization and fraud monitoring) system (10a) for authorizing and effecting payment transactions from payment accounts associated with the payment account issuer 10 in response to payment transaction instructions received via a payment association network 17.

[0040] In this embodiment, the mobile device 3 and the electronic POS terminal 5 communicate with one another via a contactless communication link 9. As those skilled in the art will appreciate, this contactless communication link 9 may be for example a near field communication (NFC) link, an infra-red and/or optical link (eg. for bar code scanning), an ultra-sonic link, a radio frequency (eg. RFID) link, a wireless link such as Bluetooth or Wi-Fi based on the IEEE 802.11 standards, or any other communication link that does not require direct physical contact. The mobile device 3 communicates

with the account management system 7 over a cellular telephone network 11 via a cellular network interface (not shown).

[0041] As shown in Figure 1, the mobile device 3 in this embodiment includes a secure memory 4 storing wallet application secure data 6 including payment account data for one or more mobile payment accounts that have been set up on the mobile device 3. The secure memory 4 is, for example, be a Universal Integrated Circuit Card (UICC) secure element, any other secure memory configuration, such as an embedded secure element chip, or as part of a peripheral accessory device to the mobile device 3, such as a micro Secure Digital card - otherwise known as a micro SD card, as are known in the art. Other forms of mobile handset software and/or hardware can be implemented to provide built-in secure electronic wallet functionality for accessing the secure memory 4, including encryption and decryption of the electronic wallet application secure data 6, as necessary. The mobile device 3 can be configured with built-in functionality providing access to the secure memory 4 on the Subscriber Identity Module (SIM) card in the mobile device 3.

[0042] In accordance with the present embodiment, payment account data for a mobile payment account that is securely stored as wallet application secure data 6 in the mobile device 3 includes data identifying a user's account at a payment account issuer 10 from which funds can be transferred to the merchant bank to complete a transaction via a payment association network 17. The payment account data can additionally include data defining an amount of pre-paid funds that have been transferred from the user's payment account issuer 10 to that mobile payment account. In this way, the electronic wallet can include a payment account linked to multiple funding sources, such as a pre-paid account, deposit account and/or credit account. As an alternative, the electronic wallet can include a plurality of mobile payment accounts, each linked to a respective funding source. The mobile payment account can be provisioned for the user by the account management system 7.

[0043] The mobile device 3 also includes a wallet application module 8 storing computer-implementable processing instructions used to control the operation of the mobile device 3, for example to i) request creation of a new mobile payment account, ii) handle a secure mobile payment account activation process, and/or iii) process a

transaction with a merchant via the electronic POS terminal 5 to effectively transfer funds from the mobile payment account on the mobile device 3 to the merchant. The wallet application module 8 can be implemented as one or more software components of an operating system running on the mobile device 3 or implemented as one or more separate software applications installed on the mobile device 3. Such software applications may be configured to run as background applications on the mobile device 3 that monitor receipt of messages or events and activate upon receipt of appropriate messages or events so as to carry out the above operations. The software applications can alternatively be launched by the user. Alternatively, as shown in Figure 1, the wallet application module 8 can be stored in the secure memory 4, and loaded into a virtual machine of the mobile device 3 to provide the functionality of the present embodiment.

[0044] Before the user can use the mobile device 3 to carry out transactions with a merchant electronic POS terminal 5, a new mobile payment account is provisioned for the user, for example in response to a user requesting a new mobile payment account via the mobile device 3. Payment account data may be created by the account management system 7 for a new mobile payment account, and the account management system 7 can be arranged to immediately transmits the payment account data 6 to the mobile device 3 for storage in the secure memory 4 of the mobile device 3. As those skilled in the art will appreciate, this is just one way in which an inactive mobile payment account can be provisioned on the mobile device 3 and any other method of delivery is envisaged. A notification message may be displayed by the mobile device 3 to alert the user that the mobile payment account is ready but requires authentication via the mobile payment account module 8 before the mobile payment account can be activated.

[0045] A secure activation process is then carried out between the mobile device 3 and the account management system 7 to authenticate the identity of the user trying to activate the new mobile payment account. Once the authentication is successful, the account management system 7 activates the mobile payment account. The activated mobile payment account data stored in the secure memory 4 of the mobile device 3 can then be used to carry out transactions with a merchant electronic POS terminal 5 via the

contactless communication link 9, whereby a requested amount of funds can be transferred from the mobile payment account stored in the mobile device 3 to the merchant's bank 12.

Account Management System

[0046] The account management system 7 in the mobile payment system 1 will now be described in more detail with reference to Figure 1, which shows the elements of the account management system 7 used in this embodiment. As shown, the account management system 7 may include a communications server 13, a middleware server 16, an account creation server 201 and a Trusted Service Manager (TSM) server 18, which communicate electronically with one another. In this embodiment, the servers communicate with one another via secure network links, for example over a private Local Area Network (LAN), a VPN connection, or other dedicated secure connection. It is appreciated that, although the components of the payment account system in this embodiment are provided as separate servers, one or more of the servers could be provided as software and/or hardware modules in the same server.

[0047] As shown in Figure 1, data can be communicated between the mobile device 3 and the middleware server 16 over the cellular telephone network 11 via a cellular telephone network interface 14 of the communications server 13. The TSM server 18 performs logical data preparation of the data to be communicated to the mobile device by forming appropriate commands to be written to the secure element 4 of the mobile device 3. The precise form of the data depends on the particular implementation of the secure element 4 of the mobile device 3 and/or the payment association scheme program for facilitating payment. The TSM server 18 can also perform encryption of the sensitive payment account information in the mobile payment account data. The TSM server 18 then passes the encrypted data to the mobile device 3 via the communications server 13 and the cellular telephone network 11.

[0048] As part of the account activation process which will be described in more detail below, the communications server 13 may receive a request for activation of a new mobile payment account from the mobile device 3 and, in response, passes a request to the middleware server 16 to initiate the activation process for a new mobile payment account. The middleware server 16 also maintains a state of the mobile payment

account for servicing throughout the account activation processes. The middleware server 16 may also performs event and notification handling to the other servers in the account provisioning system 7 throughout the account activation processes.

[0049] If creation of a new mobile payment account is required, the middleware server 16 may initiate a provisioning process by sending an instant provisioning request to the account creation server 99 via a secure network communication link, such as a web services communication link. As is known in present payment account systems, the account creation server 99 establishes an account at a payment account issuer 10 in response to receiving an instant provisioning request. This process typically involves passing account details from the instant provisioning request to the payment account issuer 10, or any other known card payment account processing platform (pre-paid, credit deposit), to establish a new account at the payment account issuer 10. Once the new account has been established by the payment account issuer 10, the account creation server 99 may receive an embossing data file from the payment account issuer 10 which would typically be used to create a physical plastic payment card for the user. The account creation server 99 creates the mobile payment account data including data from the embossing data file received from the payment account issuer 10 as well as additional data pertaining to the mobile device 3 and to the mobile user requesting the new account which will be used in the mobile account activation process.

[0050] The mobile payment account data is then be passed to the TSM server 18 via the middleware 16, which performs logical data preparation of the received mobile payment account data by forming appropriate commands to be written to the secure memory 4 of the mobile device 3. As those skilled in the art will appreciate, the precise form of the data may depend on the particular implementation of the secure memory 4 of the mobile device 3 and/or the payment association scheme program for facilitating payment. The TSM server 18 can also perform encryption of the mobile payment account data , for example of the sensitive payment account information in the mobile payment account data such as the payment keys. The TSM server 18 may then passes the encrypted payment account data of the provisioned inactive mobile payment account to the mobile device 3 via the communications server 13 and the cellular telephone network 11.

[0051] As will be described below, the middleware server 16 also handles authentication of the mobile user through validation messages communicated between the mobile device 3 and the middleware server 16 via the communications server 13. The middleware server 16 stores validation data pertaining to the mobile user requesting the new account until the mobile payment account has been activated. Alternatively or additionally, the validation data may be stored and provided by the payment account issuer 10 or by a third party system (not shown). The validation data may be in the form of identification and validation (ID&V) questions and answers, based on ID&V information associated with the mobile payment account which is stored on the middleware server 16 or payment account issuer 10, and/or based on additional ID&V information provided by a third party. The ID&V information may include publicly available information that only the user would know to be the answers, and therefore the ID&V information does not need to be transmitted over the air nor made available through the account authentication application on the mobile device 3. After the middleware server 16 and the payment account issuer 10 authenticate the mobile user, the mobile payment account is then activated by the middleware server 16 and the payment account issuer 10 to enable payments to be made from the mobile payment account.

[0052] The communications server 13 also includes a separate TSM unit 15 for establishing a trusted communication channel with a mobile device 3 via the cellular telephone network 11, and for securely routing the data to the mobile device 3. In the above example, the TSM unit 15 in the communications server 13 would not access any of the sensitive portions of the encrypted data that are routed to the mobile device 3 via the cellular telephone network interface 14. It is appreciated that the functionality of the TSM unit 15 can be integrated with the cellular telephone network interface 14.

Mobile Device

[0053] Figure 2 shows the elements of the mobile device 3 according to the first embodiment of the present invention. In this embodiment, the mobile device 3 is a mobile handset. As shown in Figure 2, the mobile handset operating system and hardware 28 includes a controller 21 for controlling the mobile device 3, and a user interface 22 arranged to process inputs from a keypad 23 and to control output on a

display 25. The keypad 23 and display 25 can be provided as separate hardware entities of the mobile device 3, or alternatively, as an integrated entity such as a touch sensitive display screen user interface. The mobile device 3 can also include components included in commonly known mobile handsets, such as a microphone, an earpiece speaker, a camera, and/or a GPS sensors/receiver etc., which are not shown. A working memory 27 is provided for use by the handset operating system and hardware units 28.

[0054] Software and data are transferred via the cellular network interface 33 or via a different data communication link interface 71 in the form of signals 72, which can be electronic, electromagnetic, optical, or other signals capable of being received by the data communication link interface 71 via a communication path 73 that carries the signals and can be implemented using wire or cable, fiber optics, a physical phone line, a wireless link, a radio frequency link, or any other suitable communication channel, including any combination of suitable communication channels. The communication path 73 can be linked or merged with the communication path from the cellular network interface 33 to the cellular telephone network 11.

[0055] As mentioned above, the mobile device 3 includes a secure memory 4. The mobile device 3 is operable to receive the wallet application secure data 6, including the payment account data, and activation request messages from and send validation messages to the account management system 7 via a cellular telephone network interface 33 and the cellular telephone network 11. The mobile device 3 is also operable to store the received wallet application secure data 6 in the secure memory 4. The mobile device 3 is also operable to receive transaction authorization request messages from and send authorization messages to the merchant's POS terminal 5 via a contactless communications link interface 37 and the contactless communications link 9. Communication between a POS terminal 5 and the mobile device 3 can involve transmission of data in a single direction from the mobile device 3 to the POS terminal 5, depending on an implemented protocol (such as the protocols used by the DISCOVER ZIP™, MasterCard PayPass™, Visa Paywave™ and AMEX ExpressPay™ cashless payment systems).

[0056] The mobile device 3 includes a wallet application module 8 as mentioned above, which stores processing instructions used to control the operation of the mobile device 3

to perform the various mobile payment account processes, as will be described in detail below. The payment account application wallet module 8 includes an account creation sub-module (not shown) which stores processing instructions to create a request for a new mobile payment account if desired, in response to user input from the user interface 22. The request may be transmitted to the account management system 7 via the cellular telephone network interface 33. The payment account wallet application module 8 also includes an account activation sub-module (not shown) which stores processing instructions used to carry out a secured account validation and activation process in response to user input from the keypad 23 and account activation request messages received from the account management system 7 via the cellular telephone network interface 33. The payment account module 8 also includes a transaction authorization sub-module (not shown) which stores processing instructions used to control the operation of the controller 21 to carry out and authorize a transaction in response to user input from the keypad 23 and transaction authorization request messages received from the merchant's POS terminal 5 via the contactless communications link interface 37. The mobile payment wallet application module 8 may be configured to store a plurality of wallet screens 24 and an account access screen 26-1 which may be output on display 23 of the user interface 22 to facilitate user interaction with the mobile payment wallet application module 8. The mobile payment wallet application module 8 may also store one or more non-payment application modules 29 including processing instructions used to control the operation of the mobile device 3 to perform other non-payment related processes. As those skilled in the art will appreciate, although the above discussed functionality is described as being provided by a single mobile payment wallet application module 8 on the mobile device 3, as an alternative, the validation and authentication functionality may be provided as a account authentication application separate from the transaction authorization functionality provided as a transaction processing application, for example. Additionally, the account authentication application and the transaction processing application may be prepared by the TSM server 18 of the account management system 7 and transmitted for storage in the mobile device 3 via the communications server 13 in advance of the account activation process. As yet a further modification, those skilled in

the art will appreciate that the payment account module 8 may instead provided as one or more hardware and/or software components of the mobile device 3.

[0057] Also schematically illustrated in the exemplary embodiment of Figure 2 are a plurality of security domains which can be implemented in the secure memory 4 of the mobile device 3. The secure element 4 is advantageously implemented to be compliant with one or more specifications of a standard infrastructure in order to facilitate communication of data and messages between the mobile device 3 (and the secure element 4) and other entities in the mobile payment system 1. For example, and in accordance with a preferred embodiment, the secure element 4 is compliant with the known GlobalPlatform Card Specifications (for example the "GlobalPlatform Card Specification 2.2", March 2006, which is incorporated herein by reference), and accordingly includes a plurality of security domains for facilitating control of the management of and accessibility to executable operations and sensitive data associated with specific areas of the secure element 4 by the various entities in the mobile payment system 1. The GlobalPlatform Card Specifications (for example the "GlobalPlatform Card Specification 2.2", March 2006) define a hierarchical arrangement of security domains, each defining functionality and data that can be accessed by a respective associated entity, for example, cryptographic keys or certificates, that can be used to support secure channel protocol operations between the mobile device 3 and the entity or entities associated with that particular security domain, and/or to authorize secure element 4 content management functions.

[0058] As shown in the exemplary embodiment of Figure 2, an issuer security domain 31 associated with a particular mobile network operator, includes a wallet security domain 32 associated with the payment account issuer 10, a Controlling Authority (CA) security domain 34 associated with a controlling authority in the mobile payment system 1, and a Supplementary Security Domain (SSD) code 35 associated with an intermediate security domain (not shown) to manage card content and perform cryptographic services for confidentiality. The wallet security domain 32 in this exemplary embodiment includes the securely stored wallet application secure data 6, which include data for use by the wallet application module 8. The wallet security domain 32 also includes an issuer security domain 36 and one or more optional other

service provider security domains 37. The issuer security domain 36 includes an issuer applet package 38, an issuer applet 39, and one or more payment applet instances 40 which enable the transaction processing functionality using an activated mobile payment account. The payment security domain 32 may also include a Proximity Payment System Environment (PPSE) package or application 41, defining application functionality associated with transaction processing functionality and, in particular, for handling communications with a contactless reader of the POS terminal 5 to identify which of the one or more mobile payment accounts is to respond.

[0059] The wallet security domain 32 also includes a PPSE controller instance 42 for accessing the application functionality in the PPSE package 41 to facilitate an additional application layer level of control of the transaction processing functionality between the one or more payment applet instances 40 and the contactless communication link interface 37. In particular, the PPSE package 41 and PPSE controller instance 42 are advantageously provided where the mobile device 3 stores a plurality of mobile payment accounts and operates to communicate with the NFC reader of the merchant POS terminal 5 to control which one of the payment applet instances 40, associated with a respective mobile payment account stored on the mobile device 3, is to respond back to the POS reader

[0060] Each security domain is associated with one or more respective entities in the mobile payment system 1 depending on the particular business model that is implemented by the mobile payment system 1. The specific implementation details of the various security domains for compliance with the GlobalPlatform Card Specifications are beyond the scope of this application and will be apparent to the skilled reader. The mobile device 3 also includes one or more other third party application modules 44 stored in the secure memory 4, for example an application module related to third party loyalty scheme. The secure memory 4 also stores a UICC applet 45 which is an application to manage and hold the mobile network operator's functionality and secure information, such as a network key and GSM (Global Systems for Mobile Communications) PIN (Personal Identification Number).

Account Activation Process

[0061] A brief description has been given above of the components forming part of the mobile payment system 1 of this first embodiment. A more detailed description of the operation of these components in this embodiment will now be given for an example computer-implemented mobile payment account provisioning process in a situation where a user wishes to request a new mobile payment account via the mobile device 3, with reference to the flow diagram of Figure 3, which comprises Figures 3a and 3b. As mentioned above, this process may not be necessary if data for an inactive mobile payment account has already been provisioned on the mobile device 3 by another method.

[0062] As shown in Figure 3, the automated process begins at step S3-1 where the middleware server 16 in the account provisioning system 7 may receive a request for a new mobile payment account from the mobile device 3 via the communications server 13, the request including data identifying the mobile device 3 and details entered by the user for provisioning the new mobile payment account. As is common under normal and customary banking processes and systems, the details may include for example the user's name, address and birth date. Next, at step S3-3, the middleware server 13 may initiate an account provisioning process for a new mobile payment account and sets the servicing state of the new mobile payment account to "Inactive" to indicate that the account has just been created and has yet to be transmitted to the mobile device 3 for authentication and activation. A mobile payment account with an "Inactive" state is not available for use by the mobile device 3 to carry out transactions. The middleware server 13 may be configured to store a database of created accounts to maintain the respective states for provisioning.

[0063] As part of the account provisioning process if necessary, at step S3-5, the middleware server 16 may send an instant mobile account provisioning request (which includes the data identifying the mobile device 3 and the user details) to the account creation server 201. At step S3-7, the account creation server 201 may extract the user details from the received instant mobile account provisioning request and sends the extracted user details to the payment account issuer 10 to establish a new account at the payment account issuer 10. At step S3-9, the account creation server may receive an

embossing data file for the new account from the payment account issuer 10 after the new account has been established at the payment account issuer 10. At step S3-11, the account creation server 201 may then create mobile payment account data for a new mobile payment account based on the received embossing data file. The new mobile payment account data includes the data identifying the mobile device 3 received in the instant mobile account provisioning request.

[0064] At step S3-13, the account creation server 201 may then send the mobile payment account data for the new provisioned mobile payment account to the TSM server 18 via the middleware server 16. At step S3-15, the TSM server 18 may prepare the mobile payment account data for transmission to and storage on the mobile device 3. This may involve logical data preparation of the mobile payment account data 6 by forming appropriate commands to be written to the secure memory 4 of the mobile device 3. At step S3-17, the TSM server 18 may also perform encryption of the sensitive payment account information in the mobile payment account data such as the payment keys, if necessary. This encryption may be performed based on known software and/or hardware functionality of the mobile device 3. At step S3-19, the TSM server 18 may send the encrypted payment account data to the mobile device 3 via the communications server 13 and the cellular telephone network 11, and at step S3-21, the mobile device 3 may store the received payment account data of the mobile payment account in the secure memory 4.

[0065] As the provisioned mobile payment account is not activated at this stage, at step S3-23, the mobile device 3 displays an indication to notify the user that a mobile payment account has been provisioned and is ready for activation. At step S3-25, the middleware server 16 carries out a user authentication and account activation process as will be described below, to activate the mobile payment account stored on the mobile device 3 ready for use by the transaction authorization sub-module 45, as well as to update the activation state of the mobile payment account at the account management system 7 and/or the payment account issuer 10.

Account Activation Process

[0066] An example of a process flow of the mobile payment system 1 for handling a user authorization and mobile account activation process between the account

management system 7 and the mobile device 3 will now be described with reference to the flow diagram of Figure 4, and also Figure 5, which comprises Figures 5a to 5f, illustrating a sequence of exemplary display screens that are presented to the user on the mobile device 3 in the transaction authorization process. As shown in the exemplary display screen 51-1 in Figure 5a, an indication 53 that a mobile payment account is ready for activation is provided on the icon 55 for the account authentication application. The user launches the account authentication application, which begins the automated account activation process at step S4-1 by establishing a secure communication session between the mobile device 3 and the middleware server 16 via the communications server 13. At step S4-3, the middleware server 16 receives a request to activate a selected provisioned mobile payment account via the secure communication session. Figure 5b shows an example display screen 51-2 which is displayed by the account authentication application for the user to select an account to activate from a list of mobile payment accounts that are ready to be activated. As the selected mobile payment account is a newly provisioned mobile payment account, the requirement to enter a security Personal Identification Number (PIN) to enable access to payment is disabled. The middleware server 16 and payment account issuer 10 then carry out an automated authentication of the mobile user associated with the selected mobile payment account, based on the stored validation data. In this embodiment, the authentication involves the middleware server 16 sending an ID&V question to the mobile device 3 via the secure communication session at step S4-5, and receiving and validating the user response to the transmitted ID&V question at step S4-7.

[0067] Additionally, those skilled in the art will appreciate that the level of security can be controlled and determined based on a risk profile for the mobile user. For example, a user that is requesting a mobile payment account for the first time may be classified as a high risk user and accordingly may be presented with a plurality of ID&V questions, for example three questions using validation information sourced from a third party to verify the user's identity with a higher level of confidence. Such ID&V questions may for example be of the form "Where did you live in 1994?", where the questions may be generated based on ID&V information obtainable from public records but where the user is the only person likely to know the answers. As mentioned above, the ID&V

information itself need not be transmitted by the account management system 7 over the cellular telephone network 11, and the ID&V questions and answers are never transmitted together in the same message, thus reducing the risk of identity theft and fraud.

[0068] A user may, on the other hand, be classified as a low risk user for example if that user is requesting an additional mobile payment account and therefore would already be registered on the account management system 7 and the payment account issuer 10, or for example may have a mobile device and/or software that facilitates a more secure communication link with the account management system 7. For a low risk user, a less complicated authentication process could be used, for example involving a single ID&V question based on user details previously provided to the account management system 7.

[0069] Therefore, at step S4-9, the middleware server 16 determines if another ID&V question is to be transmitted to the mobile device 3, and if so, steps S4-5 and S4-7 are repeated for the additional ID&V question. Figure 5c illustrates three exemplary display screens 51-3, 51-4, 51-5 that are displayed to the user in sequence to facilitate input of answers to the ID&V questions which are transmitted back to the middleware server 16 for validation. The middleware server 16 may be configured to permit a predetermined number of incorrect answers before terminating the authentication and activation process, and requiring the user to resolve the activation process by conventional methods such as calling customer support for the account activation system.

[0070] The use of ID&V questions and validation of received answers advantageously provides an additional measure of security against identification theft on top of the secured communication channels that are in place, particularly because the present invention allows for real-time activation of a mobile payment account directly from a user's mobile device 3. For example, account creation may be requested immediately after the user has purchased the mobile phone or at any later time where the user may be in a public environment and at risk of a fraudster observing as the user enters his or her identification details into the mobile device 3. More devious methods for theft of input identification details may involve hacking or eavesdropping of the secured

communication channels between the mobile device 3 and the account management system 7. The automated user authentication steps of the account activation process advantageously reduce the risk of identity theft because a fraudster is prevented from unauthorized usage of a mobile payment account merely from any stolen answers to ID&V questions as the data that is transmitted (which may be sensitive data such as the user's social security number or date of birth) does not facilitate actual payment from an activated mobile payment account which is typically enabled by user entry of a correct PIN. The present invention further advantageously provides for this secure implementation while at the same time minimizing the delay in activating a provisioned mobile payment account so that a user can effectively activate a provisioned mobile payment account in real time.

[0071] When the middleware server 16 determines at step S4-9 that no further ID&V questions are required and the identity of the mobile user has been automatically authenticated by validation of each the received user responses as compared to the stored validation data, the middleware server 16 may then wait for confirmation from the mobile device 3 that the user has agreed to the mobile payment account terms and conditions, at step S4-11. As shown in Figure 5d, this may involve a display screen 51-6 on the mobile device 3 prompting the user to view account agreement documentation on the mobile device 3 itself, for example by pressing a button 63-1 labeled "On Handset", or to view the documentation online via a web browser, for example by pressing a button 63-2 labeled "View online". Alternatively or additionally, the user may request that the account agreement documentation be sent by e-mail. The user preference for viewing the account agreement documentation may be stored on the mobile device 3 for a later account activation process for additional mobile payment accounts. In an example, once the user has read and agreed to the mobile payment account terms and conditions set out in the account agreement documentation, the user may press the OK button 63-3 and the account authentication application sends a confirmation message back to the middleware server 16. As an alternative, the user may not be required to provide confirmation of agreement to any terms and conditions and may instead simply be provided with a welcome greeting screen to inform the user that he or she has been successfully authenticated with the account management system

7. As yet a further alternative, if terms and conditions are not been delivered to the mobile device in the above exemplary way, the account management system 7 may be arranged to dynamically ensure delivery of the account agreement documentation to the user by any other suitable method of delivery.

[0072] After the middleware server 16 has received confirmation at step S4-11 as necessary, then at step S4-13, the TSM server 18 systematically generates an unblock command which is sent back to the mobile device 3, via for example the TSM unit 15 of the communications server 13. In response to receiving the unblock command, the middleware server 16 changes the state of the mobile payment account to "Issuer PIN Unblocked" at step S4-15. Then, at step S4-17, the mobile device 3 prompts for and receives a PIN input by the user for the mobile payment account, and additionally, may also prompt for and receive a user input secret word for the mobile payment account. As shown in Figure 5e, a display screen 51-7 may be displayed by the account authentication application of the mobile device 3 to prompt the user to set a PIN for the mobile payment account in a first input field 68-1, to confirm the PIN in a second input field 68-2. The user may additionally be prompted to input a secret word in a third input field 68-3. Requiring user input of a secret word may be further advantageously used to prevent phising for sensitive information and to guard against counterfeit applications. The mobile device 3 may store the user input issuer PIN for the mobile payment account in the payment account data 6 stored in the secure memory 4 so that the information is only known and accessible by the user. The stored user PIN for a mobile payment account may subsequently be required to be input by the user when executing the mobile payment wallet application 8 that is to access the payment account data 6 for the mobile payment account at a later time. At step S4-19, the mobile device 3 notifies the middleware server 16 that an issuer PIN for the mobile payment account has been set by the user on the mobile device 3. In response, at step S4-21 the middleware server 16 activates the mobile payment account, and at step S4-23, updates the state of the mobile payment account to "Active". Figure 5f illustrates an example display screen 51-8 of the mobile device 3 informing the user that the provisioned mobile payment account is active and ready for use to carry out transactions with a merchant. The TSM server 18 may then transmit a message to the mobile device 3 to

activate the transaction processing application if necessary, for example if this is the first time the user has activated a mobile payment account.

Second Embodiment

[0073] A second embodiment of the invention will now be described for a process for conducting a payment transaction using a mobile device at a merchant's electronic point of sale terminal, using corresponding reference numerals to those of preceding figures where appropriate for corresponding elements. Referring to Figure 6, the mobile payment system 201 according to the second embodiment comprises a mobile device 3, a merchant's electronic Point Of Sale (POS) terminal 5 as commonly known in the field, and a account management system 7 associated with a payment account issuer 10, as discussed in the embodiment above.

[0074] As shown in Figure 6, the mobile device 3 in this embodiment also includes a secure memory 4 storing wallet application secure data 6 for one or more mobile payment accounts that have been set up on the mobile device 3. In this embodiment, the mobile device 3 includes a payment account wallet application module 8 that is not stored in the secure memory 4, the payment account wallet application module 8 storing processing instructions used to control the operation of the mobile device 3.

[0075] Figure 7, which comprises Figures 7a and 7b, shows the elements of the mobile device 3 according to the second embodiment of the present invention. As shown in Figure 7, the mobile device 3 is a mobile handset including components as described in the embodiment above.

[0076] In this embodiment, the mobile device 3 further includes a payment shortcut module 19 that provides a shortcut to the payment feature within the mobile payment wallet application module 8. The shortcut may be implemented as processing instructions that link to the processing instructions of the transaction authorization sub-module. Alternatively, the payment shortcut module 19 may comprise separate processing instructions used to control the operation of the controller 21 to carry out and authorize a transaction in response to user input from the user interface 22. Provision of the payment shortcut module 19 advantageously enables an improved user interface for the transaction payment process that expedites the purchase process at a POS terminal 5 as the user avoids having to navigate through multiple wallet screens of the mobile

payment wallet application module 8 to authorize a payment transaction from the electronic wallet.

[0077] In an embodiment, the mobile payment wallet application module 8 may facilitate user navigation from any one of the wallet screens 24 to the main menu wallet screen 26-2. As those skilled in the art will appreciate, such navigation to the main menu wallet screen 26-2 may be direct or via one or more intermediary wallet screens 24. In this way, even though a user may have accessed the payment features of the wallet application module directly using the wallet application payment shortcut module 19 of the present invention, the user may be able to navigate to any other wallet screen 24 of the mobile payment wallet application module 8.

[0078] Also schematically illustrated in the exemplary embodiment of Figure 7a are a plurality of security domains which may be implemented in the secure memory 4 of the mobile device 3. The security domains serve to segment the management and accessibility of various parties' functionality and sensitive data as will be apparent to those skilled in the art. As shown in Figure 7a, an issuer security domain 31 may include a payment security domain 32, a Controlling Authority (CA) security domain 34, and a Supplementary Security Domain (SSD) code 35. The payment security domain includes the wallet application secure data 6, along with an issuer security domain 36 and one or more optional other service provider security domains 37. The issuer security domain 36 may include an issuer applet package 38, an authentication applet instance 46, and one or more payment applet instances 40 which enable the transaction processing functionality using an activated mobile payment account. The payment security domain 32 may also include a Proximity Payment System Environment (PPSE) package (module) 41, a PPSE controller instance 42 for facilitating the transaction processing functionality between the payment applet instances 40 and the contactless link interface 47, and a payment package 43.

[0079] The mobile device 3 may also include one or more other third party application modules 44 stored in the secure memory 4, for example an application module related to third party loyalty scheme. The secure memory 4 may also stores a UICC applet 45 which is an application to manage and hold the mobile network operator's functionality and secure information, such as a network key and GSM PIN.

[0080] Figure 7b is a block diagram showing the main functional elements of the mobile device when configured to execute processing instructions of the payment applet 40 and the authentication applet 46, according to an embodiment of the invention. As will be discussed in greater detail below, the mobile payment wallet application module 8 may call the payment applet instance 40 to conduct a payment transaction process for example when a user waves the mobile device 3 past the contactless communication interface of the POS terminal 5. As shown in Figure 7b, in this embodiment, the payment applet 40 may provide functional elements for authorizing a transaction 40-1, generating an authorization request 40-2, transmitting an authorization request 40-3 and displaying confirmation of a completed payment transaction 40-4, for example. The payment applet 40 may call the authentication applet instance 46 to process, authorize and allow a payment transaction to proceed. The authentication applet 46 tells the payment application if the PIN has been set and if it will allow the transaction to proceed based upon various PIN entry flags. As shown in Figure 7b, the authentication applet 46 may also provide functional elements for updating the PIN 46-1, locking the PIN 46-2, obtaining a user defined security word 46-3 from the secure data 6, checking if the PIN is currently writeable 46-4, verifying the PIN 46-5, setting a PIN-verified flag 46-6, clearing a PIN-verified flag 46-7, resetting the PIN 46-8, updating the security word 46-9, updating the Risk flag 46-10, resetting the Risk flag 46-11 and retrieving the PIN-verified flag 46-12. Functional elements 46-1 to 46-7 and 46-11 are typically called by the mobile payment wallet application module 8, as will be described below. Functional elements 46-8 to 46-10 may be called by the account management system 7, for example from the middleware server 16 via the TSM server 18 in the form of APDU commands to execute in the secure element for remotely setting the PIN risk flag 103, as will be described below. Functional elements 46-12, as well as 46-7, are typically called by the payment applet 40.

[0081] The authentication applet 46 maintains a PIN entry flag 101 for the state of PIN entry, a PIN risk flag 103, a security word 105, a PIN locked state 107 (from an issuer perspective) and a PIN-verified flag 109, which are stored securely as wallet application secure data 6 in the secure memory 4 of the mobile device 3. In this embodiment, the PIN risk flag 103 is provided as an indication that an incorrect PIN was previously

entered on the handset and therefore advantageously facilitates prevention of fraud from the issuer perspective, because the customer can be forced to enter a PIN effectively by setting the PIN risk flag 103. The PIN risk flag 103 further allows for flexibility in not forcing a PIN for low dollar transactions while keeping control over the use of the mobile payment account. Transactions may be allowed to continue uninterrupted unless certain conditions arise requiring PIN verification, which may include for example:

- An authorization message includes indication that incorrect PIN was previously entered and no correct PIN was provided for this transaction (as those skilled in the art will appreciate, this is possible for example with option 2 for dCVV); in such an instance, the middleware server 16 can choose to decline the payment transaction.
- Built-in logic to prompt for PIN entry if PIN was previously entered incorrectly or a configurable number of times without a PIN.
- Built in logic to detect remote set PIN entry required for next transaction.

[0082] For example, when the PIN risk flag 103 is set to true, the authentication applet 46 may cause the payment applet 40 to raise itself asking for PIN entry via a NFC push request. This condition would send an error to the payment applet 40 to not allow a transaction at this time. Upon successful PIN entry, the PIN risk flag may be reset since the customer has successfully entered the PIN and thereby allowing the transaction to be made by the next wave and invocation of the payment applet 40. In effect, the PIN entry flag would be communicated from the authentication applet 46 to the payment applet 40 and through a payment authorization request to a merchant payment transaction authorization system via the electronic POS terminal 5, as is commonly known. The merchant's authorization system would then send the PIN entry information to for example a fraud/risk assessment unit (not shown) of the middleware server 16 to reset the PIN risk flag 103, as will be described in more detail below.

[0083] As those skilled in the art will appreciate, as an alternative, the processing instructions and functionality of the payment applet 40 and the authentication applet 46 may instead be provided as a single applet within the secure element 4. As yet another alternative, a plurality of applets may be included within the secure element 4 providing the functionality of embodiments of the present invention according to any desired bundling or collection of the respective processing instructions.

Payment Transaction Process

[0084] A brief description has been given above of the components forming part of the mobile payment system 201 of this second embodiment. A more detailed description of the operation of these components in this embodiment will now be given with reference to the flow diagrams of Figure 8 and 9, for an example computer-implemented mobile payment transaction process using the mobile device 3 configured with one or more activated mobile payment accounts. Reference is also made to Figure 10, which comprises Figures 10a to 10f, schematically illustrating exemplary display screens that may be presented to the user on the mobile device 3 in a payment transaction process.

[0085] As shown in Figure 8, the process begins at step S8-1 where the mobile device 3 receives a user input to unlock the handset, if the handset is in a locked state. At step S8-3, the mobile device 3 receives a user input selection of an application icon 53 for the wallet application payment shortcut module 19, instead of the application icon 55 for the fully featured wallet application module 8. The user selection may be input for example via the mobile handset touch sensitive display screen 23 of the user interface 22. As those skilled in the art will appreciate, Figure 10a illustrates an exemplary display 51-21 of user selectable icons for the various applications stored on the mobile handset and many other known arrangements will be apparent depending for example on the operating system and hardware of the mobile handset. In response to receiving the user input selection, the mobile device 3 launches the shortcut application and executes the processing instructions. In an embodiment, the processing instructions define a link to the processing instructions of the transaction authorization sub-module. In this way, at step S8-7, the user is directly presented with a wallet screen 55 for facilitating activation of the payment feature from the electronic wallet on the mobile handset, without having to navigate through menus and options of the main wallet application module 8 in order to find the activation wallet screen. Once the payment feature of a selected mobile payment account has been activated on the mobile device 3, the mobile device 3 can be used to conduct a payment transaction with the merchant electronic POS terminal 5 via the contactless communication link 9. In response to the user waving the mobile device 3 past a contactless communication interface of the POS

terminal 5, the mobile device 3 effects a payment transaction from the selected mobile payment account and outputs confirmation of the payment transaction once completed at step S8-9.

[0086] Figure 9, which comprises Figures 9a to 9d, illustrates the main processing steps performed by the main components of the mobile payment system 201 in the above steps S8-7 and S8-9 illustrated in Figure 8. As shown in Figure 9, processing user inputs to activate the payment feature on the mobile handset may start at step S9-1 with the wallet application module 8 calling the authentication applet instance 46 to check a PIN entry mode as set by the user. In this embodiment, the customer is able to make "tap and go" purchases for low dollar transactions. However, customers may elect to have a PIN set for all transactions. Therefore, a PIN mode is required for detecting this preference. The user selected configuration for the use of PIN, for example via the wallet application module 8, supports two PIN modes:

- an "Always Required" mode, which results in no valid authorization request being transmitted from the mobile device 3 if a PIN is not entered. In this mode, the user will be required to successfully verify their PIN in order to process a valid transaction, regardless of whether the transaction value is high or low.
- an "Only As Necessary" mode, which results in an authorization request that has indication of successful user PIN entry being generated and transmitted by the mobile device 3, and authorization decisioning may then be performed for example at the middleware server 16 based on other factors such as a transaction risk level (i.e. taking into consideration if the value of the payment transaction is above a threshold value, such as $50).

[0087] If the mobile device 3 determines that the PIN mode is set to "Always Required" at step S9-1, then at step S9-3, the mobile device 3 prompts the user for entry of a PIN. As schematically illustrated in Figure 10b, the mobile device may display a wallet screen 51-22 which includes a prompt and a password field 68-11 for the user to enter a PIN and may also include a prompt for the user to change a selected one of the mobile payment accounts stored in the mobile handset as described above. The mobile payment wallet application module 8 may provide separate wallet screens 24 for facilitating user setting of a particular mobile payment account that is to be displayed as

a selected payment account by default, as indicated by a selected account indication 68-12 for the default account. Figure 10c shows an exemplary wallet screen 51-22 displaying a different selected account indication 68-13 after the user has selected a different mobile payment account 68-13 for conducting the subsequent payment transaction. User configuration of the default selected mobile payment account may be facilitated by wallet screens 24 accessible from the main menu wallet screen 26-2 for example, for accessing and changing mobile payment account details. Figures 11a to 11d show an exemplary sequence of wallet screens for accessing details for credit account linked with the mobile payment account, and for setting the credit account as the default payment method so that the credit account is displayed as the selected payment account by default.

[0088] At step S9-5, the mobile device 3 checks if user input of an entered PIN has been received, for example via the wallet screen 51-22. As those skilled in the art will appreciate, the entered PIN in the password field 68-11 may be masked on the displayed screen with hidden characters as the user inputs each character or number. Additionally, the user's sensitive mobile payment account details, such as card numbers, expiration dates and CVV codes, are encoded in the wallet application module 8 and never displayed on-screen, thereby further reducing the risk of fraud. If the mobile device 3 determines at step S9-5 that no PIN has been entered, then at step S9-7, the mobile device 3 checks if the handset has been waved past the contactless communication link interface of a POS terminal 5 and if not, processing returns to step S9-3 for the user to enter a PIN. As those skilled in the art will appreciate, when the mobile device 3 and POS terminal 5 are within range, one of the contactless communication link interfaces will initiate communication, referred to herein as "device handshaking", to establish the contactless communication link, illustrated as step S9-9. It is commonly known that such contactless communication link interfaces generally communicate under the guidelines of ISO 14443, whereby the reader at the POS terminal 5 emits a signal that is received and interpreted by the contactless link interface 47 in the mobile device 3.

[0089] In this case, the user has not entered a PIN although the mobile device 3 is expecting a PIN and has proceeded to present the mobile device 3 to the POS terminal 5

at step S9-7. This may be because the user has simply forgotten to input a PIN and therefore at step S9-11, the POS terminal may receive an error code, which the POS terminal 5 may output so that for example a store clerk may see the displayed error and communicate to the customer. In an embodiment, the mobile device 3 may be arranged to display a message to the user indicating the need to enter a PIN in order to activate the payment feature. Alternatively, the mobile device 3 may be configured to not perform any interaction between the handset and the POS terminal 5 without a user entered PIN, and consequently at step S9-11, the POS terminal 5 may not react to the presence of the mobile device 3 because no appropriate data or request has been transmitted. Processing then returns to step S9-3 where the user is again prompted to enter a PIN.

[0090] On the other hand, if the mobile device 3 determines at step S9-5 that a PIN has been entered, then at step S9-13, the mobile device 3 verifies if the user input PIN is valid by comparing the input PIN with the user's pre-defined PIN stored in the wallet application secure data 6. If the mobile device 3 determines at step S9-13 that the user input PIN is not correct, then at step S9-17, the wallet application module 8 updates a count of the number of incorrect PIN entry attempts. As those skilled in the art will appreciate, the wallet application module 8 may be configured to check, at step S9-19, if a PIN is successively entered incorrectly a defined number of times and if so, to lock the PIN at step S9-21 and to display an indication that the PIN is locked at step S9-23. Locking of the PIN effectively prohibits the payment feature for the mobile payment account until the user has unlocked the PIN for example via a PIN reset process as will be apparent to those skilled in the art. On the other hand, if the PIN has not been successively entered incorrectly a defined number of times, then processing returns to step S9-3 where the user may be prompted to re-enter a correct PIN.

[0091] When the mobile device determines at step S9-13 that a correct PIN has been entered, then at step S9-25 the authentication applet 46 resets the PIN risk flag 103. At step S9-27, the authentication applet 46 sets the PIN-verified flag 109 that will be included in the next transaction authorization request. In an embodiment, the mobile device 3 may also be arranged to display a wallet screen 51-23 for example as schematically illustrated in Figure 10d, to confirm that a verified PIN was entered and

to indicate to the user that the selected mobile payment account is now enabled to conduct a payment transaction. At step S9-29, the mobile device 3 then checks if the contactless link interface 47 has been placed within range of a contactless communication link interface of a POS terminal 5. In an embodiment, the mobile device 3 may be configured to only allow a mobile payment transaction to be conducted using the selected mobile payment account within a predefined time window for example from the time when the correct PIN has been entered by the user. Therefore, at step S9-31, the mobile device 3 may check if a predefined time has elapsed since the correct PIN has been entered by the user, and to terminate the process if the handset is not presented to a POS terminal 5 in time. As those skilled in the art will appreciate, such a time out may reset the PIN entered and PIN verified flags. As discussed above, at step S9-33, when the mobile device 3 and POS terminal 5 are within range, the respective contactless communication link interfaces will initiate communication, typically in the form of device handshaking to establish the contactless communication link. In response, the wallet application module 8 checks, at step S9-34, if a correct PIN was entered by the user in step S9-13 above as necessary. The wallet application module 8 may for example check if the PIN entry flag 101 is set. If a correct PIN was entered by the user, then at step S9-35, the mobile device 3 generates an authorization request including a data value indicating that the correct PIN was entered. Otherwise, at step S9-36, the mobile device 3 generates an authorization request where the data value indicates that the no correct PIN was entered. As is commonly known, this indication may be provided as a unique transaction identifier of a verified PIN according to the specific contactless chip and/or card technology in use (for example the known dCVV or CVC3 identifiers). At step S9-37, the mobile device 3 transmits the valid authorization message to the electronic POS terminal 5 to authorize that the payment transaction be effected from the associated payment account issuer 10 to the merchant bank 12. The user entered PIN is therefore never transmitted by the mobile device 3 thereby further reducing risk of fraud.

[0092] The above procedure described the processing steps for the "Always Required" PIN mode. If at step S9-1, the mobile device 3 determines that the PIN mode is set to the "Only as necessary" mode, then step S9-4, the mobile device 3 checks if the PIN

Risk flag 103 is set, thus requiring input of a passcode before a payment transaction can be authorized. If the PIN Risk flag 103 is set, then processing proceeds to step S9-3 as discussed above. However, if the PIN Risk flag 103 is not set, then processing proceeds directly to step S9-27 where the PIN verified flag 109 is set and the payment feature is activated without requiring user input of a PIN or passcode.

[0093] Thereafter, the POS terminal 5 may instruct a payment transaction from the user selected mobile payment account to the merchant bank in the normal manner, as will be briefly discussed with reference to Figure 9. At step S9-39, the POS terminal 5 receives the authorization request from the mobile device 3 and at step S9-41 transmits a transaction instruction, via the payment association network 17, to the payment processing system 10a of the payment account issuer 10 associated with the user selected mobile payment account. At step S9-43, the payment processing system 10a receives the transaction instruction from the POS terminal 5 and in response, performs authorization decisioning for the instructed transaction at step S9-45. Authorization decisioning can be based on any number of factors, primarily checking that the available balance of the associated user payment account is sufficient to cover the payment transaction, and then for example checking if the PIN verified flag is set based on a transaction risk level (for example if the value of the transaction is above a predefined threshold value), and/or checking if the PIN was previously entered incorrectly, etc. Other factors related to internal account status, such as usage thresholds, existing restrictive status, unusual purchase patterns and/or suspicious transactions identified by predefined rules or conditions, can also be considered by the payment processing system 10a when determining if a requested transaction is to be authorized. Optionally, the payment processing system 10a can also consider whether the PIN risk flag 103 is set on the mobile device 3 by comparing the PIN risk flag value to server settings at step S4-46.

[0094] When the payment processing system 10a determines that the payment transaction is authorized, the transfer of funds from the account associated with the selected mobile payment account is effected at step S9-47, and confirmation of the transaction is transmitted to the POS terminal 5 at step S9-49. At step S9-51, the POS

terminal 5 receives confirmation of the completed transaction from the middleware server 7 and at step S9-53, the POS terminal 5 outputs the confirmation to the merchant.

[0095] At step S9-54, the middleware server 16 of the account management system 7 receives confirmation of the completed transaction from the payment processing system 10. In response, at step S9-55, the account management system 7 can optionally transmit confirmation of the completed transaction to the mobile device 3 via the cellular telephone network 11, for example. At step S9-57, the mobile device 3 receives the payment transaction confirmation from the account management system 7 and outputs, at step S9-59, confirmation of the payment transaction via a wallet screen 51-24, for example as schematically illustrated in Figure 10e. The mobile device 3 may also be configured to output an audible confirmation of the payment.

[0096] On the other hand, the payment processing system 10a can determine at step S4-45 that the payment transaction is to be declined due to a PIN related reason, such as an incorrect entered PIN or the absence of PIN entry. If the payment transaction is declined, then in response at step S4-61, the payment processing system 10a generates a transaction declined response message including information identifying the reason for the declined transaction. The transaction declined response message is transmitted to the mobile device 3 at step S4-63 and displayed by the mobile payment wallet application module 8 at step S4-65.

[0097] In the embodiment described above, the authorization request generated by the mobile device 3 at step S9-35 or step S9-36 included a binary data value indicating whether or not a correct PIN was entered to the mobile device 3. In an alternative embodiment, the mobile device 3 is adapted to generate an authorization request including a multi-faceted value instead of a binary data value relating to PIN entry through the mobile payment wallet application module 8 of the mobile device 3. The multi-faceted value can be used to identify one of more than two states of a user's PIN-related actions, for example:

1. A PIN was entered to the mobile payment wallet application module 8 and was verified as a correct PIN matching the pre-defined PIN stored in the wallet application secure data 6.

2. A PIN was entered to the mobile payment wallet application module 8 but was not verified as a correct PIN because the entered PIN did not match the pre-defined PIN stored in the wallet application secure data 6.
3. A PIN was not entered in the mobile payment wallet application module 8 because the PIN mode was set to "Only as necessary".

[0098] In a further alternative embodiment, the user selected mobile payment account can be linked to a checking account at a payment account issuer 10. The authorized account details transmitted to the POS terminal 5 via the contactless communication link 9 identifies the payment account as a checking account. Typically, the POS terminal 5 will then request additional input from the user before the payment transaction can be completed by the POS terminal 5. For example, the additional input may be in the form of a prompt to select a specific payment type such as credit or debit, and the user may be required to input a signature for example via a touch sensitive input screen of the POS terminal 5.

[0099] In an embodiment, the middleware server 16 may be additionally configured to receive details of the payment transaction, for example from the payment account issuer 10 after the payment has been transferred or from the merchant POS terminal 5 or merchant bank 12 directly. In response, the middleware server 16 may be further arranged to communicate additional confirmation of the payment to the mobile device 3, including for example details of the amount of funds that was transferred, the name of the target recipient, and the date of the payment transaction. The additional payment confirmation may be displayed by the mobile device 3 as a further payment confirmation wallet screen 51-25, for example as schematically illustrated in Figure 10f.

Remote PIN Management

[00100] In a further embodiment of the present invention, the payment processing (authorization and fraud monitoring) system 10a may additionally be configured to offer additional tools to remotely set the PIN risk flag 103 stored securely on the mobile device 3 to force a challenge the next time the mobile device 3 is used to make a transaction attempt as described above. With the PIN risk flag 103 set on the mobile

device 3, the customer will be always be asked to enter their passcode/PIN before another transaction, regardless of transaction amount, can be made on the mobile device in the manner described above. Once the passcode is entered on the mobile device 3, the risk flag 103 is unset on the secure element 4 to allow a transaction to the point of sale. Without the PIN risk flag 103, a thief may steal a phone and would be able to use that phone indefinitely for multiple low dollar transactions without ever being prompted for a PIN. With the facility to remotely set the PIN risk flag 103, the payment processing system 10a could be additionally configured with a set threshold of usage or to react to unusual purchase patterns or based upon a number of low dollar transactions since the PIN was entered last. Such an implementation can beneficially be used to efficiently monitor low dollar transactions. As is commonly known, such low dollar transactions are typically the payment issuer's liability and are not generally able to be charged back to the retailer. As discussed above, the information that a verified passcode or PIN entry has been made would be sent with the next transaction to inform the merchant and payment issuer systems that the customer has verified themselves. Even small dollar transactions could be blocked at the issuing bank until the customer verified themselves.

[00101] In order to set the risk flag remotely, the payment processing system 10a may be configured to detect unusual usage based upon a variety of predefined risk factors. The risk factors detect unusual behavior from a customer and can include a combination of attributes such as unusual merchant locations for the customer, time of day differences from normal usage patterns, a higher velocity of transaction attempts, or other proprietary models. Current issuing bank processes can shut off the payment capability of a payment account until the user verifies possession of the payment account to the bank, but this new process allows for a gentler interaction between the customer and the bank. The present embodiment advantageously allows for the customer to verify themselves in the act of payment when the customer wishes to make their next payment. This further reduces the number of bank resources required to contact customers and manage the fraud flags on accounts.

[00102] Current plastic card based contactless technologies can only be updated when in contact with a chip card reader. Some payment association specifications allow

for account updates to contactless cards via these chip card readers, but these are rarely used since these payment accounts are typically waved over a reader versus inserted into a dedicated chip card reader. Adding the payment account to a mobile device allows for additional data fields to be sent over the air to the mobile device to effect payments.

[00103] A summary of the remotely set risk flag process in mobile device enabled payment transactions will now be provided.

[00104] In this further embodiment, the process would detect the anomaly using current payment authorization processes and then communicate the new risk flag value to the mobile device 3, for example over the air via a Trusted Service Manager (TSM) and cellular communication networks. The updated risk flag value would be stored into the secure memory space 4 of the mobile device 3 where the PIN risk flag 103 resides, in control of the payment account issuer 10. This PIN risk flag 103 updating process may start for example with an issuing bank fraud detection system deciding the payment account is not to be trusted without further customer verification. The fraud detection system may elect to prevent any new transactions until the PIN risk flag 103 has been cleared. The bank fraud detection system would then send a message to the bank's payment processing system 10a with the specific customer account information and risk flag setting. In many cases, the issuing bank will have a TSM of their own that will broker communication to a mobile network operator's TSM which will talk to the phone. The bank's payment processing system 10a would communicate with the issuing bank TSM to logically and physically prepare the new risk flag data commands for the targeted mobile device 3. The issuing bank TSM communicates with the mobile network operator TSM to deliver the new risk flag 103 to the mobile device 3. It will be appreciated that alternatively or additionally, the mobile device 3 can be configured for direct communication with the issuing bank TSM, for example to receive settings and information from the payment processing system 10a via push and/or Short Message Service (SMS) technology. Once received by the mobile phone 3, the new risk flag setting will be placed into the secure memory storage 4 for use in the next transaction as described above with reference to Figure 9.

[00105] As described above, on the mobile device 3, the transaction process can vary based upon user provided settings to either require a passcode prior to any transaction attempt, or provide a passcode only for high value transactions – for example any transactions above a threshold value between $25 and $50 based upon the issuing bank and payment association rules. Payments from mobile devices 3 as described above generally follow a process as follows. The mobile device is held near a point of sale (POS) reader. The reader emits a signal received and interpreted by the contactless link interface 47 in the mobile device. The contactless reader interface is a near field communication (NFC) process generally communicating under the guidelines of ISO 14443 and further refined by payment association specifications for specifying the message values between the contactless reader interface of the POS terminal 5 and mobile device 3.

[00106] The contactless reader interface identifies the point of sale communication is a payment request. As configured in the mobile device 3, the PPSE application 41 may be called to provide a payment account instance within the secure element 4 processor subsystem. The PPSE 41 determines the payment account currently selected for use on the mobile handset and hands control to a payment association specific instantiation 40 of a payment application that ultimately provides the account information.

[00107] The payment application 40 within the secure element 4 of the mobile device 3 will determine if the passcode was required, entered and then pass that information along with the payment account information for use in the transaction. The payment application 40 can also access other data values stored within the secure element 4 such as the risk flag 103. The payment application 40 may also use local values to determine if the user preference for the passcode needing to be verified or other counters for allowing only so many transactions before a passcode to be entered. The remote setting of the risk flag 103 is one opportunity for issuing banks to allow multiple small dollar transactions within normal customer transaction operations and ask only for the passcode in case of unusual customer activity.

[00108] If the risk flag 103 is set to a value requiring user input, the payment application 40 may return an error value to the contactless reader interface as well as

messaging to the mobile device to alerting the user that a passcode is required before a transaction can be made. Other reasons for passcode required entry are if the user has set their preference to always require passcode entry for any transaction. Otherwise, the payment application will allow the transaction.

[00109] If the payment application 40 allows the transaction to proceed, the specific payment account data is passed back to the POS terminal 5. The POS terminal 5 interprets the message and assembles the payment account data for a transaction request to the association payment network. The message is routed through the payment network to the payment account issuer 10.

[00110] The transaction request is received at the payment account issuer 10 and processed for approval based upon funds availability as well as fraud decision strategies. The setting of the value of the risk flag is kept at the issuer systems and the current value of the passcode verification is sent with each mobile transaction request to the payment account issuer 10 over the payment network authorization message. Among all other rules determining transaction success at the issuer's payment authorization system, the transaction will be denied if the passcode is not verified and the risk flag is set to a value on the mobile device. Additional risk and fraud strategies may be employed by the payment account issuer 10 to determine if this transaction will be allowed as per normal business processes.

[00111] If the risk flag 103 is set at the time of transaction attempt, and the passcode has been entered - passed in via the transaction request, this action will clear then the payment processing system 10a flags that the fraud check has been passed. This action will restart any low dollar risk checks for unusual usage and the risk flag 103 may be set again at some future point of time.

[00112] The remote setting of a risk flag 103 therefore allows customers to make a number of low dollar transactions without ever having to enter a passcode if the bank system sees the activity as normal use. The customer will not be forced to enter a passcode every set number of low dollar transactions if the bank feels the risk is low.

[00113] An addition to this process could be a remote setting of the number of low dollar transactions to be used before the next passcode verification is required. If a local counter mechanism for passcode verification is employed on the mobile handset 3,

the counter could be set remotely by the payment account issuer 10 via the same TSM process described above. This could allow a flexible counter to be increased over time as usage patterns are determined by the issuing bank and customer habits are formed. Upon successful entry of the passcode, the counter is reset to the value.

Third Embodiment

[00114] A third embodiment of the invention will now be described, using corresponding reference numerals to those of preceding figures where appropriate for corresponding elements. Referring to Figure 12, the mobile payment system 301 according to the third embodiment comprises a plurality of mobile devices 3a, 3b, a merchant's electronic Point Of Sale (POS) terminal 5 as commonly known in the field, and an account management system 7 associated with a payment account issuer 10, as described in the embodiments above.

[00115] As will be described below, the user associated with the first mobile device 3a may be the primary account holder and owner of the account associated with the mobile payment account stored on the first mobile device 3a, and may wish to add a user associated with a second mobile device 3b as an additional authorized user of the same account. In the present embodiment, the mobile device 3a is configured to enable the account owner to select a contact person from contacts data 50 stored on the mobile device 3a as an authorized user of a selected mobile payment account. It is commonly known to store such contacts data 50 on a mobile device 3, such as in the form of an electronic phone book or address book, storing data for each contact person identifying the contact's name and mobile directory number. In response to a received request from the mobile device 3a associated with the account owner to add a selected contact person as an authorized mobile account user, the account management system 7 is arranged to verify the selected contact person and then to carry out a mobile payment account provisioning and/or activation process with the second mobile device 3b associated with the authorized user.

[00116] Verification of the authorized user involves prompting the authorized user to enter an activation code that is generated by the account management system 7 and securely communicated to the account owner. The account owner canthen communicate the activation code to the authorized user by any desired transmission

means, for example, face to face which would be highly secure, or via other communication channels such as Short Message Service (SMS) messaging over the cellular telephone network or email via the Internet, which are external to the mobile payment account management system. In this way, an account owner is able to safely, securely and expediently allow another user to use the same account on their own mobile device. The process is advantageously carried out through the account owner's mobile device, and provides a level of security through the requirement of an activation code which is never transmitted between the mobile devices 3a, 3b via the account management system 7 as part of the add authorized user process, thus preventing identity theft and fraudulent access to the mobile payment account from a hacker eavesdropping on the data communications between the first mobile device 3a and the second mobile device 3b. Additionally, the add authorized user process is more efficient than known processes for adding an additional account holder to a payment account as the process does not require time-consuming identification and verification procedures involving manual intervention by personnel at the payment account issuer.

[00117] Figure 13 shows the elements of a mobile device 3 according to the third embodiment. As shown in Figure 13, the mobile device 3 is a mobile handset including components as described in the embodiments above. In the present embodiment, another plurality of wallet screens in the mobile payment wallet application module 8 are provided as "add authorized user" wallet screens 26-3 which are displayed in response to user selection of an option to add an additional user authorized to use the associated mobile payment account to conduct payment transactions, as will be described in more detail below.

[00118] A description of the operation of the components in this third embodiment will now be given with reference to the flow diagram of Figure 14, which comprises Figures 14a to 14d. Figures 14a to 14d provide an example computer-implemented process for adding an authorized user of a selected mobile payment account using the mobile device 3 configured with one or more activated mobile payment accounts. Reference is also made to Figure 15, which comprises Figures 15a to 15g, schematically illustrating exemplary display screens that may be presented to the

primary account owner on the mobile device 3a in the process of adding an authorized user.

[00119] As shown in Figure 14a, the process begins at step S14-1 where the mobile device 3a of the account owner receives user input to launch the mobile payment wallet application module 8. Figure 15a shows an example user interface 51-31 of the account owner's mobile device 3a for enabling a user (the account owner) to launch the mobile payment wallet application module 8 by selection of a respective application icon 55 displayed by the handset operating system 28. Many other forms of user interface are possible depending on the particular mobile device used to implement the present embodiment. After the user has launched the wallet application module 8, the mobile device 3a receives, at step S14-3, user selection of a mobile payment account stored on the mobile device 3a, for example via a wallet summary screen 51-32 displayed by the mobile device 3a as schematically illustrated in Figure 15b. In the example shown in Figure 15b, four mobile payment accounts are stored in the electronic wallet, a "BC Credit" mobile payment account associated with a credit account at a payment account issuer 10, a "BC Debit" mobile payment account associated with a debit account at a payment account issuer 10, a "BC Pre-Paid" mobile payment account linked with an account at a payment account issuer 10 and containing a transferred amount of funds, and a "Points" mobile payment account linked with a points based payment account at a payment account issuer 10. The wallet summary screen 51-32 may be configured to display a retrieved balance of one or more of the listed mobile payment accounts. The user may scroll through the list of displayed mobile payment accounts to highlight and select a desired mobile payment account 64-1.

[00120] In response to the user selection of a mobile payment account at step S14-3, the mobile device 3a may be configured to authenticate the user at step S14-5 by prompting for input of a PIN to verify the identity of the account owner, as will be apparent to the skilled person. An exemplary PIN prompt and input screen 51-33 is shown in Figure 15c. Once the user has been authenticated by the wallet application module 8, the mobile device 3a may display an account detail wallet screen 51-34 displaying a plurality of user selectable options for accessing information about and/or managing the selected mobile payment account. As shown in the exemplary screen in

Figure 15d, the account detail wallet screen 51-34 may display the type of account (Credit), the balance ($102.00), and a plurality of user selectable options including checking the available credit for the mobile payment account, checking the date when payment is due, and adding an authorized user for the selected mobile payment account as indicated by the highlighted menu item 64-2. A further indication, such as an arrow 66, may be displayed to indicate that additional selection options are available for managing the selected mobile payment account. Accordingly, at step S14-7, the mobile device 3a receives a user selection of the menu option to add an authorized user for the selected mobile payment account.

[00121] At step S14-9, the mobile device 3a may display a first add authorized user wallet screen 51-35 displaying a plurality of user selectable options for choosing a data source for selecting an authorized user. As shown in the exemplary screen 51-35 in Figure 15e, the select authorized user data source wallet screen 51-35 may display the user selectable options "AU Added online" to select an external database as the data source, or "From phonebook" to select the contacts data 50 as the data source. A further option "Enter new user" is also provided to enable the user to input the data as a new data source. Accordingly, at step S14-11 the user selects one of the displayed options. If at step S14-11, the user selects the "From phonebook" option, as indicated by the highlighted menu item 64-3 in Figure 15e, then the process proceeds to step S14-13 where the mobile device 3a displays a further add authorized user wallet screen 26 to enable user selection of an authorized user from the contacts data 50 stored on the mobile device 3a. An exemplary display screen 51-36 is shown in Figure 15f, where the user has highlighted 64-4 one of the contacts "John Smith (mobile)" and that person's associated Mobile Directory Number (MDN) from the list of contacts. Alternatively, if the added online option is selected at step S14-11, then the process proceeds to step S14-15, where the mobile device 3a retrieves details for an authorized user as previously added via an external online interface as will be apparent to those skilled in the art. If the enter new user details option is selected instead at step S14-11, then the process proceeds to step S14-17 where the mobile device may display a further add authorized user wallet screen 26 to prompt for and receive user input of details, such as the name and MDN of an authorized user.

[00122] Referring now to Figure 14b, once the user has selected an authorized user from a data source or entered details of an authorized user, then at step S14-19, the mobile device 3a generates a request to add the authorized user and transmits the request to the middleware server 16 of the mobile payment account management system 7. It is appreciated the request will include data identifying the user to be added as an authorized user of the mobile payment account, the data including the MDN of the authorized user. However, and in accordance with an alternative embodiment, other forms of data may instead be used to identify the authorized user that may suitably be used by the account management system 7 to identify a mobile device 3b associated with the authorized user, such as the unique International Mobile Equipment Identity (IMEI) of the mobile device 3b. Accordingly, at step S14-21, the middleware server 16 receives the request to add an authorized user for a mobile payment account from the account owner's mobile device 3a via the communications server 13 of the account management system 7.

[00123] At step S14-23, the middleware server 16 may check if the authorized user identified in the request is registered with the account management system 7. This may involve checking that the authorized user is associated with a mobile device 3b that is configured with the mobile payment account wallet application module 8 and operable to communicate securely with the account management system 7. This check may be performed based, on the MDN associated with the authorized user. If at step S14-23, the middleware server 16 determines that the authorized user identified in the request is not registered with the account management system 7, or is not associated with a mobile device enabled for conducting mobile payment transactions, then at step S14-25, the account management system 7 may proceed to create new account data for the authorized user and initiate creation of a plastic card for the authorized user. Alternatively, the account management system 7 may be arranged to transmit a message to a mobile device 3b associated with the authorized user with the mobile payment account wallet application module 8 or instructions to configure the mobile device 3b to enable mobile payment transactions from that device. However, if at step S14-23 the middleware server 16 determines that the authorized user is registered with the account management system 7 and is associated with a suitably configured mobile device 3b,

then at step S14-25, the middleware server 16 generates an activation code for this add authorized user process. The activation code may be generated randomly or pseudo-randomly using any known random code generation technique, and is temporary in nature. The generated activation code is then transmitted by the middleware server 16, at step S14-29, to the account owner's mobile device 3a.

[00124] At step S14-31, the activation code is received at the account owner's mobile device 3a, which outputs the received activation code at step S14-32 on a wallet screen 51-37 as schematically shown in Figure 15g. The account owner may then communicate, at step S14-33, the activation code to the authorized user by any desired transmission means, for example face to face, by SMS messaging over the cellular telephone network or email via the Internet. At step S14-35, the activation code is received by the authorized user at the authorized user's mobile device although this is not necessary. In preferred embodiments, the transmission path over which the activation code is communicated from the account owner to the authorized user is separate from the communication paths of the mobile payment system 1. Therefore, steps S14-33 and S14-35 are shown as dashed lines in Figure 14b, to indicate that these steps are preferably performed external to the mobile payment system 301 of the present invention.

[00125] After the middleware server 16 has transmitted the activation code to the account owner's mobile device at step S14-29, then at step S14-37, the middleware server 16 may be arranged to create a new mobile payment account for the authorized user, the new mobile payment account being linked to the selected payment account of a payment account issuer 10 as identified in the add authorized user request. At step S14-39, the middleware server 16 provisions the inactive mobile payment account data 6b to the authorized user's mobile device 3b identified by the details provided in the request. The inactive mobile payment account data 6b is received at the authorized user's mobile device 3b at step S14-41 and stored in the secure memory 4b. This process of creating, provisioning and securely storing inactive mobile payment account data for a mobile device is discussed in the embodiments above.

[00126] The process of activating a new mobile payment account linked to the primary account will now be described with reference to Figure 14c. Reference is also

made to Figure 16, which comprises Figures 16a to 16e, schematically illustrating exemplary display screens that may be presented to the authorized user on the mobile device 3b in the activation process. Once the inactive mobile payment account data 6b is stored in the secure memory 4b, the authorized user's mobile device 3b notifies the authorized user that a new mobile payment account is ready for activation at step S14-43. As shown in Figure 16a, the authorized user's mobile device 3b may display an indication 53 over an application icon 55 in the user interface 51-38 displayed by the handset operating system 28, as the notification that a provisioned mobile payment account is available for activation. It is appreciated that that many other forms of user interface and indication are possible depending on the particular mobile device used to implement the present embodiment. At step S14-45, the mobile device 3b of the authorized user receives user input to launch the mobile payment wallet application module 8.

[00127] After the user has launched the wallet application module 8 of the mobile device 3b, a wallet screen 24 may be provided to display the inactive mobile payment account or a list of inactive mobile payment accounts awaiting activation as shown in the exemplary display screen 51-39 in Figure 16b. Accordingly, at step S14-47, the mobile device 3b receives a user selection 64-5 of an inactive mobile payment account stored in the secure memory 4 of the authorized user's mobile device 3b. In response, the mobile device 3b displays at step S14-49 a subsequent display screen 51-40 as shown in Figure 16c, to prompt the authorized user to input the activation code for the selected mobile payment account. This is the activation code that was generated by the middleware server 16 in response to receiving the "add authorized user" request, transmitted to the account owner's mobile device 3a, and communicated by the account owner to the authorized user, as described above. At step S14-51, the mobile device 3b receives the user input activation code via a text input field 68-21 of the display screen 51-40, and at step S14-53, the user input activation code is transmitted by the mobile device 3b to the middleware server 16, via the communications server 13 of the account management system 7.

[00128] At step S14-55, the middleware server 16 receives the activation code as input by the authorized user to the mobile device 3b and compares the received user

input activation code to the previously generated activation code as transmitted to the authorized user's mobile device 3a, at step S14-57. If the middleware server 16 determines that the two codes do not match, then the user input activation code is not correct and in response, the middleware server 16 may transmit an error message back to the authorized user's mobile device 3b at step S14-59. In such an embodiment, the authorized user's mobile device 3b may be configured to display the error message and return to step S14-49 where the user is prompted for the correct activation code. On the other hand, if the middleware server 16 determines at step S14-57 that the user input activation code is correct, then at step S14-61, the middleware server 16 may set the account state of the authorized user's mobile payment account that is linked to the primary account to "Issuer PIN unblocked" to indicate that the authorized user has been verified (by input of the correct activation code, which will only be known to the account owner and the authorized user) and that the mobile payment account can be configured for activation and use by the authorized user on the mobile device 3b. Therefore, at step S14-63, the middleware server 16 transmits a PIN unblock command to the authorized user's mobile device 3b, and may also transmit a message to the payment account issuer 10 with the state of the mobile payment account.

[00129] In response to receiving the PIN unblock command, the mobile device 3b displays a wallet display screen 51-41 at step S14-65 to prompt the authorized user to set a PIN (or passcode) for the mobile payment account. As shown in Figure 16d, this wallet display screen 51-41 may prompt the authorized user to input the PIN a second time as confirmation of the correct PIN being set, and may also prompt for a secret word to be set, which may be used as a user verification in the event that the user wishes to recover a forgotten PIN. As those skilled in the art will appreciate, the PIN or passcode may be used for verifying or authenticating the user before effecting payment transactions from the associated mobile payment account, or before any servicing of the mobile payment account on the mobile device 3b. At step S14-67, the mobile device 3b receives and stores the user input PIN and secret word as mobile payment account data for the activated mobile payment account in the secure memory 4b of the mobile device 3b. At step S14-69, the mobile device 3b then transmits a confirmation message back to the middleware server 16 to inform the account management system 7 that the PIN has

been set by the user. In response to receiving the confirmation at step S14-71, the middleware server 16 automatically activates the authorized user's mobile payment account by setting the state to "Active". The authorized user is then able to use the activated mobile payment account in the electronic wallet of the authorized user's mobile device 3b, that is linked to a primary account belonging to another user, to carry out contactless payment transactions as described in the embodiments above.

Fourth Embodiment

[00130] A fourth embodiment of the invention will now be described, using corresponding reference numerals to those of preceding figures where appropriate for corresponding elements. Referring to Figure 18, the mobile payment system 401 according to the fourth embodiment comprises a mobile device 3, a merchant's electronic Point Of Sale (POS) terminal 5 as commonly known in the field, and an account management system 7 associated with a payment account issuer 10, as described in the embodiments above.

[00131] As will be described below, a user associated with the mobile device 3 can search and apply for new mobile payment account products that are available for the user. In the present embodiment, the mobile payment system 1 is configured to enable the user to apply for a new mobile payment account product directly from the mobile device 3, including provisioning and activation of the requested mobile payment account once approved by the account management system and/or payment account issuer, as well as providing, monitoring and receiving acceptance of digital disclosure documentation during the application process. In this way, a user is able to efficiently apply for a new mobile payment account product solely through the mobile device 3, and the account management system 7 is able to advantageously track the application process of the user. For example, the application process of the user may be tracked from the initial user selection of a menu option to browse for eligible products, through the user viewing and accepting specific and crucial terms, conditions and agreement clauses set out in digital disclosure documents particular to a product, and finally through approval and activation of a mobile payment account product on the user's mobile device 3.

[00132] Figure 19 shows the elements of a mobile device 3 according to the fourth embodiment. As shown in Figure 19, the mobile device 3 is a mobile handset including components as described in the embodiments above. In the present embodiment, another plurality of wallet screens in the mobile payment wallet application module 8 are provided as "apply for new product" wallet screens 26-4 to prompt for and receive user input of details to complete the application for the desired mobile payment account product, as will be described in more detail below.

[00133] A more detailed description of the operation of these components in this fourth embodiment will now be given with reference to the flow diagram of Figure 20, which comprises Figures 20a to 20d. Figures 20a to 20d provide an example computer-implemented process for applying for and provisioning a mobile payment account using the mobile device 3 in communication with the account management system 7. Reference is also made to Figure 21, which comprises Figures 21a to 21g, schematically illustrating exemplary display screens that can be presented to a user on the mobile device 3 in the application process.

[00134] As shown in Figure 20a, the process begins at step S20-1 where the mobile device 3 receives user input to launch the mobile payment account wallet application module 8. Figure 21a shows an example user interface 51-51 of the user's mobile device 3 for enabling the user to launch the mobile payment account wallet application module 8 by selection of a respective application icon 55 displayed by the handset operating system 28. Many other forms of user interface are possible depending on the particular mobile device used to implement the present embodiment. After the user has launched the wallet application module 8, the mobile device 3 receives, at step S20-3, user selection of a menu option to search for eligible mobile payment account payment products and/or to apply for a new mobile payment account product. In the example shown in Figure 21b, a "main menu" wallet screen 51-52 is displayed by the mobile device 3 to the user, providing a plurality of user selectable options for the electronic wallet. The user scrolls through the list of displayed options to highlight 64-11 and select a desired menu option. In response to selection of the option to apply for a new product, the mobile device 3 displays a user details input wallet screen 51-53 as shown in Figure 21c to prompt for user input of personal details,

such as the user's name and address, into respective input fields 68-41 and 68-42. Alternatively or additionally, predetermined personal details are stored in the wallet application secure data 6 in the secure memory 4 and are automatically input to the respective fields. Other user related information and/or search criteria can be obtained at this step via input field 68-43 for use in determining a list of eligible products for the user. Accordingly, at step S20-5 the mobile device 3 receives input of personal details and/or product search criteria and displays, at step S20-7, a list of eligible products based on the input details and/or search criteria. The list of eligible products is determined by the mobile device 3, based on stored data identifying all available mobile payment products and associated prerequisites and eligibility criteria. Alternatively, the determination is carried out by the account management system 7 based on the input details and/or search criteria received from the mobile device 3. Figure 21d shows an exemplary wallet screen 51-54 displaying a list of user selectable eligible products.

[00135] At step S20-9, the mobile device 3 receives user input of a selected 64-12 one of the eligible mobile payment account products and in response, transmits data identifying the selected product to the account management system 7 to initiate an application process for that product to be automatically provisioned to the requesting mobile device 3 once the associated user has been approved by the account management system 7 and/or payment account issuer 10. At step S20-11 the middleware server 16 in the account management system 7 receives the request for application of a new mobile payment account product and in response, transmits application form data for the new product back to the mobile device 3, together with a digital document including pre-application terms and conditions (T&C). It is appreciated that the pre-application terms and conditions may be particular to the product and may set out specific product terms that the user must review and accept before the automated application process for the product can proceed. The digital document can be generated by the middleware server 16 in real-time, and can be a customer specific product disclosure based on user details. In an embodiment, the digital document is generated from a template document, and populated with user-specific details. Accordingly, at step S20-13 the mobile device 3 receives the application form data and the T&C digital document, and may store the T&C digital document in the secure memory 4. The digital document is stored by the

mobile device 3 for a predetermined amount of time, such as for 15 business days. At step S20-15, the mobile device 3 displays the T&C digital document to the user. Figure 21e shows an exemplary wallet display screen 51-55 displaying the user navigatable T&C digital document, and a user input button 63-41 that the user can press to indicate acceptance of the pre-application terms and conditions.

[00136] In this embodiment, the mobile device 3 is configured to transmit an indication to the middleware server 16 that the user is viewing the T&C digital document, at step S20-17. It is appreciated that this indication is in the form of a data message. Alternatively, the mobile device 3 may be configured to provide a plurality of messages to the middleware server 16 as the user navigates through the digital document to indicate the user's progress through the terms and conditions. The middleware server 16 can be configured to automatically update the tracked progress of the user's application process in response to receipt of the indication that the T&C digital document is being viewed.

[00137] At step S20-19, the mobile device 3 receives user input indicating acceptance of the pre-application terms and conditions. In response, the mobile device 3 transmits a further indication to the middleware server 16 that the user has accepted the terms and conditions, at step S20-21. The middleware server 16 is then configured to automatically update the tracked progress of the user's application process in response to receipt of the indication that the user has accepted the pre-application terms and conditions. After the user has input acceptance of the terms and conditions by pressing the user input button 51-56, the mobile device 3 displays one or more of the "apply for new product" wallet screens 26-4 to prompt for and receive user input of details to complete the application for the desired mobile payment account product, at step S20-23. After the user has completed the application form displayed via the "apply for new product" wallet screens 26-4, the mobile device 3 transmits the completed application form data to the middleware server 16 to initiate the new mobile payment account provisioning process. This provisioning process includes approving the user's application, as well as creating, transmitting and securely storing inactive mobile payment account data on the mobile device 3, as discussed in the embodiments above. Accordingly, at step S20-25, the middleware server 16 is arranged to create a new

mobile payment account for the user in accordance with the user selected mobile payment account product. In addition, the inactive mobile payment account data 6 is provisioned by the middleware server 16 to the mobile device 3 and stored in the secure memory 4. If the user's application for a new product cannot be automatically approved by the account management system 7 and/or the payment account issuer 10, the user is notified that the decision is pending manual intervention. Once a final decision has been made, notification that the application has been approved or declined is communicated to the user, for example, via a message transmitted to the mobile device 3 or online through a check application status web page.

[00138] In this embodiment, after the inactive mobile payment account has been provisioned to the mobile device 3 at step S20-25, the middleware server 16 transmits a post-application cardmember agreement (CMA) digital document to the mobile device 3 at step S20-27, including further specific product terms particular to the product that the user must review and accept in order to complete the application process. It is appreciated that the CMA digital document may alternatively be transmitted to the mobile device 3 together with the provisioned mobile payment account data 6. At step S20-29, the mobile device 3 receives the CMA digital document and may store the digital document in the secure memory 4. At step S20-31, the mobile device 3 displays a notification to the user that the application for the selected product has been approved, together with or followed by display of the received CMA digital document. In a similar manner as described above with reference to the T&C digital document, the mobile device 3 is configured to transmit one or more messages to the middleware server 16 as the user is navigating through the CMA digital document via the mobile device 3. Figure 21f shows an exemplary wallet screen 51-56 displaying the user navigatable CMA digital document, and a user input button 63-42 that the user can press to indicate acceptance of the post-application clauses of the agreement.

[00139] At step S20-35, the mobile device 3 receives user input indicating acceptance of the CMA, and in response, transmits a message to the middleware server 16 to indicate that the user has accepted the post-application agreement. At step S20-37, the middleware server 16 receives the indication of user acceptance of the CMA and can be configured to automatically update the tracked progress of the user's application

process with the indication that the user has accepted the post-application CMA. After the user has input acceptance of the CMA, the mobile device 3 proceeds at step S20-39 to the mobile payment account activation process as described in the embodiments above. Once the activation process has been completed, the activated mobile payment account in the electronic wallet of the mobile device 3 can then be used to carry out contactless payment transactions as described in the embodiments above.

[00140] An alternative embodiment will now be described for facilitating further monitoring and tracking of the mobile payment account product application process. In particular, this alternative embodiment enables tracking of user navigation through a digital document prior to user input of acceptance. In the fourth embodiment described above, the mobile device 3 receives a digital document from the middleware server 16, for example the T&C or CMA digital document, and waits for user input of acceptance of terms and conditions or of the CMA. It is mentioned above that the mobile device 3 is configured to transmit one or more messages back to the middleware server 16 indicating the user's progress through the digital document. In this alternative embodiment, an enhanced digital document is described with reference to Figure 22 for facilitating enhanced monitoring and tracking of user navigation through the document. As shown in Figure 22, a digital document 81 has a hierarchical document structure including a plurality of sections each with a respective heading, with a portion 82-1 of the digital document 81 being viewable at any one time via the display 25 of the mobile device 3. It is appreciated that the amount of the digital document 81 that is viewable at one time depends on the hardware capability of the mobile device 3 such as the display resolution. It will be further appreciated that the digital document 81 can be displayed as a plurality of successive pages of the document, or alternatively can be displayed as a single scrollable document. For example, in the digital document 81 illustrated in Figure 22, navigation through the digital document 81 may include display of an initial portion 82-1 of the document, typically the start of the document, followed by one or more intermediary portions 82-2, and finally to a portion 82-3 corresponding to the end of the digital document 81 including the user selectable button 63-41 to confirm acceptance of the clauses in the digital document 81. User navigation throughout the digital document 81 does not need to be performed in a linear manner. As a further

alternative, the wallet application module 8 is configured to enable user configuration of the amount of the document to be displayed, for example, via a zoom function.

[00141] In the exemplary T&C digital document illustrated in Figure 22, three sub-sections 83-1, 83-2, 83-3 are shown corresponding to respective clauses indicated by the sub-headings 85-1, 85-2, 85-3. The sub-headings 85 are presented at the beginning of the digital document 81 as a list of user selectable links or bookmarks to the respective position in the digital document. The links effectively provide efficient user navigation to the respective portion of the digital document, as illustrated by the navigation arrow 87. In this alternative embodiment, the digital document 81 includes embedded data for respective locations in the digital document 81, illustrated schematically in Figure 22 as dashed boxes 89-1, 89-2 and 89-3 located after each section 83-1, 83-2 and 83-3, respectively in the digital document 81. When a particular portion of the digital document 81 associated with such an embedded data item 89 is displayed by the mobile device 3, the embedded data 89 triggers the mobile payment account wallet application module 8 to transmit a message to the middleware server 16 to indicate that the user has viewed that portion of the digital document 81. In this way, the alternative embodiment advantageously facilitates enhanced monitoring of user navigation throughout a digital document and more detailed tracking of the automated application progress.

[00142] Additionally, by providing enhanced monitoring of user navigation throughout a digital document, the account management system 7 and the payment account issuer 10 are able to automatically ascertain with increased confidence that a user has thoroughly viewed the pre-application T&C and the post-application CMA terms and clauses. In a further alternative embodiment, the middleware server 16 is further configured to determine when one or more portions of a digital document has not been viewed by the user, and to then transmit a message to prompt for confirmation of consent to the respective terms or clauses.

[00143] In yet a further alternative embodiment, the mobile device 3 is further configured to track user review of the digital documents including one or more of monitoring of time stamps associated with when the digital document, or each portion of the digital document, is viewed, the areas reviewed and consented, and the location

of review for example via Global Positioning System functionality of the mobile device 3.

Fifth Embodiment

[00144] A fifth embodiment of the invention will now be described, using corresponding reference numerals to those of preceding figures where appropriate for corresponding elements. Referring to Figure 23, the mobile payment system 501 comprises a mobile device 3, a merchant's electronic Point Of Sale (POS) terminal 5 as commonly known in the field, and an account management system 7 associated with a payment account issuer 10, as described in the embodiments above.

[00145] In this fifth embodiment, a user associated with the one or more mobile payment accounts configured on the mobile device 3 is provided with an online account configured at the account management system 7 to facilitate secure online access to information and account management services in a secure manner via the Internet 30. The account management system 7 additionally provides for secure registration of the user's online account after a mobile payment account has been provisioned on the user's mobile device 3. As illustrated in Figure 1, the user can register and store online account data 59 in a web module 57 in the account management system 7 via a computing device 2 including a web browser 58 that is able to communicate data to and from the web module 57 over one or more networks, for example, the Internet 30 in accordance with the embodiment described herein. In an alternative embodiment, the mobile device 3 may instead be configured to include a web browser 58 for facilitating the online account registration process. It is appreciated that although the web module 57 is provided in the middleware server 16 in the exemplary embodiment, the web service functionality of the web module 57 may instead be provided in a separate web server in the account management system 7.

[0019] As will be described in more detail below, the registration process uses information that is stored securely on the account management system 7 and the mobile device 3, which is not transmitted over the Internet 30 or the cellular telephone network 11. This secure information is an encryption key 60 that is securely stored in the middleware server 16 of the account management system 7. The same encryption key 60 is stored in the secure memory 4 of the mobile device 3, for example, as data

securely embedded in a wallet application module 8. A passcode generator, in particular, a cryptography module 61 in the middleware server 16, uses the encryption key 60 to generate a one-time passcode that is used to verify the user during the online account registration process. The cryptography module 61 may also be configured to generate the one-time passcode based on additional information such as the user's Mobile Directory Number (MDN), a hardware identifier of the mobile device, and/or a time-based element such as a session identifier. The one-time passcode is generated using known technology, for example, via a counter or cryptogram generator, and the one-time passcode expires based upon the passing of a time period set at the web module 57. The generated passcode may take any respective form, and may be composed of numeric or alphabetic symbols, non-alphanumeric symbols, or a combination of such symbols. A similar passcode generator, in particular, a cryptography module 62, is provided in the secure memory 4 of the mobile device 3, for example, as executable processing instructions in the wallet application module 8, for generating the same one-time passcode. The cryptography module 61 in the middleware server 16, may instead be provided as a separate unit in the account management system 7 with a secure communication path to the web module 57, and the cryptography module 62 in the mobile handset 3 may instead be provided as a separate application module or hardware unit in the secure memory 4.

[0020] In this way, the account management system 7 is able to advantageously provide for secure and efficient user registration of an online account, associated with the user's mobile payment accounts. In this way the account management system 7 ties the mobile solution to the web channel, reduces the ability for fraudsters to compromise customer identification and verification (ID&V) information through malicious software at end user computing devices because the web registration process no longer requires use of a physical plastic card, information (e.g. the CVV value) or ID&V information. The online account registration process also advantageously performs a two-factor authentication prior to registration by utilizing information that must be present and available (the mobile device 3 with the encryption key 60) as well as information that is known only to the user (for example, a user configured PIN as will

be described below). This further reduces payment account compromise by malicious code.

[00146] Figure 24 shows the elements of a mobile device 3 according to the fifth embodiment. As shown in Figure 24, the mobile device 3 is a mobile handset including components as described in the embodiments above. In the present embodiment, another plurality of wallet screens in the mobile payment wallet application module 8 are provided as "online registration" wallet screens 26-5 which are displayed in response to user selection of an option to register an online account associated with a mobile payment account, as will be described in more detail below. It is appreciated that the mobile payment wallet application module 8, which is stored securely in the secure memory 4 of the mobile device 3 in this embodiment, is schematically illustrated as forming part of the handset operating system and hardware 28 in Figure 24.

[00147] A more detailed description of the operation of the components in this fifth embodiment will now be given with reference to the flow diagram of Figure 25. Figure 25 describes a computer-implemented process for provisioning and activating a mobile payment account using the mobile device 3 in communication with the account management system 7, and for creating, activating and securely registering an associated online account. As shown in Figure 25, the process begins at step S25-1 where the wallet application module 8, including the authentication and payment applications, are prepared by the account management system 7 and transmitted to the secure element 4 of the mobile device 3 via the cellular telephone network 11 as discussed above. The wallet application module 8 is provided with a security mechanism for accessing the application data, by way of a user configurable application PIN in this embodiment. Accordingly, the first time the wallet application module 8 is received and stored in the mobile device 3, the requirement for input of an application PIN to access the wallet application module 8 is disabled as illustrated by step S25-3 because the user has yet to configure a PIN for the application. It is appreciated that the application PIN may take any respective form, and may be composed of numeric or alphabetic symbols, non-alphanumeric symbols, or a combination of such symbols. In alternative embodiments, other forms of user identification can be used to verify and validate a user wishing to access the wallet application module 8, such as using

biometrics including one or more of finger or hand print scanning, face recognition, DNA profiling, iris or retina recognition, voice recognition, and drawl pattern matching.

[0033] At step S25-5, payment account data in the wallet application secure data 6 for an inactive mobile payment account is received by the mobile device 3 and stored in the secure element 4. The payment account data may be received by the mobile device 3 via any appropriate data communication channel or mechanism. Once the payment account data has been stored in the secure element 4, the wallet application module 8 displays, at step S25-7, an indication that an inactive mobile payment account is available for activation on the mobile device 3. As discussed above, the user is provided with an online account associated with the mobile payment account. The web module 57 of the account management system 7 creates an online account (accessible via the Internet) for the user at step S25-9. The online account may initially include basic information associated with the user and the online account such as a unique account name or identification number of the user's mobile device (for example a unique Mobile Directory Number of the mobile handset), as well as shared information (for example, the shared encryption key 60) that is used for cryptographic functions when the user registers the online account as will be discussed later. A user may preferably be associated with a single online account that is associated with each of the user's one or more mobile payment accounts. Alternatively, the user may be associated with one online account for each mobile payment account.

[0034] At step S25-11, a user validation process is conducted in response to the user launching the wallet application module 8 and selecting the inactive mobile payment account to activate. An exemplary user validation process involving a sequence of identification and verification questions is described in the above embodiment, although any alternative process may be used to validate the user of the mobile device 3 via the wallet application module 8. Once the user has been validated at step S25-11, the middleware server 16 generates and transmits an unblock command to the wallet application module 8 of the mobile device 3, at step S25-13. Upon receiving the unblock command, the wallet application module 8 prompts the user to enter an application issuer PIN and a trust phrase, which are securely stored in the wallet application module 8 in the secure element 4 at step S25-15. After the user input

application issuer PIN has been set, the wallet application module 8 in the mobile device 3 transmits, at step S25-17, an authorization validation flag and the user input trust phrase to the middleware server 16 of account management system 7 via the secure and trusted communication connection established by the communications server 13. The middleware server 16 then communicates the received user input to the web module 57 to securely store the user input trust phrase in the online account data associated with online account created for that user at step S25-9. At step S25-19, the web module 57 activates the online account by configuring data identifying a state of the online account to indicate that the online account is ready for registration by the user.

[0035] At step S25-21, the middleware server 16 activates the mobile payment account and transmits an indication to the mobile device 3 that the mobile payment account is activated for conducting contactless transactions via the mobile device 3. In this embodiment, the user is prompted to proceed with the online account registration process as illustrated by step S25-23. The user may be directed to an appropriate web page URL to proceed with the registration process in any known manner, via a wallet screen 24 displayed by the mobile device and/or by an e-mail automatically generated and sent by the web module 57 to an e-mail address previously provided by the user.

[0036] The online account registration process will now be described in more detail with reference to Figure 26. Reference is also made to Figure 27, which comprises Figures 27a to 27d, schematically illustrating exemplary display screens that can be presented to a user on the mobile device 3 in the online account registration process, and to Figure 28, which comprises Figures 28a to 28d, schematically illustrating exemplary display pages that can be presented to a user via the web browser 58 on the computing device 2 in the online account registration process.

[0037] The online account registration process begins with the user launching the web browser 58 of the computing device 2 and requesting the registration web page from the web module 57 of the account management system 7 as prompted at step S25-23 discussed above. In response to requesting the registration web page via the appropriate URL, the registration web page is received and displayed to the user at step S26-1, as illustrated in Figure 26. In this embodiment, the web page is configured to

prompt the user to enter a MDN, for example, as an input box 68-59 of the web page 65-1 as schematically illustrated in Figure 27a. At step S26-3, the user enters a MDN, and the user input data is transmitted to the web module 62. The validity of the user input data may be performed by the web browser 58 and/or the web module 62. At step S26-5, the web module 62 receives the user input MDN and retrieves the stored online account data 59 associated with the user input MDN, including the securely stored cryptography key 60 for that user's online account. At step S26-7, the web browser 58 displays a subsequent web page received from the web module 62 to prompt the user for input of a passcode as generated by the user's mobile device 3, within a predetermined amount of time (for example a window of two minutes from display of the subsequent web page by the web browser). Figure 27b schematically illustrates an example web page 65-2 confirming the user input MDN and prompting for input of a passcode in an input box 68-52. The web page can also include code or processing instructions to configure the browser to monitor for the authentication timeout at step S26-9. If the predetermined amount of time has not elapsed, the web browser 58 determines if the user input passcode has been received at step S26-11, and if not, continues to monitor for the user input within the predetermined time window. If at step S26-9, the web browser 58 determines that the user has not input a passcode within the predetermined time window, then the web browser may notify the user that the authentication input step has timed out and the user may be directed back to the initial registration web page to restart the registration process.

[0038] As discussed above, the user is prompted to enter a passcode that is generated by the cryptography module 62 in the wallet application module 8 of the user's mobile device 3. The user may initiate the passcode generation process by launching the wallet application module 8 at step S26-13 in response to the prompt at step S26-7. Alternatively, the user may use the wallet application module 8 to generate a passcode at any suitable time before receiving the prompt at step S26-7, once the user has set an application issuer PIN at step S25-15 and a mobile payment has been activated at S25-21. Figure 28a shows an example user interface 51-61 of the user's mobile device 3 for enabling the user to launch the wallet application module 8 by selection of a respective application icon 55 displayed by the handset operating system 28. Many other forms of

user interface are possible depending on the particular mobile device used to implement the present embodiment. After the user has launched the wallet application module 8, the mobile device 3 receives, at step S26-15, user selection of a menu option to generate a passcode for online account registration. In the example shown in Figure 28b, a "main menu" wallet screen 51-62 is displayed by the mobile device 3 to the user, providing a plurality of user selectable options for the electronic wallet. The user scrolls through the list of displayed options to highlight 64-51 and selects a desired menu option. In response to selection of the option to generate a passcode, the mobile device 3 displays an application issuer PIN input wallet screen 51-63 as shown in Figure 28c to prompt for user input of the application issuer PIN into an input field 68-56. At step S25-17, the wallet application module 8 can then check the user input PIN against the stored application issuer PIN that was set previously at step S25-15 to verify that the user is authorized to access the wallet application module 8 to generate a passcode. Once the user input PIN is verified, an authorization validation flag is set in the wallet application module 8.

[0039] At step S26-62, the wallet application module 8 validates that the authorization validation flag is set and then uses the cryptography module 62 to generate a passcode based on the encryption key 60 (that is also stored on the web module 62 in a secure manner) as discussed above. At step S26-21, the generated passcode is displayed by the mobile device 3 to the user for a predetermined amount of time (for example one minute from initial display of the generated passcode), as shown in the exemplary display screen 51-64 of Figure 28d. The wallet application module 8 monitors the amount of time that the passcode has been displayed to the user at step S26-23, and once the predetermined amount of time has passed, the wallet application module 8 displays, at step S26-25, a notification message to the user that the display operation has timed out. Processing may then return to step S26-17 to prompt the user to reenter the application issuer PIN in order to restart the process to generate a new one time passcode.

[00148] Returning now to step S26-11, as indicated by the dashed line from step S26-21, the web browser 58 receives user input of the generated passcode and transmits the user input passcode to the web module 62. In response to receipt of the user input passcode, the cryptography module 61 in the middleware server 16 is used to recreate a

passcode, at step S26-27, using the retrieved encryption key 60 that is stored securely in the web module (which is the same as the encryption key 60 stored securely in the mobile device 3). At step S26-29, the web module 62 compares the received user input passcode to the recreated passcode, and if it is determined at step S26-31 that the user input passcode matches the recreated passcode, then the user input passcode is determined to be valid. It is appreciated that in an alternative embodiment, the web module 62 may instead use the cryptography module 61 to generate and securely store a passcode for each online account prior to prompting the user to input a passcode generated on the mobile device at step S26-7. The online account registration process continues to step S26-33 where a further web page is transmitted to and displayed by the web browser 58 to prompt the user to set up a security question and answer for the online account. Figure 27c schematically illustrates an example web page 65-3 confirming the user's trust phrase 68-53 (as previously provided by the user at step S25-15 and transmitted to the middleware server 16 at step S25-17) and prompting for input of a security answer in an input box 68-54. The user input security answer is then transmitted to the web module 62 and stored in the online account data 59 for that user. In this embodiment, a further subsequent registration web page is transmitted to the web browser 58 to prompt the user to enter additional anti-phishing information at step S26-35. Figure 27d schematically illustrates an example web page 65-4 prompting for input selection of an image 68-54 for the online account, as well as user input of a username 68-55 which may be used to access the online account instead of the user's MDN. The user input additional information is then transmitted to the web module 62 and stored in the online account data 59 for that user to complete the online registration process.

Sixth Embodiment

[00149] A sixth embodiment of the invention will now be described, using corresponding reference numerals to those of preceding figures where appropriate for corresponding elements. Referring to Figure 30, the mobile payment system 601 comprises a mobile device 3, a merchant's electronic Point Of Sale (POS) terminal 5 as commonly known in the field, and an account management system 7 associated with a payment account issuer 10, as described in the embodiments above.

[00150] As shown in Figure 30, in this embodiment, the mobile device 3 includes a plurality of secure wallet application modules 8a storing computer-implementable processing instructions in the secure memory 4. The processing instructions are used to control the operation of the mobile device 3, to facilitate the application for and management of one or more mobile payment accounts on the mobile device 3, and to handle the process of conducting a transaction with a merchant via the electronic POS terminal 5. A payment transaction with a merchant via the electronic POS terminal 5 is facilitated using a mobile payment account on the mobile device 3 to effectively transfer funds from the mobile payment account on the mobile device 3, or an associated payment account issuer 10, to the merchant. Other forms of transactions will be apparent to the skilled person to facilitate ticketing, coupons, and other activities.

[00151] The secure wallet application modules 8a can be implemented as one or more software components of an operating system running on the mobile device 3 or implemented as one or more separate software applications installed on the mobile device 3. In this embodiment, the secure wallet application modules 8a comprises an authentication module 48 for verifying or validating a user to conduct a transaction using a provisioned mobile payment account, and a plurality of transaction modules 49 for facilitating transactions using an activated mobile payment account after the user has been validated. As will be described in greater detail below, one authentication module 48 associated with a single controlling passcode is provided to dictate usage to a series of subordinate transaction modules 49 that are all within the ownership rights of the security domain for the collection of modules of a particular issuer. The authentication and transaction modules described herein are preferably software applications (such as applets), and can be configured to run as background applications on the mobile device 3. The software applications monitor receipt of messages or events and activate upon receipt of appropriate messages or events so as to carry out the above operations. The software applications can alternatively be launched by the user. Alternatively, the secure wallet application modules 8a (that is, the authentication module and transaction modules) are loaded into a virtual machine of the mobile device 3 to provide the functionality of the present embodiment.

[00152] A secure mobile payment account provisioning and activation process can be carried out between the mobile device 3 and the account management system 7, as described in the embodiments above. The activated mobile payment account data stored in the secure memory 4 of the mobile device 3 is then used to carry out payment transactions with a merchant electronic POS terminal 5 via the contactless communication link 9, whereby a requested amount of funds is transferred from the mobile payment account stored in the mobile device 3 to the merchant's bank 12. Techniques and protocols for implementing the authorization and transfer of funds between the merchant POS terminal 5, the merchant bank 12, and the payment account issuer 10 via the payment association network 17 are well known to those skilled in the art and are therefore not described further herein.

[00153] Figure 31 shows the elements of the mobile device 3 according to the sixth embodiment of the present invention. As shown in Figure 31, the mobile device 3 is a mobile handset including components as described in the embodiments above. In the present embodiment. the mobile device 3 also includes a plurality of additional mobile payment wallet application modules 20 which are not stored in the secure memory 4. The additional wallet application modules 20 store processing instructions used to control the operation of the mobile device 3 to perform various mobile payment account processes using the secure wallet application modules 8a discussed above. As shown in Figure 31, a plurality of application modules 20-1, 20-2, 20-m, 20-n, for example, are provided for carrying out transactions with a plurality of different payment account issuers (referred to as Issuer-1, Issuer-2, … Issuer-n) as well as a non-issuer application module 20m for carrying out non-issuer related operations. Each application module 20 is operable to call the secure wallet application modules 8a of the corresponding issuer in order to complete the requested transaction after user validation, as will be described in greater detail below. The additional wallet application modules 20 can also include an account creation sub-module and an account activation sub-module (not shown) storing processing instructions to create a request for a new mobile payment account if desired and to carry out a secured account validation and activation processes in response to user input from the keypad 25 as described in the embodiments above.

[00154] Figure 31 also schematically illustrates the secure memory 4 of the present embodiment including a wallet security domain 31 associated with one or more payment account issuers and other service providers. In this embodiment, the wallet security domain 31 (corresponding to the issuer security domain 31 in the previous embodiments) includes a security domain 36-1 associated with the payment account issuer 10 (referred to as Issuer-1) and the secure wallet application modules 8a for Issuer-1. The secure wallet application modules 8a are provided as an applet package associated with Issuer-1, and include the authentication applet instance 48 and a plurality of transaction applet instances 49 which enable the transaction processing functionality using an activated mobile payment account. The authentication applet instance 48 and the plurality of transaction applet instances 49 correspond to the authentication module 48 and the transaction modules 49 respectively shown in Figure 30. The wallet security domain 31 also includes one or more other service provider security domains 37 each associated with respective one or more other wallet application modules 54. The wallet security domain 31 also includes wallet application secure data 6 for use by the wallet application modules 8a. The payment account data is also securely stored in the wallet security domain 31, for example, within the wallet application secure data 6.

[00155] The wallet security domain 31 also includes a Proximity Payment System Environment (PPSE) module 41 (corresponding to the PPSE package in the previous embodiments), defining application functionality associated with transaction processing functionality and, in particular, for handling communications with a contactless reader of the POS terminal 5 to identify which of the one or more mobile payment accounts is to respond. The PPSE module 41 facilitates an additional application layer level of control of the transaction processing functionality between a respective one of the transaction applet instances 49 and the contactless communication link interface 47. The PPSE module 41 is a program module inside the secure memory 4 but is generally provided in a security domain associated with and controlled by the owner of the secure memory 4 and not with a specific payment account issuer 10, thus providing for segregation that allows for privacy among issuers and mobile operators.

[00156] In this embodiment, a central authentication applet 48 residing in the secure memory 4 in the Issuer-1 security domain 36-1 is configured to control verification of the passcode. The central authentication applet 48 is a program that manages and verifies input of the passcode for a mobile application, such as an electronic wallet, as well as managing the passcode communication to the subordinate transaction applets 49 that will control its use over the contactless communication link interface 47 through the PPSE module 41.

[00157] Transaction applet instances 49 also reside within the same span of control of an issuer security domain 36-1. The roles of the transaction applets 49 are for implementing contactless link based transaction and actions such as payment, ticketing, coupon redemption, or other offer interactions. These transaction applets 49 can be defined by an association and are licensed by the authentication applet's issuer and security domain owner. The transaction applets 49 include all the logic and control to execute the associated transactions once the passcode has been verified as being entered correctly by a user.

[00158] Typically, execution of each applet is controlled within a security domain to control scope of execution and ability to control the applet. Only those applets with the right security domain access can execute, modify or change the applet. Additionally, each applet has a finite set of exposed interfaces for interacting with the applet over specified channels. Preferably, the authentication applet 48 is used as a central passcode manager among a series of associated subordinate applets associated with the same payment account issuer 10.

[00159] Figure 32 is a block diagram showing the main functional elements of the mobile device 3 when configured to execute processing instructions of the transaction applets 49 and the authentication applet 48, according to the sixth embodiment of the invention. As will be discussed in greater detail below, the Issuer-1 application module 20-1 calls the secure wallet application module 8a associated with the payment account issuer 10 to conduct a transaction process, for example, when a user waves the mobile device 3 past the contactless communication interface of the POS terminal 5. As shown in more detail in Figure 32, the Issuer-1 authentication applet 48 in the secure wallet application module 8a in this embodiment includes a passcode

verifier 77a functional element for verifying a passcode 79a (referred to as PIN-1) associated with all of the transaction applets 49a associated with Issuer-1, and a transaction applet interface 80 for communicating the success or failure of user validation by the passcode verifier 79a to the Issuer-1 transaction applets 49a.

[00160] The other application modules 20 provided in the operating system 28 can be configured to communicate with respective secure applets to conduct different transaction processes and functions after user validation using different mechanisms. For example, Figure 32 shows an example of a typical secure wallet application module 8b associated with a different payment account issuer (referred to as Issuer-2) that is optionally provided in addition to the Issuer-1 secure wallet application module 8a. This additional secure application module 8b can communicate with the Issuer-2 application module 20-2 to conduct transaction processes associated with Issuer-2. In this example, the Issuer-2 application module 8b is not configured with a respective central authentication applet and instead provides a passcode verifier 77b in the Issuer-2 transaction applet 49b for verifying a passcode 79b (referred to as PIN-2) that is separately associated with the transaction applet 49b associated with Issuer-2. Figure 32 also shows a non-issuer application module that is configured to provide electronic wallet functionality to a user that is not associated with any particular payment account issuer 10, for example, through a Mobile Network Operator (MNO) secure domain applet 84 for processing and performing functions and actions associated with the mobile network operator, through the cellular telephone network interface 33.

[00161] A more detailed description of the operation of these components in this first embodiment will now be provided with reference to the flow diagram of Figure 4 which illustrates a computer-implemented process for a contactless mobile transaction where the plurality of transaction applets 49a associated with a payment account issuer 9 uses a central authentication applet 48 for passcode validation. As shown in Figure 33, the mobile transaction process begins at step S33-1 where the contactless communication link interface 47 and PPSE module 41 pick up or receive a signal from the POS terminal 5 for initiating a transaction. The POS terminal 5 typically sends out a request associated with a specific type of transaction, such as payment or ticketing. In response, at step S33-3, the contactless communication link interface 47 is instructed by

the mobile operating system 28 to use the PPSE module 41 to initiate a transaction. The PPSE module 41 typically stores a list of the possible executable application identifiers (AID) within the secure memory 4 based upon categories such as payment, ticketing and the like.

[00162] The PPSE module 41 determines at step S33-5 a specific AID of a transaction applet 49a for execution of the transaction, from the PPSE's list of AIDs, such as an AID for an application which the user has previously selected as their default for that transaction category or type. The PPSE module 41 responds to the POS terminal 5 with the specific AID. At step S33-7, the POS terminal 5 receives and optionally verifies that the AID is within an allowed set or range for that transaction category and proceeds to ask the mobile device 3 in subsequent interactions to execute that specific AID to complete the transaction. Accordingly, at step S33-9, the contactless communication link interface 47 receives a new request message to carry out a transaction using one of transaction issuer applets 49a as identified by the AID.

[00163] In this embodiment, the subordinate transaction applet 49a performing the transaction will call the interface 80 on the authentication applet 48, at step S33-11, to verify that the correct passcode 79a was entered by the user. It will be appreciated that the user can authenticate to the authentication applet 48 prior to engaging with the POS terminal 5, whereby the user selects the mobile payment account they wish to use for a transaction, enters in a passcode, and the user input passcode is transmitted to the authentication applet 48 for verification. If the passcode verifier 77a determines that the passcode 79a is correct and the authentication applet 48 is in a state where it is allowing transactions, the authentication applet 48 will allow the next transaction requested by a transaction applet 49a to proceed. Alternatively, the authentication applet 48 is configured to process validation of the controlling passcode (PIN-1) as required in response to a request from the transaction applets 49a.

[00164] Therefore, at step S33-13, the authentication applet 48 will respond with a permission to perform the requested transaction and any supporting data for the applet to use in the transaction. At step S33-15, the subordinate transaction applet 49a determines from the received information if passcode authentication was successful. If the authentication applet 48 was not able to validate the user input passcode, then at step

S33-17, the transaction applet 49a proceeds to block the transaction from happening and map to a specific error code. On the other hand, if passcode authentication was successful, then at step S33-19, the transaction applet 49a proceeds to allow the transaction to take place.

[00165] When processing the transaction request, the transaction applet 49a determines the required transaction detail information to transmit the POS terminal 5 based upon factors such as whether the passcode verification is in the proper state. Details of how the transaction applets 49a perform processing to carry out an allowed transaction are well known to those skilled in the art and are therefore not described further herein. Once the transaction is performed, the Issuer-1 wallet applet can prevent further transactions without subsequent authentication. This also prevents "virtual pickpocketing" by ensuring only the intended transaction is performed.

[00166] The authentication applet 48 can also process the request from the subordinate transaction applet 49a to ensure the request is properly made from an allowed transaction applet 49a, before starting the verification process. The authentication applet 48 stores the passcode 79a and an allowed number of possible user input attempts of the passcode before blocking any transactions from proceeding before a passcode reset. If the number of incorrect entries exceeds the configured maximum entries before a successful passcode validation, the authentication applet 48 will not allow any more transaction attempts. Once locked, a controlling passcode reset process is typically performed by the issuer of the authentication applet 48 through a trusted service manager connection into the secure element 4 where commands are sent to the secure element 4 to reset the counter in a conventional manner.

[00167] The initial instantiation and setting of the controlling passcode is a process managed by the payment account issuer 10 and the issuer's TSM server 18. The issuer's security domain 36 can be set up by the TSM server 18 and the authentication applet 48 can be installed and instantiated into the issuer's security domain 36. The TSM server 18 can then send commands to make the authentication applet 48 available for execution and initialize the passcode into an initial state along with passcode counters.

[00168] The authentication applet 48 is configured in the issuer's security domain 36 so that it can limit the interfaces allowed to execute commands to a finite set of wallet applications in the mobile handset operating system, as well as verification requests coming from the transaction applets 49a.

Seventh Embodiment

[00169] A seventh embodiment will now be described using corresponding reference numerals to those of preceding figures where appropriate for corresponding elements. Figure 34 is a block diagram showing the main functional elements of the mobile device 3 when configured to execute processing instructions of the transaction applets 49 and the authentication applet 48. In the sixth embodiment described above, single passcode control is provided by the central authentication applet 48 in the issuer wallet applet 8a controlling the passcode verification for the subordinate transaction applets 49a. In this embodiment, the passcode verification process involves a passcode requestor 88 in the subordinate transaction applet 49a directly calling the authentication applet 48 to retrieve an associated transaction applet passcode for automatic passcode verification by a passcode verifier 90 in the transaction applet 49a. The authentication applet 48 stores its known value of the transaction passcodes 86 internally in the secure element 4 for the transaction applets 49a to use. In this way, the security mechanism of this embodiment effectively simulates user passcode entry to manage multiple passcodes to multiple applets.

[00170] As will be discussed in greater detail below, and in accordance with this seventh embodiment, the Issuer-1 authentication applet 48 in the secure wallet application module 8a also provides a passcode verifier 77a functional element for verifying a passcode 79a (referred to as PIN-1) associated with the Issuer-1 wallet applet 8a and a transaction applet interface 80 for communicating with the plurality of issuer-1 transaction applets 49a. The authentication applet 48 stores a plurality of Issuer-1 transaction applet passcodes 86 associated with the Issuer-1 transaction applets 49a (referred to as PIN-1a to PIN-1n), in addition to the single controlling passcode 79a as in the first embodiment. Additionally, each of the subordinate Issuer-1 transaction applets 49a in this embodiment stores a respective applet passcode 91, corresponding to the transaction applet passcodes 79a stored and controlled by the authentication applet

48, and requires verification of the transaction applet passcode 91 as part of the authentication process.

[00171] Figure 35 illustrates a computer-implemented process for a contactless mobile transaction where the plurality of transaction applets 49a associated with a payment account issuer 10 perform passcode validation for a transaction process by requesting the passcode from the central authentication applet 48. As shown in Figure 35, the mobile transaction process begins at step S35-1 where the contactless communication link interface 47 and PPSE module 41 picks up or receives a signal from the POS terminal 5 for initiating a transaction. The processing steps up to S35-9 correspond to steps S33-1 to S33-9 of the sixth embodiment and are not repeated here for conciseness.

[00172] In accordance with this seventh embodiment, after the contactless communication link interface 47 has received the new request message at step S35-9, the subordinate transaction applet 49a performing the transaction will call the interface 80 on the authentication applet 48, at step S35-11, to request a passcode 79a to complete the transaction. In response, the Issuer-1 authentication applet 48 will determine if the single controlling passcode (PIN-1) 79a has been correctly entered by the user prior to the transaction request, or proceed to request input of the single controlling passcode by the user as described above. If the passcode verifier 77a determines that the passcode 79a is correct and the authentication applet 48 is in a state where it is allowing transactions, the authentication applet 48 will retrieve the transaction applet passcode 86a (PIN-1a) for the requesting transaction applet 49a and proceed to communicate the retrieved transaction applet passcode 86a back to the Issuer-1 transaction applet 49a. Alternatively, the authentication applet 48 is configured to process user input and verification of the single controlling passcode PIN-1 using the passcode verifier 77a in the authentication applet 48 as required before responding to the request from the transaction applets 49a.

[00173] Therefore, at step S35-13, the authentication applet 48 will respond with a retrieved transaction applet passcode 86 and any supporting data for the applet to use in the transaction. At step S33-15, the transaction applet passcode 86 received the authentication applet 48 is checked by the passcode verifier 90 in the subordinate

transaction applet 49a to determine if it matches the stored transaction applet passcode 91. If the passcodes do not match, then at step S35-17, the transaction applet 49a proceeds to block the transaction from happening and map to a specific error code. On the other hand, if the transaction applet passcode authentication was successful, then at step S35-19, the transaction applet 49a proceeds to allow the transaction to take place.

[00174] In a further alternative method, the authentication applet 48 can be used to broadcast the appropriate transaction passcode to the designated transaction applet for use, after validating the user using a single controlling passcode. In this alternative, the user using the wallet application would provide the authentication applet 48 with the controlling passcode 79a along with which transaction applet is to be used for the subsequent transaction. The controlling passcode 79a would be verified by the passcode verifier 77a in the authentication applet 48 in the same manner as the sixth embodiment, but instead of waiting for a transaction applet 49a to ask for a transaction applet passcode for verification, the authentication applet 48 would communicate to the transaction applet 49a with the appropriate transaction passcode 79a.

[00175] The authentication applet 48 can effectively translate any transaction passcodes 79a necessary to the transaction applets 49a if necessary. This can allow for the wallet application 8a to not necessarily use the same passcode 79a or even restrict the single controlling passcode 79a to the same mechanisms prescribed by the transaction applets 49a.

[00176] The transaction applets 49a in this embodiment can keep a respective predefined number of allowed passcode entry attempts, as described in the first embodiment. It will be appreciated that this should be minimally used as the authentication applet 48 is storing the appropriate transaction applet passcodes, and access control therefore limits access to the transaction applets 49a.

Summary and Advantages

[00177] In the above embodiments, a description of the components of a mobile payment account activation system embodying aspects of the present invention has been given. A detailed description has also been given of the functional operations of each component during various processes in the mobile payment system.

[00178] A number of advantages are achieved with the account management system described in the first embodiment above. As mentioned above, the account management system can advantageously activate a new mobile payment account for a mobile user in real time, as the computer-implemented user authentication and activation processes are automated by the account management system so that a mobile user can efficiently and securely activate an inactive mobile payment account provisioned on a mobile device, without requiring manual intervention to provide additional verification in order to complete the activation process, such as a preset pass code by way of a telephone call, or in person in store or in branch, or logging on to a website of an account issuer or bank through a web browser, or delivery of any authentication or verification documents between the user and the account issuer or bank by mail or post. The present invention thereby facilitates real time provisioning and activation of the mobile payment account ready to be used to carry out transactions at a merchant POS.

[00179] The account management system can also be configured to adjust a level of security relating to the user authentication and activation process depending for example on a determined risk of the mobile user. Therefore, a lower risk mobile user may have the additional convenience of a simplified activation process, whereas an unfamiliar or higher risk mobile user will have a more complicated activation process, thereby reducing the chances of fraudulent account activation and identity theft.

[00180] The above described account management system also has the advantage that the merchant POS terminal and the secure payment account issuers operate in a conventional manner. The system can therefore be easily incorporated into existing contactless mobile payment systems.

[00181] A number of advantages will be also understood from the above description of the second embodiment of the present invention.

[00182] In particular, the remote setting of a risk flag can prevent monetary loss by the issuing bank for low dollar transactions made by a perpetrator.

[00183] The solution allows the customer to easily self correct any possession activity verification without requiring an outbound contact from the issuing bank. The customer simply enters their passcode prior to making their next transaction.

[00184] The issuing bank can set the risk flag ahead of any transaction attempt by the customer at a merchant. The merchant checkout does not have to communicate a declined transaction attempt to the customer. If the merchant were an unattended vending machine, this error could cause customer confusion and frustration. The customer is able to correct their risk setting locally as part of the transaction flow.

[00185] The transaction information process flow with merchant point of sale systems is unchanged requiring no additional work by a merchant.

[00186] The second embodiment allows the bank to decide when a customer requires authentication of the payment account based upon flexible risk criteria.

[00187] The second embodiment also allow for remote management of local passcode verification counters to allow the bank to automatically ask for passcode verification after a configurable number of low dollar transactions.

Computer Systems

[00188] The computer servers of the account management system described herein may be implemented by computer systems such as computer system 1000 as shown in Figure 36. Embodiments of the present invention may be implemented as programmable code for execution by such computer systems 1000. After reading this description, it will become apparent to a person skilled in the art how to implement the invention using other computer systems and/or computer architectures.

[00189] Computer system 1000 includes one or more processors, such as processor 1004. Processor 1004 may be any type of processor, including but not limited to a special purpose or a general-purpose digital signal processor. Processor 1004 is connected to a communication infrastructure 1006 (for example, a bus or network). Various software implementations are described in terms of this exemplary computer system. After reading this description, it will become apparent to a person skilled in the art how to implement the invention using other computer systems and/or computer architectures.

[00190] Computer system 1000 also includes a main memory 1008, preferably random access memory (RAM), and may also include a secondary memory 610. Secondary memory 1010 may include, for example, a hard disk drive 1012 and/or a removable storage drive 1014, representing a floppy disk drive, a magnetic tape drive,

an optical disk drive, etc. Removable storage drive 1014 reads from and/or writes to a removable storage unit 1018 in a well-known manner. Removable storage unit 1018 represents a floppy disk, magnetic tape, optical disk, etc., which is read by and written to by removable storage drive 1014. As will be appreciated, removable storage unit 618 includes a computer usable storage medium having stored therein computer software and/or data.

[00191] In alternative implementations, secondary memory 1010 may include other similar means for allowing computer programs or other instructions to be loaded into computer system 1000. Such means may include, for example, a removable storage unit 1022 and an interface 1020. Examples of such means may include a removable memory chip (such as an EPROM, or PROM, or flash memory) and associated socket, and other removable storage units 1022 and interfaces 1020 which allow software and data to be transferred from removable storage unit 1022 to computer system 1000. Alternatively, the program may be executed and/or the data accessed from the removable storage unit 1022, using the processor 1004 of the computer system 1000.

[00192] Computer system 1000 may also include a communication interface 1024. Communication interface 1024 allows software and data to be transferred between computer system 1000 and external devices. Examples of communication interface 1024 may include a modem, a network interface (such as an Ethernet card), a communication port, a Personal Computer Memory Card International Association (PCMCIA) slot and card, etc. Software and data transferred via communication interface 1024 are in the form of signals 1028, which may be electronic, electromagnetic, optical, or other signals capable of being received by communication interface 1024. These signals 1028 are provided to communication interface 1024 via a communication path 1026. Communication path 1026 carries signals 1028 and may be implemented using wire or cable, fiber optics, a phone line, a wireless link, a cellular phone link, a radio frequency link, or any other suitable communication channel. For instance, communication path 1026 may be implemented using a combination of channels.

[00193] The terms “computer program medium” and “computer usable medium” are used generally to refer to media such as removable storage drive 1014, a hard disk

installed in hard disk drive 1012, and signals 1028. These computer program products are means for providing software to computer system 1000. However, these terms may also include signals (such as electrical, optical or electromagnetic signals) that embody the computer program disclosed herein.

[00194] Computer programs (also called computer control logic) are stored in main memory 1008 and/or secondary memory 1010. Computer programs may also be received via communication interface 1024. Such computer programs, when executed, enable computer system 1000 to implement embodiments of the present invention as discussed herein. Accordingly, such computer programs represent controllers of computer system 1000. Where the embodiment is implemented using software, the software may be stored in a computer program product and loaded into computer system 1000 using removable storage drive 1014, hard disk drive 1012, or communication interface 1024, to provide some examples.

[00195] Alternative embodiments may be implemented as control logic in hardware, firmware, or software or any combination thereof.

Alternative Embodiments

[00196] It will be understood that embodiments of the present invention are described herein by way of example only, and that various changes and modifications may be made without departing from the scope of the invention.

[00197] For example, in the embodiments described above, the mobile device includes a communication interface for facilitating communications over a respective type of contactless communication link. As an alternative, the mobile device may include a plurality of communication interfaces for enabling the plurality of transaction applets to carry out contactless communications over a plurality of respective types of contactless communication links. In this way, the mobile device would be capable of conducting contactless transactions over a combination of contactless communication links such as near field communication (NFC), infra-red and/or optical (eg. for bar code scanning), ultra-sonic, radio frequency (eg. RFID), wireless such as Bluetooth or Wi-Fi based on the IEEE 802.11 standards, and any other communication link that does not require direct physical contact.

[00198] As a further alternative, the mobile device may be additionally or alternatively configured for conducting mobile transaction operations over any other form of communication link that requires a contact and/or coupling of communication interfaces. In this case, the mobile device may include a plurality of transaction modules operable to process mobile transaction operations with a respective transaction account over a communication link via an associated communication interface of the mobile device. Preferably but not essentially, at least one of the transaction modules is configured for contactless transaction operations over at least one type of contactless communication link.

[00199] In the first embodiment described above, the mobile payment account is provisioned on a mobile handset which communicates with the account activation system via a cellular telephone network. As those skilled in the art will appreciate, instead of a mobile handset, other portable electronic devices configured for contactless payment with a merchant electronic POS and having suitable input and display means, may be adapted to carry out the functionality of real time provisioning and/or activation as described in the first embodiment. Additionally, those skilled in the art will appreciate that the portable electronic device may be configured to communicate with the account activation system via any other form of communication channel, such as a wired or wireless network connection, a Bluetooth connection, or the like. Alternatively, the mobile payment account data may be provisioned on the portable electronic device by means of data transfer for example via any suitable data communication path or by way of a computer readable medium.

[00200] In the first embodiment described above, the mobile device is provisioned with a mobile payment account by the account activation system through secure transfer of data representing the mobile payment account, which data including data defining an amount of pre-paid funds transferred from the user's payment account issuer and/or data identifying a user's account at a payment account issuer from which funds can be transferred to a merchant bank to complete a transaction. As those skilled in the art will appreciate, the mobile device may instead or additionally be securely provisioned with data representing one or more other types of accounts, such as an insurance account, a loyalty and rewards scheme membership or the like, and the

account activation system may be configured to conduct a secure data transfer to the mobile device of data representing such an account, for example including the account or membership number or any other type of secure reference number.

[00201] In the second embodiment described above, the mobile payment account is provisioned on a mobile handset which communicates with the account activation system via a cellular telephone network. As those skilled in the art will appreciate, instead of a mobile handset, other portable electronic devices configured for contactless payment with a merchant electronic POS and having suitable input and display means, may be adapted to carry out the functionality of real time provisioning and/or activation as described in the second embodiment. Additionally, those skilled in the art will appreciate that the portable electronic device may be configured to communicate with the account activation system via any other form of communication channel, such as a wired or wireless network connection, a Bluetooth connection, or the like. Alternatively, the mobile payment account data may be provisioned on the portable electronic device by means of data transfer for example via any suitable data communication path or by way of a computer readable medium.

[00202] In the second embodiment described above, the mobile device is provisioned with a mobile payment account through secure transfer of data representing the mobile payment account, which data including data defining an amount of pre-paid funds transferred from the user's payment account issuer and/or data identifying a user's account at a payment account issuer from which funds can be transferred to a merchant bank to complete a transaction. As those skilled in the art will appreciate, the mobile device may instead or additionally be securely provisioned with data representing one or more other types of accounts, such as an insurance account, a loyalty and rewards scheme membership or the like, and the account activation system may be configured to conduct a secure data transfer to the mobile device of data representing such an account, for example including the account or membership number or any other type of secure reference number.

[00203] In the second embodiment described above, the wallet application secure data stores a plurality of flags that are accessed and maintained by the payment and authentication applets. As those skilled in the art will appreciate, the flags are data

values indicative of one of a plurality of predefined states of an associated variable. In the second embodiment described above, separate flags are provided for the plurality of variables, each flag having a true or false state. Many alternative forms of representing the flags and variable states will be apparent to the skilled person.

[00204] In the second embodiment described above, the mobile device includes a user configured "PIN mode", one of "Always Required" and "Only As Necessary". As an alternative to the user setting whether or not a PIN is required, the POS can be configured to transmit a low transaction value indication to the mobile device, based on a predefined threshold for the transaction value. For example, a POS terminal of a vending machine can be configured to always transmit a low transaction value indication with any payment request message if all of the items in the vending machines are known to be under a predefined threshold value. In such an alternative, the mobile device would be configured to determine if PIN entry is required based on the received low transaction value indication. For example, the mobile device can be configured to require PIN entry if the message received from the POS terminal indicates that the transaction involves a high transaction value.

[00205] In the third embodiment described above, the mobile payment wallet application module on a mobile device provides a wallet screen for an account owner to select a contact person from the contacts data (phone book) of the account owner's mobile device. It is appreciated that the contacts data may be adapted to include data indicating whether or not a contact person is registered with the account management system or otherwise associated with a mobile device enabled to carry out contactless payment transactions with a mobile payment account. In such an alternative embodiment, the wallet screen may be configured to display a list of only those contact persons who are suitable for authorized use of the payment account via a provisioned and activated mobile payment account on the authorized user's mobile device.

[00206] In the third embodiment described above, an additional user is authorized to use the primary payment account to conduct payment transactions from the authorized user's mobile device. In an alternative embodiment, the account management system and the authorized user's mobile device may be further configured to enable the authorized user to perform predetermined selected account servicing tasks

on the primary payment account in addition to conducting payment transactions from the mobile payment account, via other service channels (web, phone, IVR etc). It is appreciated that authorizing such additional servicing may require establishing and confirming additional credentials from the authorized user. Accordingly, in this alternative embodiment, the wallet application module on the authorized user's mobile device may be configured to display a further wallet screen 24 to prompt the authorized user for additional information which may be used for multi-channel servicing. As shown in the exemplary display screen in Figure 16e, the authorized user may be prompted to securely input sensitive information such as the user's social security number, date of birth, and mother's maiden name, after the PIN has been set and activated. This input information may be securely transmitted by the mobile device to the account management system and utilized in different environments provided for configuration and access by the authorized user to selected servicing options for the mobile payment account, such as via the mobile device, a web-based interface or a conventional telephone call center, etc.

[00207] In the third embodiment described above, the process for confirming that the authorized user has input a correct activation code involves communication between the authorized user's mobile device and the middleware server in response to receipt of the user input activation code to the authorized user's mobile device. It is appreciated that as an alternative the activation code may instead be generated by the middleware server and transmitted to the authorized user's mobile device prior to receipt of the user input activation code by the authorized user's mobile device. The activation code generated by the middleware server could be provided as a PIN in the inactive mobile payment account data that is communicated to the authorized user's mobile device for account provisioning as described above. The generated activation code transmitted as a PIN in this way may be a one time PIN whereby user input of the activation code to the authorized user's mobile device forces a PIN reset upon successful entry of the activation code. In this way, the communication process for authenticating the additional authorized user is simplified because the generated activation code is stored locally on the authorized user's mobile device and need not be verified against the middleware server directly. Additionally, rather than the process requiring

communication back to the middleware server to check and force a PIN entry state (steps S14-61 and S14-63), the process in this alternative embodiment may proceed directly from confirming, by the authorized user's mobile device, that the user input activation code matches the one-time PIN to the step of prompting the authorized user for a PIN (step S14-65) in order to activate the provisioned mobile payment account, as described above.

[00208] In the third embodiment described above, the process of selecting an additional authorized user for a primary payment account is carried out through the wallet application module on the account owner's mobile device. It is appreciated that as an alternative the interface may instead be provided via a web interface over a secure communication channel between the mobile device and the account management system. An exemplary sequence of display screens according to this alternative embodiment is shown in Figure 17, which comprises Figures 17a to 17d. Figure 17a shows a log-in web interface display screen prompting the user to log in, and corresponds to the wallet display screen shown in Figure 15c. Figure 17b shows a web menu of user selectable options for servicing a particular payment account, including adding an authorized user and managing the mobile authorized users, which corresponds to the wallet display screen shown in Figure 15d. Figure 17c shows a web interface display screen prompting the user to enter details of the authorized user, which corresponds to step S14-15 or S14-17 discussed in the third embodiment above. Finally, Figure 17d shows a web interface display screen outputting the generated activation code, which corresponds to the wallet display screen shown in Figure 15g.

[00209] In the fourth embodiment described above, the application process is carried out automatically via a mobile device. The process of conducting and tracking the application process, and in particular of digital document delivery and monitoring of user navigation through a digital document, is applicable to alternative embodiments and scenarios involving one or more additional devices other than the user's mobile device. In a first exemplary alternative scenario, the process involves integration with the electronic POS terminal, and the digital document may instead or additionally be delivered to the POS to be printed out for presentation to the user. In a second alternative scenario similar to the first scenario, the POS is integrated in the process but

comprises a mobile device such as a portable computer or electronic tablet device. It is appreciated that in this scenario, the digital documents are formatted for optimized display and user interaction on the target mobile device. The digital documents are then delivered to the merchant mobile device in this scenario, in a similar manner as described above. In a third alternative scenario, the process is carried out from a merchant store via an Internet or web-based kiosk. It is appreciated that in this scenario, the digital documents are instead formatted for optimized display and user interaction via a web browser executed by the kiosk. In a fourth alternative scenario, the process involves the user's personal computer interacting with the account management system via the Internet and, similar to the third scenario, the digital documents are formatted for optimized display and user interaction via a web browser of the personal computer.

[00210] In the fourth embodiment described above, the application process involves delivery of a pre-application T&C digital document and a post-application CMA digital document. Alternatively, a single document is generated and transmitted to the mobile device. The digital document is transmitted to the mobile device at any time prior to the activation process, or is pre-loaded onto the mobile device prior to supply to the user, whereby the inactive provisioned mobile payment account can only be activated once the user has viewed and accepted the terms, conditions and/or agreement clauses.

[00205] In the embodiment described above, the registration process involves a sequence of separate registration web pages communicated from the web module to the computing device. Instead of separate web pages, the web browser on the computing device may be configured to open a secure communication session with the web module, and to communicate information to be displayed and user input information therebetween.

[00206] In the fifth embodiment described above, the user is prompted to enter an MDN into an input field of an online account registration web page, which information is used to identify an online account created for the user on the web module. In an alternative embodiment, the web module may instead be configured to create a pre-established online account for the user including a pre-established username, as well as additional information associated with the user that is available to the web module, such

as the user's MDN and trusted phrase received from the middleware server. In this alternative embodiment, the user can then use the web browser to log in to the pre-registered account using the pre-registered user name, for example as illustrated in the exemplary web page in Figure 29a. Figure 29b shows a subsequently transmitted and displayed exemplary web page confirming the user's online account details after a successful login. The web browser can then display a further web page as shown in Figure 29c to prompt for user input of a generated passcode, as described in the embodiment above. Figure 29d shows an exemplary web page that can be displayed to the user following input of a valid user input passcode and successful website login to the pre-registered online account.

[00207] In the fifth embodiment described above, the mobile payment system facilitates secure activation and integration of a mobile payment account sub-system and an online banking sub-system via a web browser in communication with a web module over the Internet. In alternative embodiments, the account management system may instead, or additionally, provide for communication with a user over other alternate channels (separate from the network through which payment transactions are conducted), so as to facilitate the secure activation of the online account associated with a mobile device configured for contactless payment operations. For example, the account management system may instead or additionally comprise a automated voice detection sub-system for communication by the user of the generated passcode via a telephone.

[00208] In the embodiments described above, the mobile device stores a plurality of application modules (also referred to as computer programs or software) in memory, which when executed, enable the mobile device to implement embodiments of the present invention as discussed herein. As those skilled in the art will appreciate, the software may be stored in a computer program product and loaded into the mobile device using any known instrument, such as removable storage disk or drive, hard disk drive, or communication interface, to provide some examples.

[00209] In embodiments described above, the account management system is described as a separate entity to the payment account issuer and the associated payment processing system. As those skilled in the art will appreciate, the account management

system may be provided as an integral part or sub-system of the payment account issuer and/or payment processing system.

[00210] In the embodiments described above, the passcodes are personal identification numbers (PINs). Alternatively or additionally, the wallet application could use any other form of passcode such as an alphanumeric passcode, a numeric passcode of varying length, gesture based actions, or facial recognition.

[00211] Alternative embodiments may be envisaged, which nevertheless fall within the scope of the following claims. In particular, it is appreciated that the various embodiments are not necessarily mutually exclusive and can be combined with one or more other embodiments to form new embodiments. For example, the above-described embodiments may be combined to form a mobile payment system having all of the described aspects thereof.

CLAIMS

1. A mobile payment account activation system for facilitating the automated activation of a mobile payment account stored on a portable electronic device, comprising an account activation unit for automatically authenticating a user associated with an inactive mobile payment account by transmitting validation data to the portable electronic device and for activating the mobile payment account after the user has been authenticated based on the transmitted validation data.

2. The system of claim 1, wherein activating the mobile payment account enables a payment transaction to be made from the mobile payment account.

3. The system of claim 1, wherein mobile payment account data associated with an inactive mobile payment account is stored on the portable electronic device.

4. The system of claim 3, wherein the mobile payment account data further includes data identifying the portable electronic device.

5. The system of claim 1, wherein the account activation unit is arranged to maintain a state of the provisioned mobile payment account indicative of whether the mobile payment account is active or inactive.

6. The system of claim 1, wherein the transmitted validation data comprises at least one validation question.

7. The system of claim 6, wherein the account activation unit is arranged to receive a validation answer to the at least one validation question from the portable electronic device and to automatically authenticate the user based on the received validation answer.

8. The system of claim 7, wherein the validation questions and answers are based on identification and validation (ID&V) information associated with the mobile payment account.

9. The system of claim 8, wherein the ID&V information is stored at one or more of the account activation unit and a payment account issuer.

10. The system of claim 8, wherein the validation questions and answers are further based on additional ID&V information provided by a third party.

11. The system of claim 8, wherein the ID&V information is not transmitted to the mobile electronic device.

12. The system of claim 6, wherein the account activation unit is arranged to configure the number of validation questions transmitted to the portable electronic device based on a determined level of security associated with the user.

13. The system of claim 1, wherein the validation data does not facilitate payment from the activated mobile payment account.

14. The system of claim 1, wherein the account activation unit is operable to automatically authenticate a user associated with an inactive mobile payment account substantially in real-time.

15. A mobile payment account activation system for facilitating the automated activation of a mobile payment account stored on a portable electronic device, comprising data for a plurality of mobile payment accounts associated with a user and an account activation unit operable to receive a user selection of an inactive one of said mobile payment accounts, automatically authenticate the user associated with the selected mobile payment account via the portable electronic device, and activate the selected mobile payment account after the user has been authenticated.

16. The system of claim 1, wherein the portable electronic device is a mobile handset.

17. The system of claim 16 wherein the account activation unit is arranged to communicate with the mobile handset via a cellular telephone network.

18. The system of claim 16, further comprises a communications server for handling secure communication between the account activation unit and the mobile handset.

19. The system of claim 1, further comprising an account creation unit arranged to receive a request from a user for a new mobile payment account and to create an inactive mobile payment account in response to said request.

20. A mobile device for use in a mobile payment system, the mobile device comprising:

a communication network interface;

a secure memory for storing data associated with at least one inactive mobile payment account data;

an account activation module operable to receive validation data from the account provisioning system to facilitate automatic authentication of the user and automatically activation of the mobile payment account.

21. The mobile device of claim 20, wherein activating the provisioned mobile payment account enables a payment transaction to be made from the mobile payment account.

22. The mobile device of claim 20, wherein the received validation data comprises at least one validation question.

23. The mobile device of claim 22, wherein the account activation module is further operable to transmit a validation answer to the at least one validation question and to facilitate automatic authentication of the user based on the received validation answer.

24. The mobile device of claim 20, wherein the payment account module comprises a software application executing on the mobile device.

25. The mobile device of claim 20, further comprising a contactless communication link interface for communicating with an electronic point of sale terminal to perform a financial transaction using an activated mobile payment account on the mobile device.

26. The mobile device of claim 25, further comprising a payment account module operable to process a financial transaction using an activated mobile payment account.

27. The mobile device of claim 20, wherein the payment account module is stored in the secure memory.

28. A computer-implemented method of activating a mobile payment account stored on a portable electronic device, comprising automatically authenticating a user associated an inactive mobile payment account by transmitting validation data to the portable electronic device, and automatically activating the provisioned mobile payment account after the user has been authenticated based on the transmitted validation data.

29. A method of facilitating secured payment from an electronic wallet on a portable device, comprising:

storing, on the portable device, an electronic wallet comprising data for authorizing a payment transaction, wherein said data includes a passcode for enabling access to the electronic wallet and a flag indicating whether input of the passcode is required to access the electronic wallet;

receiving, from a remote apparatus, a command to set the flag to indicate that input of the passcode is required to access the electronic wallet; and

responsive to a request to conduct a payment transaction from the electronic wallet, prompting for input of a passcode if the flag indicates that input of the passcode is required, verifying the input passcode, and providing payment information to authorize the payment transaction.

30. The method of claim 29, wherein the remote apparatus is a server associated with a payment account issuer.

31. The method of claim 29, wherein the flag is set based on a threshold of usage of the electronic wallet.

32. The method of claim 29, wherein the flag is set based on an unusual purchase pattern from the electronic wallet.

33. The method of claim 29, wherein the flag is set when an incorrect passcode is entered.

34. The method of claim 29, wherein the flag is set after a predefined number of payment transactions have been authorized without requiring input of the passcode.

35. The method of claim 29, wherein the flag is reset upon verification of an input passcode.

36. The method of claim 29, wherein the flag is reset in response to a remote command.

37. The method of claim 29, wherein the electronic wallet data is stored in a secure element of the mobile device.

38. The method of claim 29, wherein the received command is encrypted.

39. A method of facilitating payment from an electronic wallet on a portable device, comprising:

storing, on the portable device, wallet application software for accessing the electronic wallet, including executable code for facilitating access to data defining one or more mobile payment accounts in the electronic wallet and executable code for facilitating activation of a secure payment from a mobile payment account;

storing, on the portable device, further payment application software associated with the executable code in the wallet application software for facilitating activation; and

receiving a user input selection of the second application software and in response, directly executing the associated executable code in the first application software to facilitate activation of a secure payment from the mobile payment account.

40. The method of claim 39, wherein payment is secured by validating a user input passcode before payment from the electronic wallet is activated.

41. The method of claim 40, wherein validating the user input passcode comprises comparing the input passcode with a stored passcode for the electronic wallet.

42. The method of claim 39, wherein the further payment application software comprises executable code defining a shortcut link to the executable code of the wallet application software for facilitating activation of a secure payment from a mobile payment account.

43. The method of claim 39, wherein the payment application software is further associated with executable code for conducting a payment transaction after activation.

44. The method of claim 43, wherein the electronic wallet stores a plurality of mobile payment accounts, and wherein the executable code for conducting a payment transaction after activation comprises prompting for a user selected one of the mobile payment accounts.

45. The method of claim 44, wherein the selected mobile payment account is predefined as a default selected mobile payment account.

46. The method of claim 45, wherein the plurality of mobile payment accounts enable the user to conduct a payment transaction with an associated debit account, credit account, linked checking or decoupled debit account and/or pre-paid account.

47. The method of claim 11, wherein the wallet application software further includes executable code for facilitating creation of a mobile payment account in the electronic wallet, the mobile payment account associated with a payment account issuer.

48. A portable device comprising means for performing the method of any one of claims 29 to 47.

49. A method of conducting a contactless secured payment from an electronic wallet on a mobile device, comprising:

storing, on the mobile device, an electronic wallet comprising data for authorizing a payment transaction, wherein the data includes a passcode for enabling access to the electronic wallet;

generating, by the mobile device, a transaction request message including a value identifying one of a plurality of passcode entry related states; and

transmitting, by the mobile device, the generated transaction request message to a remote apparatus.

50. The method of claim 49, wherein the plurality of passcode entry related states include:

1) a first state indicative that a passcode was received and verified by the mobile device;

2) a second state indicative that a passcode was received and identified by the mobile device as an incorrect passcode; and

3) a third state indicative that a passcode was not received by the mobile device.

51. The method of claim 49, further comprising determining, by the remote apparatus, that the transaction request message is declined based at least on the value received identifying a passcode entry related state.

52. The method of claim 51, wherein responsive to determining that the transaction request message is declined for a passcode related reason, the remote apparatus transmits a transaction decline response to the mobile device identifying the passcode related reason for decline.

53. The method of claim 52, wherein the transaction decline response comprises a value representing that a passcode was not entered at all or that an incorrect passcode was entered.

54. The method of claim 53, further comprising displaying, by the mobile device, a transaction declined response including the received passcode related reason for decline.

55. The method of claim 51, wherein the remote apparatus determines that the transaction request message is declined based additionally on a threshold of usage of the electronic wallet.

56. The method of claim 51, wherein the remote apparatus determines that the transaction request message is declined based additionally on an unusual purchase pattern from the electronic wallet.

57. The method of claim 49, wherein the remote apparatus is a server associated with a payment account issuer.

58. The method of claim 49, wherein the data of the electronic wallet is stored in a secure element of the mobile device.

59. The method of claim 49, wherein the passcode comprises numeric, alphabetic, alphanumeric or non-alphanumeric symbols.

60. A mobile device for conducting contactless payment from an electronic wallet on the mobile device, comprising means for performing the method of any one of claims 49 to 59.

61. A method of facilitating mobile payment account management from a first electronic wallet on a first portable device, comprising:

storing, on the first portable device, the first electronic wallet comprising data for authorizing a payment transaction from a primary payment account;

receiving, by the first portable device, user input of an additional authorized user authorized to use the primary payment account;

generating an activation code for the additional authorized user;

storing, on a second portable device, a second electronic wallet comprising data for authorizing a payment transaction from the primary payment account; and

enabling payment transactions from the primary payment account to be authorized from the second portable device after receiving user input of the activation code at the second portable device.

62. The method of claim 61, wherein user input of the additional authorized user comprises input of data identifying the additional authorized user.

63. The method of claim 61, wherein user input of the additional authorized user comprises selection of a contact person from contact data stored on the first portable device, wherein the contact data includes data identifying the additional authorized user.

64. The method of claim 63, wherein the data identifying the additional authorized user comprises a mobile directory number.

65. The method of claim 64, further comprising transmitting, by the first portable device, a request to add an authorized user of the primary payment account to a middleware server associated with a payment account issuer, wherein the request comprises data identifying the primary payment account and the mobile directory number for the additional authorized user.

66. The method of claim 65, wherein generating the activation code is performed by the middleware server in communication with the first portable device.

67. The method of claim 66, wherein the authorized user is authenticated by the middleware server based on the activation code input to the second portable device.

68. The method of claim 66, wherein the middleware server communicates the activation code with the data for authorizing a payment transaction from the primary payment account that is stored on the second portable device, and wherein the authorized user is authenticated by the second portable device based on user input of the activation code.

69. The method of claim 66, wherein the middleware server stores data indicating a state of the first electronic wallet stored on the first portable device and the second electronic wallet stored on the second portable device.

70. The method of claim 69, wherein the state comprises an inactive state where the first electronic wallet or the second electronic wallet cannot be used to authorize a payment transaction from the primary payment account and an active state where the first electronic wallet or the second electronic wallet can be used to authorize a payment transaction from the primary payment account.

71. The method of claim 61, further comprising receiving user input sensitive information after receiving user input of the activation code at the second portable device.

72. The method of claim 61, wherein the first electronic wallet and the second electronic wallet are stored in respective secure memory elements of the first portable device and the second portable device.

73. The method of claim 61, wherein the first portable device and the second portable device are mobile handsets.

74. The method of claim 61, wherein the first portable device and the second portable device are adapted for contactless payment transactions.

75. A system for facilitating mobile payment account management from a first electronic wallet on a first portable device, comprising means for performing the method of any one of claims 61 to 74.

76. A computer-implemented method of tracking a process of provisioning, by a middleware server to a portable device in a mobile payment system, payment account data for authorizing a payment transaction, the method comprising:

transmitting, by the portable device to the middleware server, a user request for a payment account product;

initiating, by the middleware server responsive to the user request, a provisioning process for the payment account product requested by the user request, including storing status data indicative of an initiated state of the provisioning process;

transmitting, by the middleware server to the portable device, a digital document including information that must be viewed by a user and updating the status data indicative of a transmitted state of the digital document;

receiving, by the middleware server from the portable device, an indication that the digital document has been viewed by the user, and in response updating the status data indicative of a viewed state of the digital document; and

provisioning, by the middleware server to the portable device, payment account data for the payment account product as requested.

77. The method of claim 76, wherein the portable device is arranged to display a user selectable plurality of payment account products that the user is eligible to request.

78. The method of claim 77, wherein the plurality of payment account products is determined based on user details or search criteria.

79. The method of claim 76, wherein the digital document includes pre-application terms and conditions that the user must view and acknowledge before the middleware server provisions the payment account data for the requested payment account product.

80. The method of claim 79, further comprising transmitting, by the middleware server to the portable device, a second digital document including post-application agreement information specific to the payment account product that must be viewed by the user, and updating the status data indicative of a transmitted state of the second digital document.

81. The method of claim 80, further comprising transmitting, by the portable device, an indication to the middleware server that the user has viewed the second digital document, and updating, by the middleware server responsive to receipt of the indication, the status data indicative of a viewed state of the second digital document.

82. The method of claim 81, wherein the payment account data provisioned by the middleware server to the portable device comprises an inactive mobile payment account, the method further comprising an activation process for activating the payment account product after the user has viewed the second digital document.

83. The method of claim 76, wherein the digital document comprises data associated with one or more portions of the digital document for triggering transmission of an indication that a particular portion of the digital document has been viewed.

84. The method of claim 76, further comprising tracking a time of viewing one or more portions of the digital document.

85. The method of claim 76, further comprising tracking a location of viewing one or more portions of the digital document.

86. The method of claim 76, wherein the digital document is formatted for the portable device.

87. The method of claim 76, wherein the portable device is a mobile handset.

88. The method of claim 76, wherein the portable device is for contactless payment transactions.

89. A computer-implemented method of provisioning, by a middleware server to a portable device in a mobile payment system, payment account data for authorizing a payment transaction and at least one digital document associated with the payment account data that is to be displayed by the portable device, wherein the middleware server automatically monitors the progress of the method of provisioning.

90. A mobile payment account system comprising means for performing the method of any one of claims 76 to 89.

91. A mobile payment account system comprising:

a mobile device configured for contactless payment operations from a mobile payment account and including:

a secure element storing a wallet application module, data defining a first encryption key, and user verification data associated with the mobile payment account;

a user verifier adapted to verifying a user based on said user verification data; and

a first passcode generator adapted to generate a first passcode based at least on the first encryption key; and

an online account server including:

a memory storing online account data defining a user account associated the mobile device, the online account data comprising data defining a second encryption key;

a communication interface adapted to receive user input data identifying the passcode generated by the mobile device;

a second passcode generator adapted to generate a second passcode based at least on the second encryption key; and

a user validator adapted to compare the first passcode to the second passcode in a registration process to register the user account.

92. The system of claim 91, wherein the passcode generator of the mobile device displays the generated first passcode for a predetermined amount of time.

93. The system of claim 91, wherein the mobile device is a mobile handset.

94. The system of claim 3, wherein the user account is identified by a Mobile Directory Number (MDN) associated with the mobile device.

95. The system of claim 91, wherein the user verification data associated with the mobile payment account comprises a Personal Identification Number (PIN).

96. The system of claim 91, wherein the user verification data associated with the mobile payment account comprises biometric data.

97. The system of claim 91, wherein the first encryption key is the same as the second encryption key.

98. The system of claim 91, wherein the first and second passcode generators generate the respective first and second passcodes based on additional information associated with a time-based element.

99. The system of claim 91, wherein the first and second passcode generators generate the respective first and second passcodes based on additional information associated with a hardware identifier of the mobile device.

100. The system of claim 91, wherein the first and second passcodes are numeric, alphabetic symbols, non-alphanumeric symbols, or a combination thereof.

101. The system of claim 91, wherein the user validator verifies the user account associated with the mobile device when the generated passcode matches the recreated passcode.

102. The system of claim 91, wherein the wallet application module, data defining an encryption key, and the data associated with the mobile payment account are transmitted to the secure element of the mobile device by a secure communication channel.

103. The system of claim 91, wherein the secure element is an embedded secure memory chip or a Universal Integrated Circuit Card (UICC) secure element.

104. The system of claim 91, wherein the secure element is a peripheral memory device or a micro Secure Digital card.

105. The system of claim 91, further comprising a computing device including a web browser for communication with the online account server.

106. The system of claim 105, wherein the web browser receives a web page including an input field for receiving a user input passcode.

107. The system of claim 106, wherein the web page enables user input of the passcode within a predetermined time window.

108. The system of claim 107, wherein the mobile device is the computing device.

109. An online account server in the mobile payment account system of claim 91, comprising:

a memory storing online account data defining a user account associated the mobile device, the online account data comprising data defining a second encryption key;

a communication interface adapted to receive user input data identifying the passcode generated by the mobile device;

a second passcode generator adapted to generate a passcode based at least on the second encryption key; and

a user validator adapted to compare the received generated passcode to the passcode generated by the second passcode generator, in a registration process to register the user account.

110. A computer-implemented method of registering an online account associated with a mobile device configured for contactless payment operations in a mobile payment account system, the method comprising:

storing online account data defining a user account associated a mobile device;

receiving user input data identifying a first passcode generated by the mobile device based at least on an encryption key stored securely in the mobile device;

generating a second passcode based at least on an encryption key stored in an online account server;

comparing the first passcode to the second passcode to determine a match; and registering the online account when a match is determined.

111. A computer implemented method of registering an online account associated with a mobile device configured for contactless payment operations in a mobile payment account system, the method comprising:

initiating a registration process to register an online account associated with a mobile device;

receiving user input data identifying a first passcode generated by the mobile device; and

transmitting the first passcode to an online account server for registering the online account when the online account server determines that the first passcode matches a second passcode generated by the online account server based at least on an encryption key stored in the online account server.

112. A mobile device configured as an electronic wallet for transaction operations from a plurality of mobile transaction accounts, comprising:

a plurality of transaction modules operable to process mobile transaction operations with a respective transaction account, each transaction module configured to allow a transaction operation to be completed after an authentication process; and

an authentication module coupled to the plurality of transaction modules, operable to verify a user input passcode and to respond to authentication requests from the plurality of transaction modules after the user input passcode is verified.

113. The mobile device of claim 112, wherein each of the plurality of transaction modules performs an authentication process comprising transmitting to the authentication module a request for confirmation that the plurality of transaction modules can allow the transaction operations to be completed.

114. The mobile device of claim 112, wherein each of the plurality of transaction modules further comprises a passcode verifier operable to verify a transaction passcode associated with as associated transaction module, and wherein each of the plurality of transaction modules is operable to perform an authentication process comprising

transmitting to the authentication module a request for a transaction passcode associated with the associated transaction module.

115. The mobile device of claim 114, wherein the authentication module communicates a requested transaction passcode to the associated transaction module after the user input passcode is verified.

116. The mobile device of claim 114, wherein the authentication module broadcasts a transaction passcode to the associated transaction module after the user input passcode is verified.

117. The mobile device of claim 114, wherein the authentication module stores a plurality of transaction passcodes associated with the plurality of transaction modules.

118. The mobile device of claim 117, wherein the authentication module maps the user input passcode to a stored transaction passcode.

119. The mobile device of claim 117, wherein the plurality of transaction passcodes associated with the plurality of transaction modules are the same as the user input passcode.

120. The mobile device of claim 112, further comprising a secure element storing the plurality of transaction modules and the authentication module.

121. The mobile device of claim 120, wherein the secure element is an embedded secure memory chip or a Universal Integrated Circuit Card secure element.

122. The mobile device of claim 120, wherein the secure element is a peripheral memory device or a micro Secure Digital card.

123. The mobile device of claim 112, wherein the plurality of mobile transaction modules are associated with one or more payment account issuers, and wherein the plurality of transaction modules and the authentication module are associated with the same payment account issuer.

124. The mobile device of claim 123, further comprising a security domain associated with the payment account issuer, and wherein the authentication module is provided in the same security domain as the plurality of transaction modules.

125. The mobile device of claim 124, further comprising at least one other security domain associated with a different payment account issuer, and at least one other transaction applet associated with a different payment account issuer and provided in said at least one other security domain.

126. The mobile device of claim 123, wherein each of the plurality of transaction modules comprises computer-implementable instructions for processing transaction operations with the payment account issuer using a communication protocol.

127. The mobile device of claim 112, wherein at least one of the plurality of transaction modules is configured to process a contactless transaction operation with the payment account issuer using a contactless communication protocol.

128. The mobile device of claim 112, wherein the transaction operations comprise a payment transaction, a ticketing transaction and a coupon transaction.

129. The mobile device of claim 112, wherein the passcode comprises numeric, alphabetic, alphanumeric or non-alphanumeric symbols.

130. The mobile device of claim 112, wherein the authentication module further comprises a counter operable to maintain a count of user input attempts for passcode

verification, wherein the authentication module is operable to communicate failure of the passcode verification when the count exceeds a predefined number of attempts.

131. The mobile device of claim 112, further comprising a non-issuer application module operable to process non-issuer related operations associated with the electronic wallet, wherein the non-issuer application module is configured to allow an operation to be completed after an authentication process using the authentication module.

132. A system comprising an account management system coupled to at least one payment account issuer, the account management system comprising:

a database storing data associated with a plurality of mobile transaction accounts; and

a middleware server storing computer-implementable instructions to configure a mobile device for transaction operations from the mobile transaction accounts, the middleware server comprising:

computer-implementable instructions to provide a plurality of transaction modules for processing transaction operations from a respective mobile transaction account, each of the plurality of transaction modules having a respective authentication mechanism to allow a transaction operation to be completed; and

computer-implementable instructions to provide an authentication module coupled to the plurality of transaction modules, operable to verify a user input passcode and to respond to authentication requests from the plurality of transaction modules after the user input passcode is verified.

133. In a mobile device, a method of processing transaction operations from a plurality of mobile transaction accounts in an electronic wallet, comprising:

using a plurality of transaction modules to process transaction operations with a respective mobile transaction account, each of the plurality of transaction modules configured to allow a transaction operation to be completed after an authentication process; and

using an authentication module coupled to the plurality of transaction modules to verify a user input passcode and to respond to authentication requests from the plurality of transaction modules after the user input passcode is verified.

134. A computer program comprising program code arranged to perform the method of any one of claims 28 to 47, 49 to 74, 76 to 90, 110 and 111.

135. A computer program product comprising the computer program of claim 134.

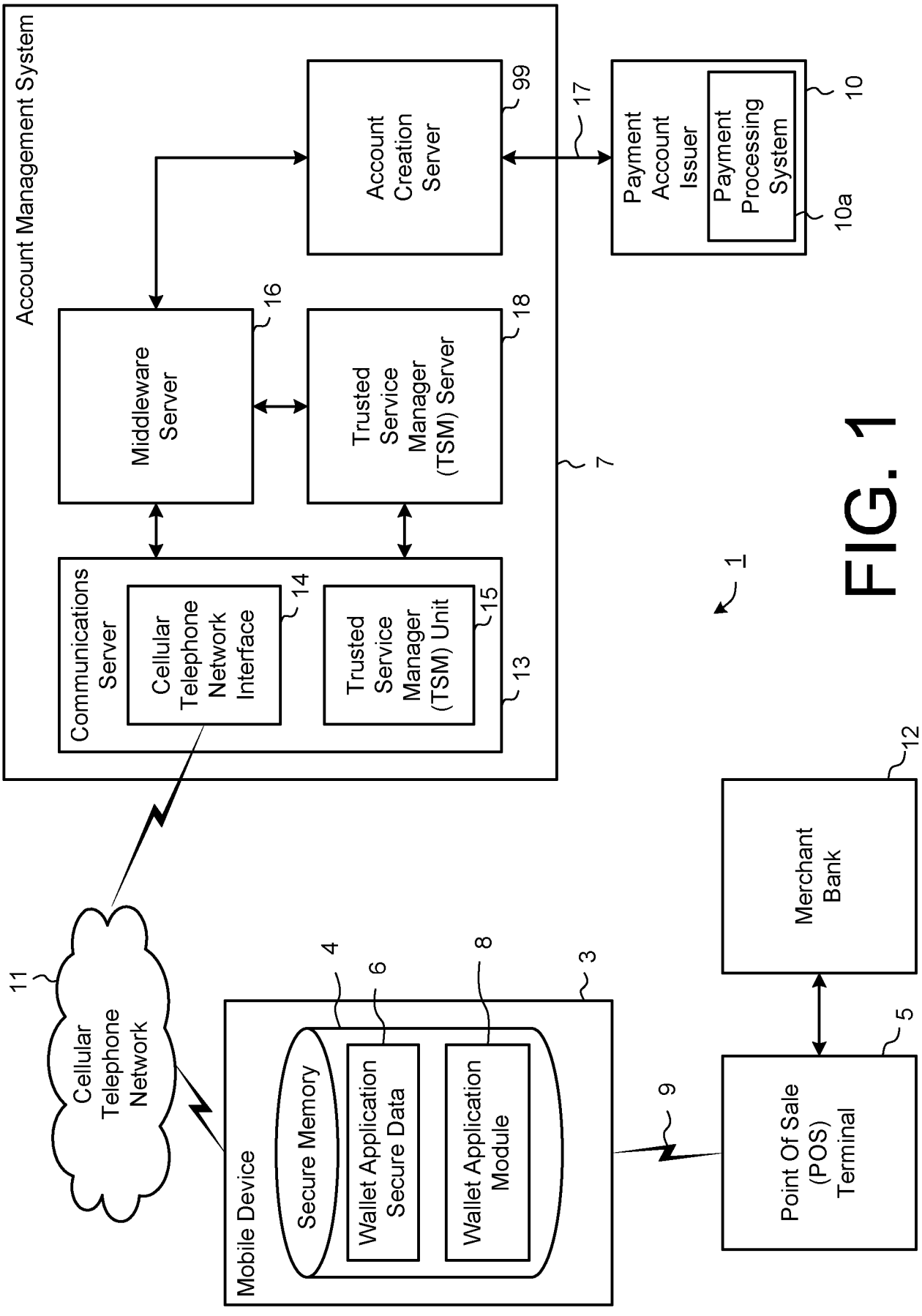

Account Management System
Account Creation Server
99
17
Payment Account Issuer
Payment Processing System
10
10a
Middleware Server
16
Trusted Service Manager (TSM) Server
18
7
Communications Server
Cellular Telephone Network Interface
14
Trusted Service Manager (TSM) Unit
15
13
1
Merchant Bank
12
11
Cellular Telephone Network
4
6
8
3
Mobile Device
Secure Memory
Wallet Application Secure Data
Wallet Application Module
9
Point Of Sale (POS) Terminal
5

FIG. 1

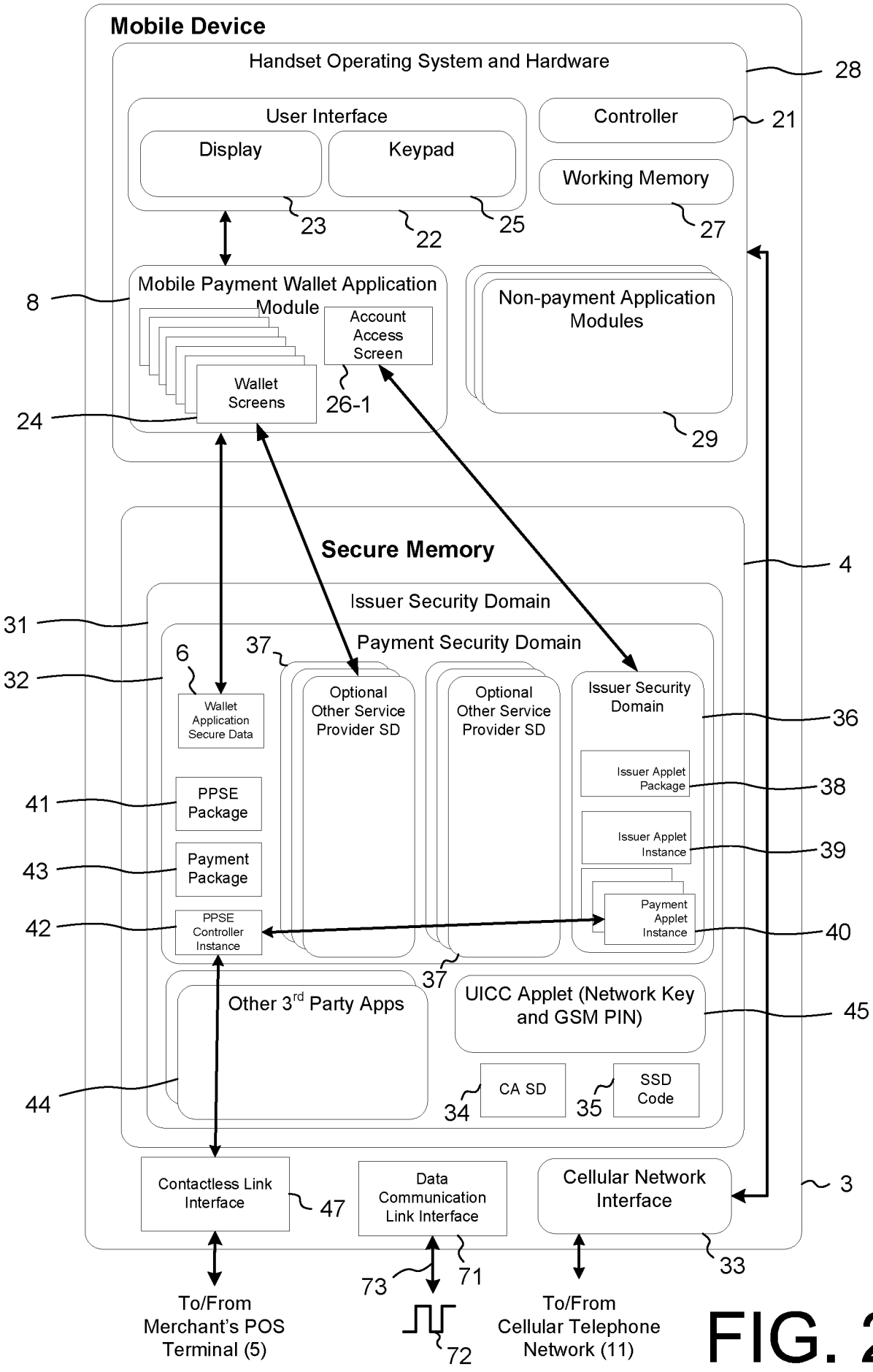

Mobile Device
Handset Operating System and Hardware
28
User Interface
Display
Keypad
23
22
25
Controller
21
Working Memory
27
8
Mobile Payment Wallet Application Module
Account Access Screen
Wallet Screens
26-1
24
Non-payment Application Modules
29
Secure Memory
4
Issuer Security Domain
31
Payment Security Domain
37
6
32
Wallet Application Secure Data
Optional Other Service Provider SD
Optional Other Service Provider SD
Issuer Security Domain
36
Issuer Applet Package
38
41
PPSE Package
Issuer Applet Instance
39
43
Payment Package
Payment Applet Instance
42
PPSE Controller Instance
40
37
Other 3rd Party Apps
UICC Applet (Network Key and GSM PIN)
45
44
CA SD
34
SSD Code
35
Contactless Link Interface
47
Data Communication Link Interface
Cellular Network Interface
3
33
73
71
72
To/From Merchant's POS Terminal (5)
To/From Cellular Telephone Network (11)

FIG. 2

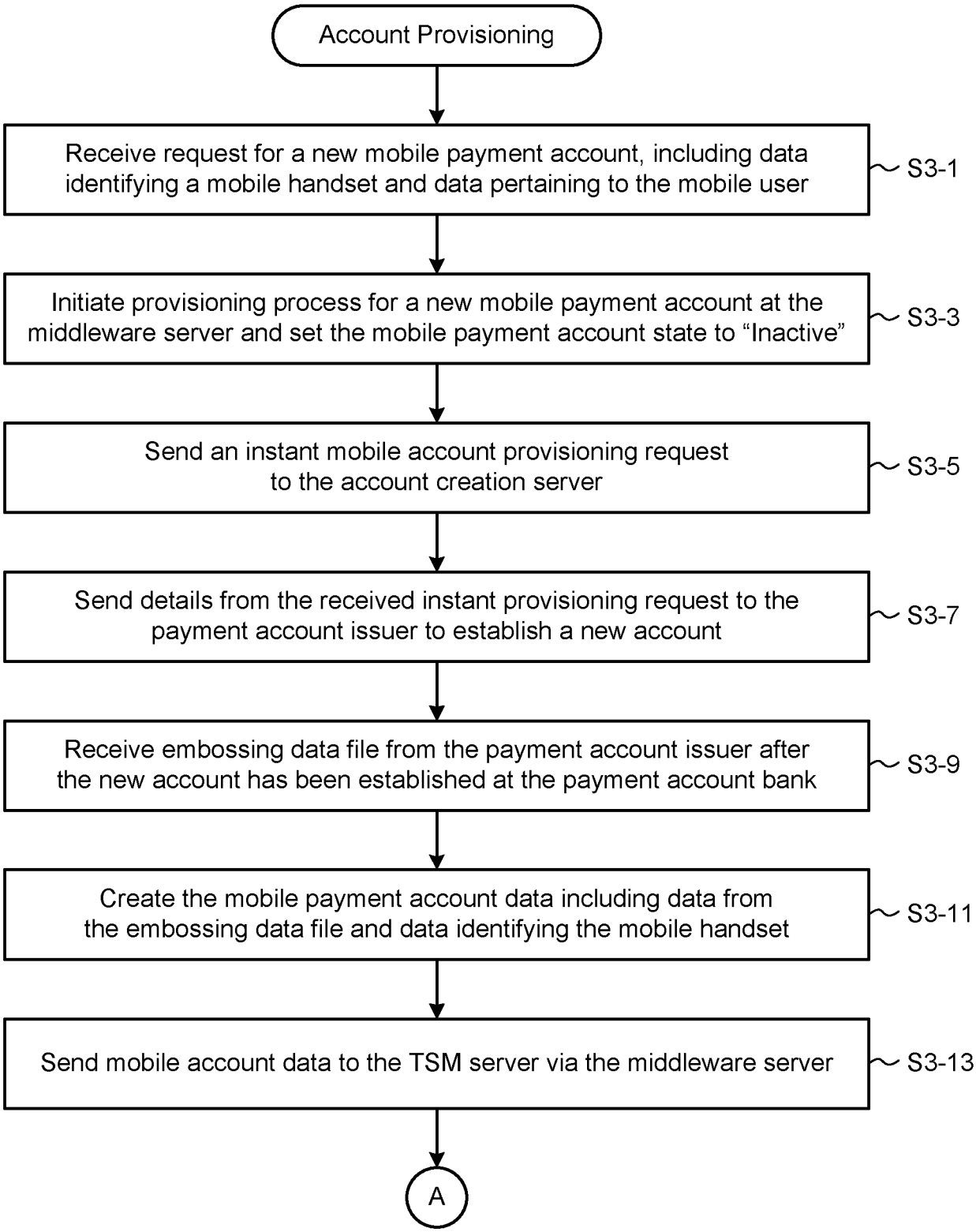

Account Provisioning
Receive request for a new mobile payment account, including data identifying a mobile handset and data pertaining to the mobile user
S3-1
Initiate provisioning process for a new mobile payment account at the middleware server and set the mobile payment account state to “Inactive”
S3-3
Send an instant mobile account provisioning request to the account creation server
S3-5
Send details from the received instant provisioning request to the payment account issuer to establish a new account
S3-7
Receive embossing data file from the payment account issuer after the new account has been established at the payment account bank
S3-9
Create the mobile payment account data including data from the embossing data file and data identifying the mobile handset
S3-11
Send mobile account data to the TSM server via the middleware server
S3-13
A

FIG. 3a

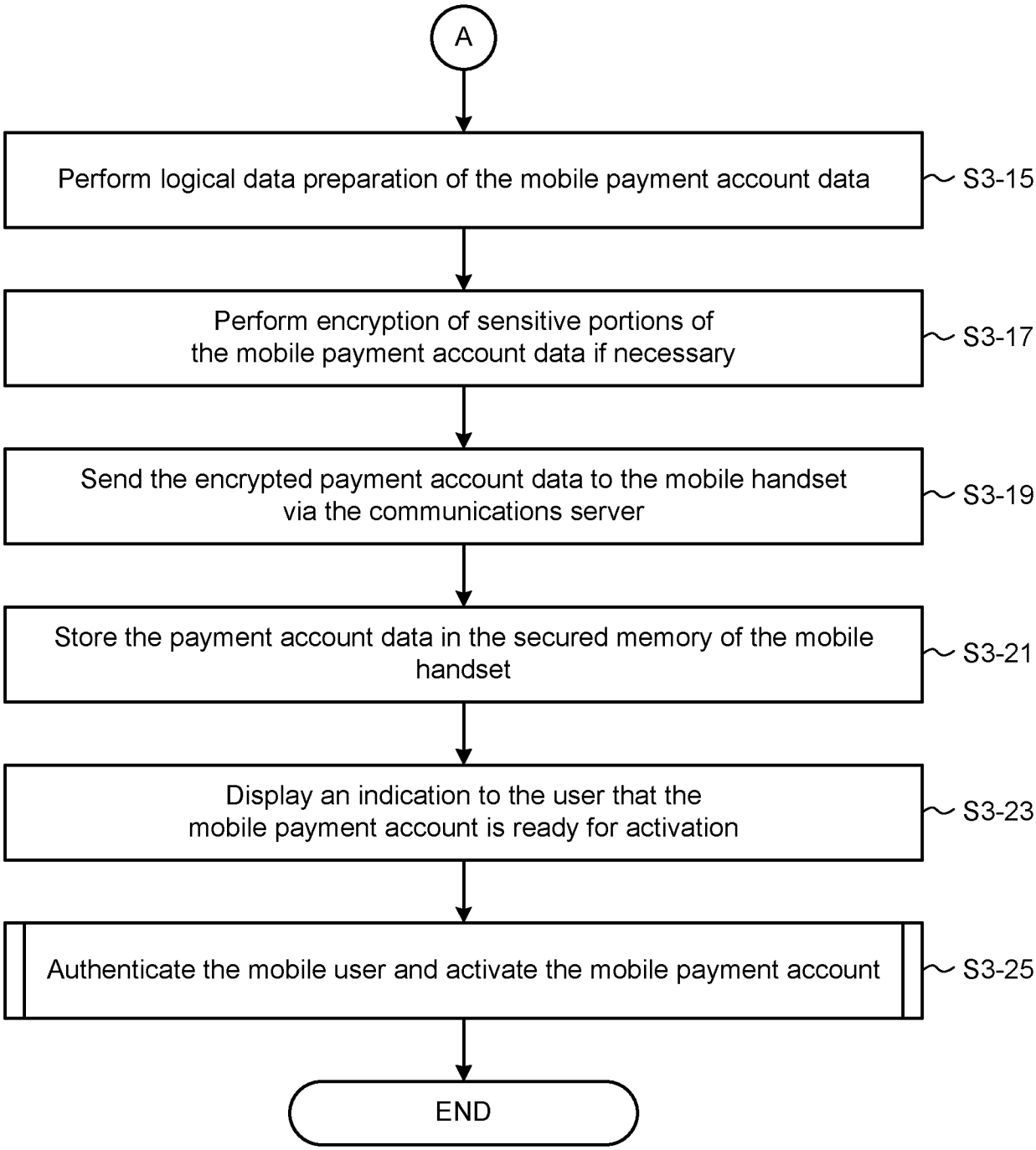

A
Perform logical data preparation of the mobile payment account data
S3-15
Perform encryption of sensitive portions of the mobile payment account data if necessary
S3-17
Send the encrypted payment account data to the mobile handset via the communications server
S3-19
Store the payment account data in the secured memory of the mobile handset
S3-21
Display an indication to the user that the mobile payment account is ready for activation
S3-23
Authenticate the mobile user and activate the mobile payment account
S3-25
END

FIG. 3b

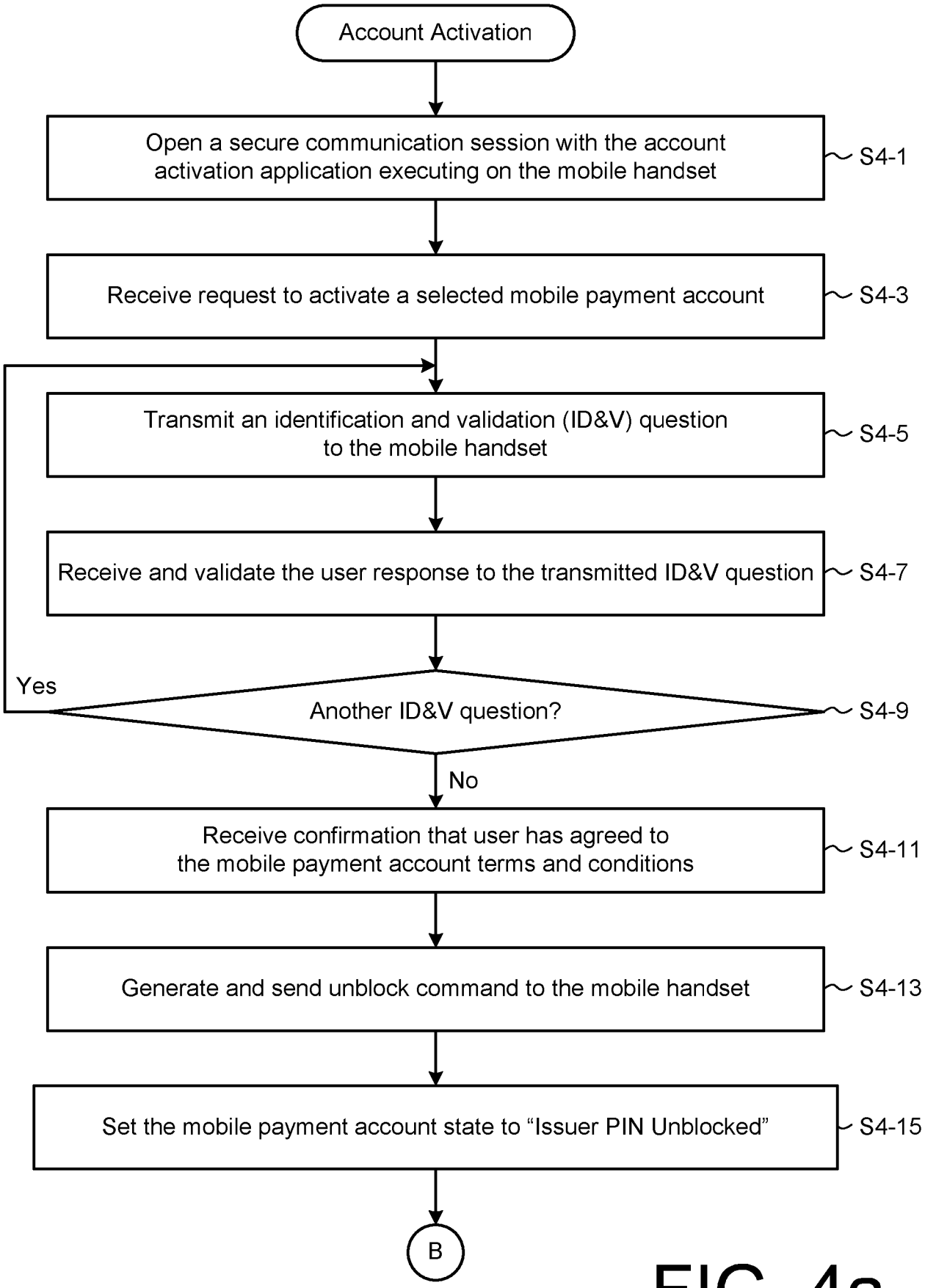

Account Activation
Open a secure communication session with the account activation application executing on the mobile handset
S4-1
Receive request to activate a selected mobile payment account
S4-3
Transmit an identification and validation (ID&V) question to the mobile handset
S4-5
Receive and validate the user response to the transmitted ID&V question
S4-7
Another ID&V question?
S4-9
Yes
No
Receive confirmation that user has agreed to the mobile payment account terms and conditions
S4-11
Generate and send unblock command to the mobile handset
S4-13
Set the mobile payment account state to "Issuer PIN Unblocked"
S4-15
B

FIG. 4a

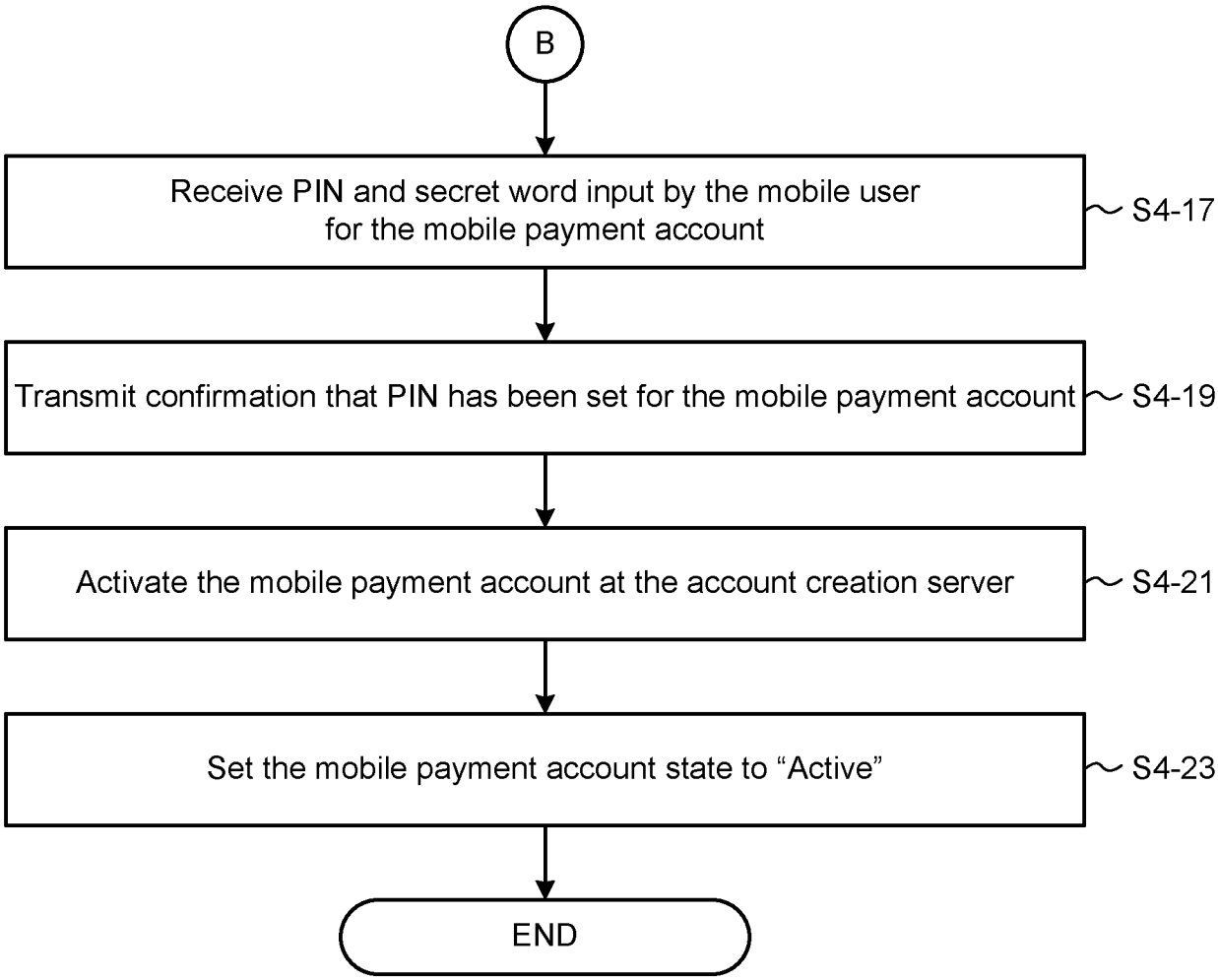

B
Receive PIN and secret word input by the mobile user for the mobile payment account
S4-17
Transmit confirmation that PIN has been set for the mobile payment account
S4-19
Activate the mobile payment account at the account creation server
S4-21
Set the mobile payment account state to “Active”
S4-23
END

FIG. 4b

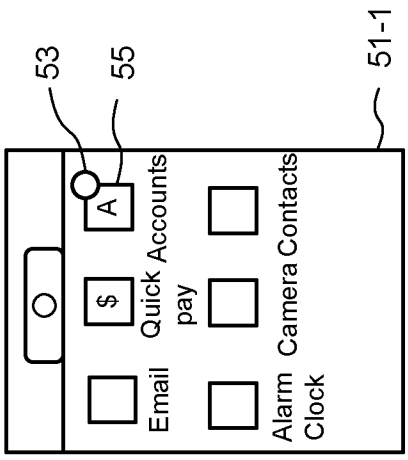


FIG. 5a

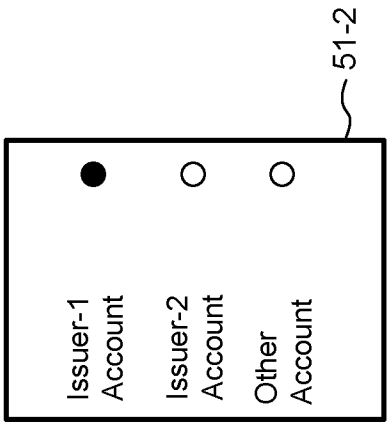


FIG. 5b

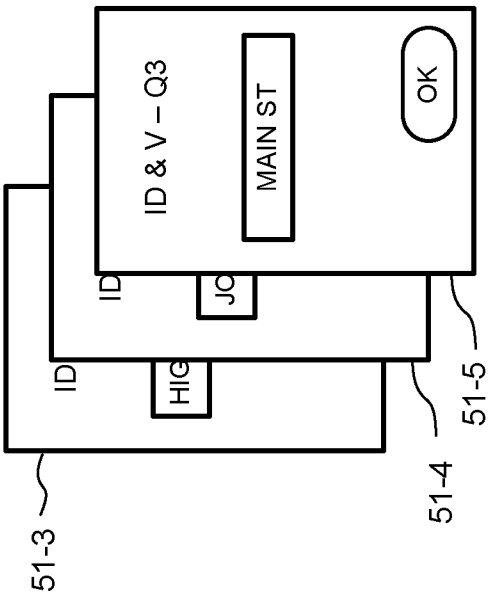


FIG. 5c

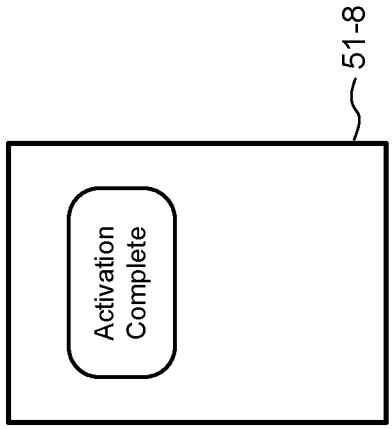


FIG. 5f

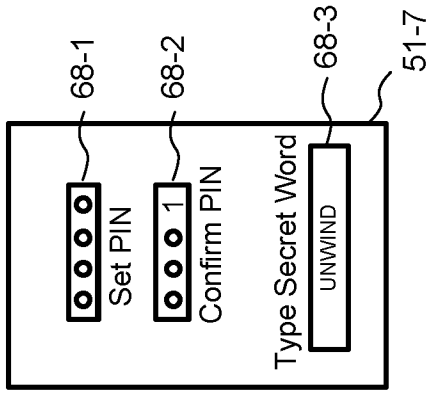


FIG. 5e

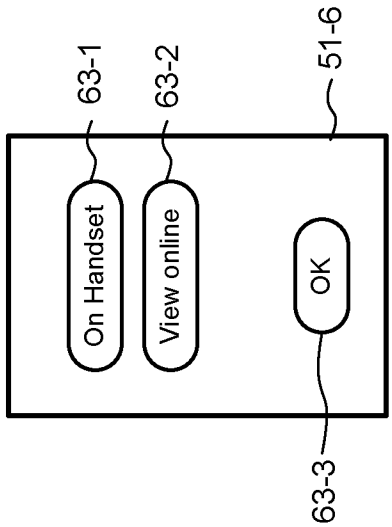


FIG. 5d

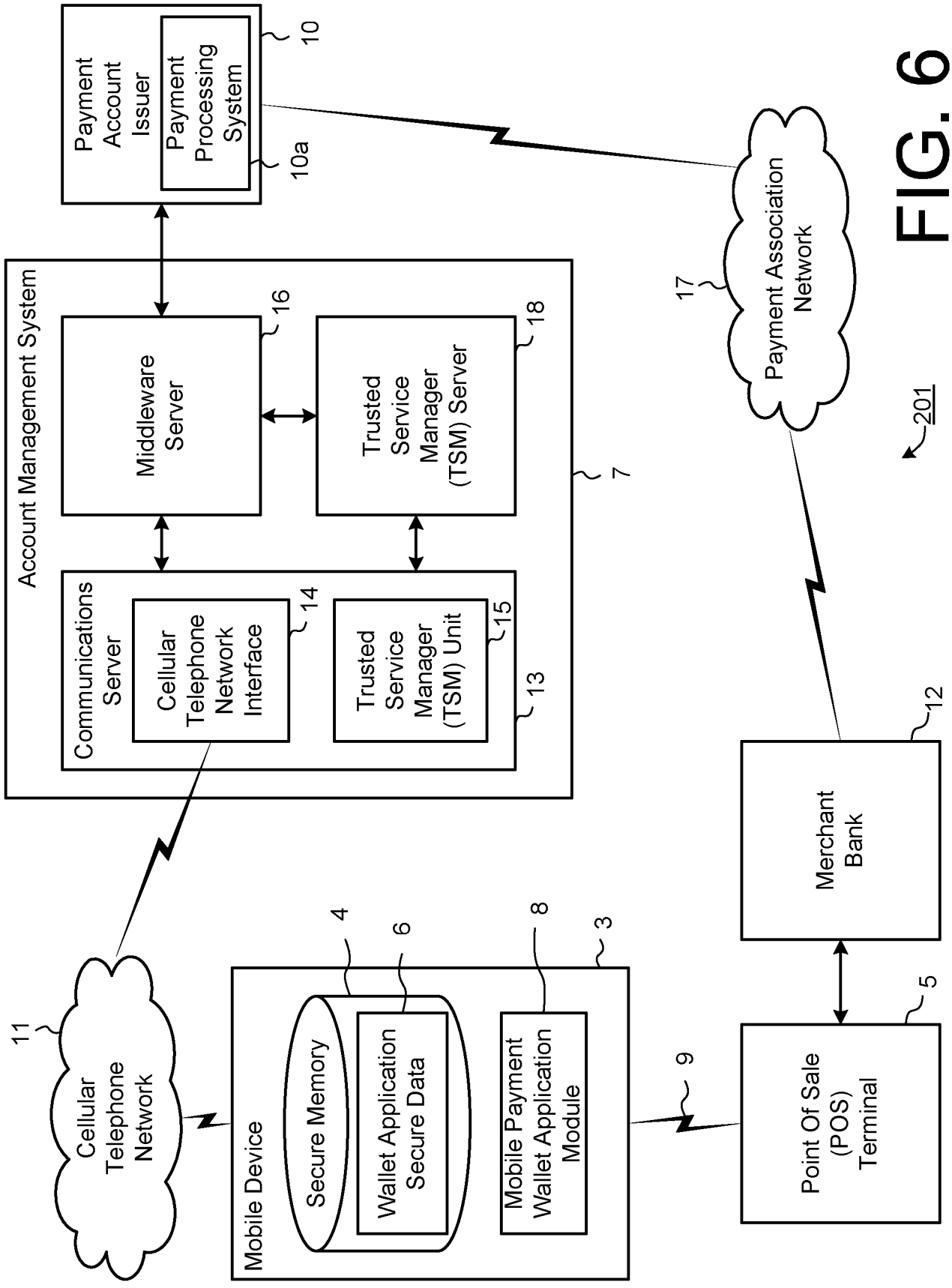

Payment Account Issuer
Payment Processing System
10
10a
Payment Association Network
17
201
Account Management System
Middleware Server
16
Trusted Service Manager (TSM) Server
18
7
Communications Server
Cellular Telephone Network Interface
14
Trusted Service Manager (TSM) Unit
15
13
Merchant Bank
12
Cellular Telephone Network
11
Mobile Device
Secure Memory
4
Wallet Application Secure Data
6
Mobile Payment Wallet Application Module
8
3
9
Point Of Sale (POS) Terminal
5

FIG. 6

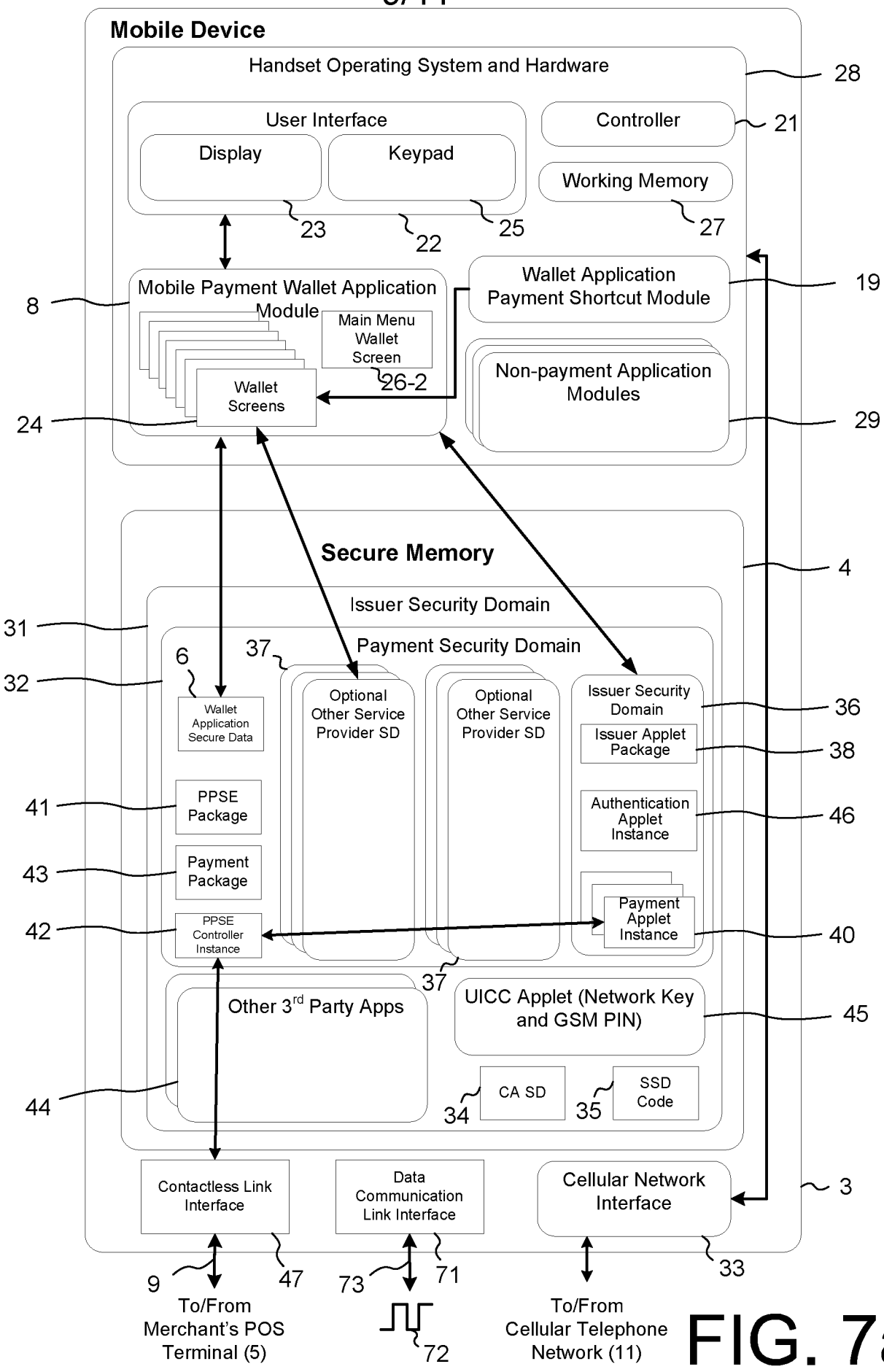

Mobile Device
Handset Operating System and Hardware
28
User Interface
Display
Keypad
23
22
25
Controller
21
Working Memory
27
Mobile Payment Wallet Application Module
8
Main Menu Wallet Screen
26-2
Wallet Screens
24
Wallet Application Payment Shortcut Module
19
Non-payment Application Modules
29
Secure Memory
4
Issuer Security Domain
31
Payment Security Domain
37
6
32
Wallet Application Secure Data
Optional Other Service Provider SD
Optional Other Service Provider SD
Issuer Security Domain
36
Issuer Applet Package
38
41
PPSE Package
Authentication Applet Instance
46
43
Payment Package
Payment Applet Instance
42
PPSE Controller Instance
40
37
Other 3rd Party Apps
UICC Applet (Network Key and GSM PIN)
45
44
CA SD
34
SSD Code
35
Contactless Link Interface
Data Communication Link Interface
Cellular Network Interface
3
9
47
73
71
33
To/From Merchant's POS Terminal (5)
72
To/From Cellular Telephone Network (11)

FIG. 7a

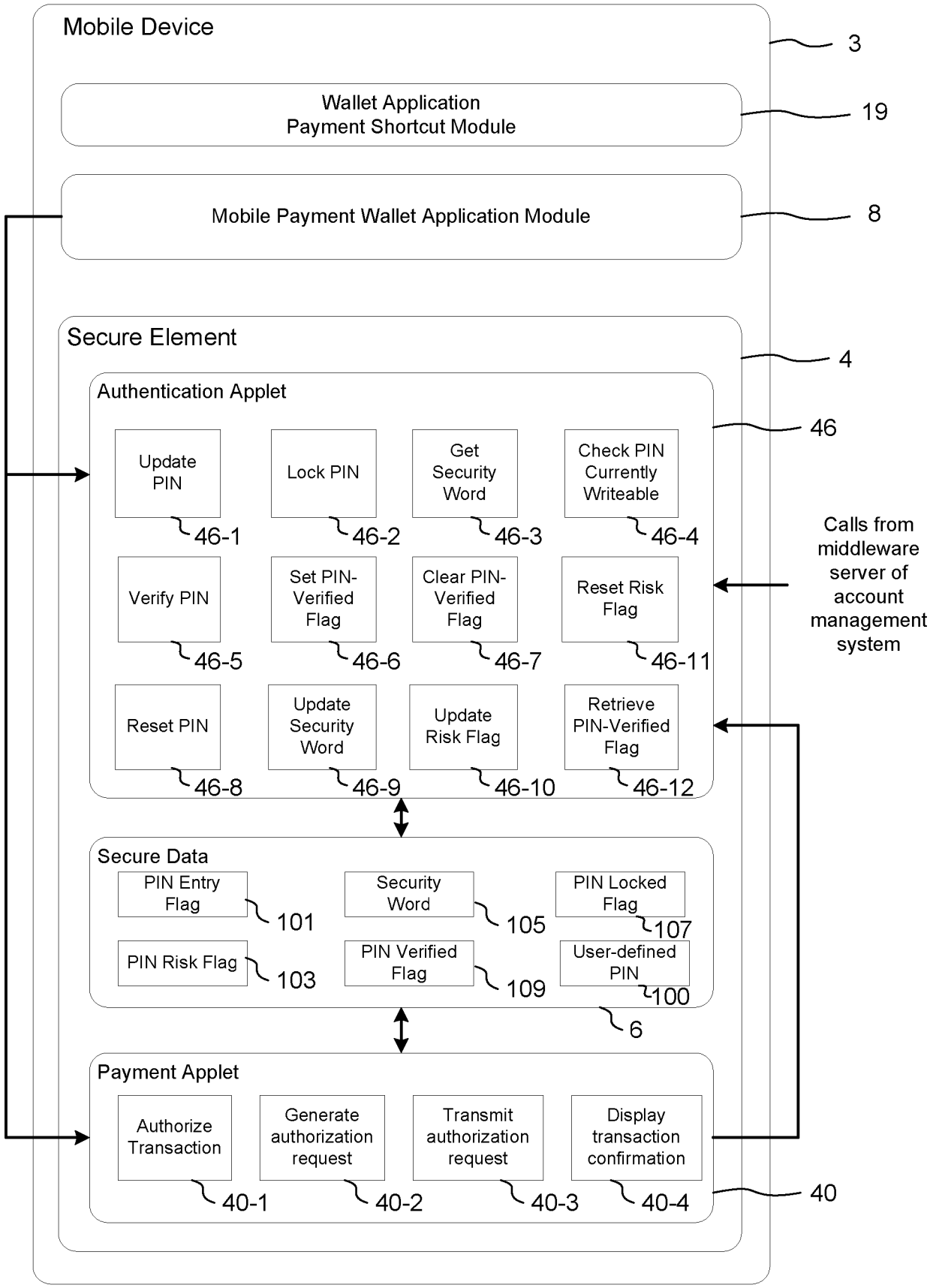

Mobile Device
3
Wallet Application
Payment Shortcut Module
19
Mobile Payment Wallet Application Module
8
Secure Element
4
Authentication Applet
46
Update PIN
46-1
Lock PIN
46-2
Get Security Word
46-3
Check PIN Currently Writeable
46-4
Verify PIN
46-5
Set PIN-Verified Flag
46-6
Clear PIN-Verified Flag
46-7
Reset Risk Flag
46-11
Reset PIN
46-8
Update Security Word
46-9
Update Risk Flag
46-10
Retrieve PIN-Verified Flag
46-12
Calls from middleware server of account management system
Secure Data
PIN Entry Flag
101
Security Word
105
PIN Locked Flag
107
PIN Risk Flag
103
PIN Verified Flag
109
User-defined PIN
100
6
Payment Applet
Authorize Transaction
40-1
Generate authorization request
40-2
Transmit authorization request
40-3
Display transaction confirmation
40-4
40

FIG. 7b

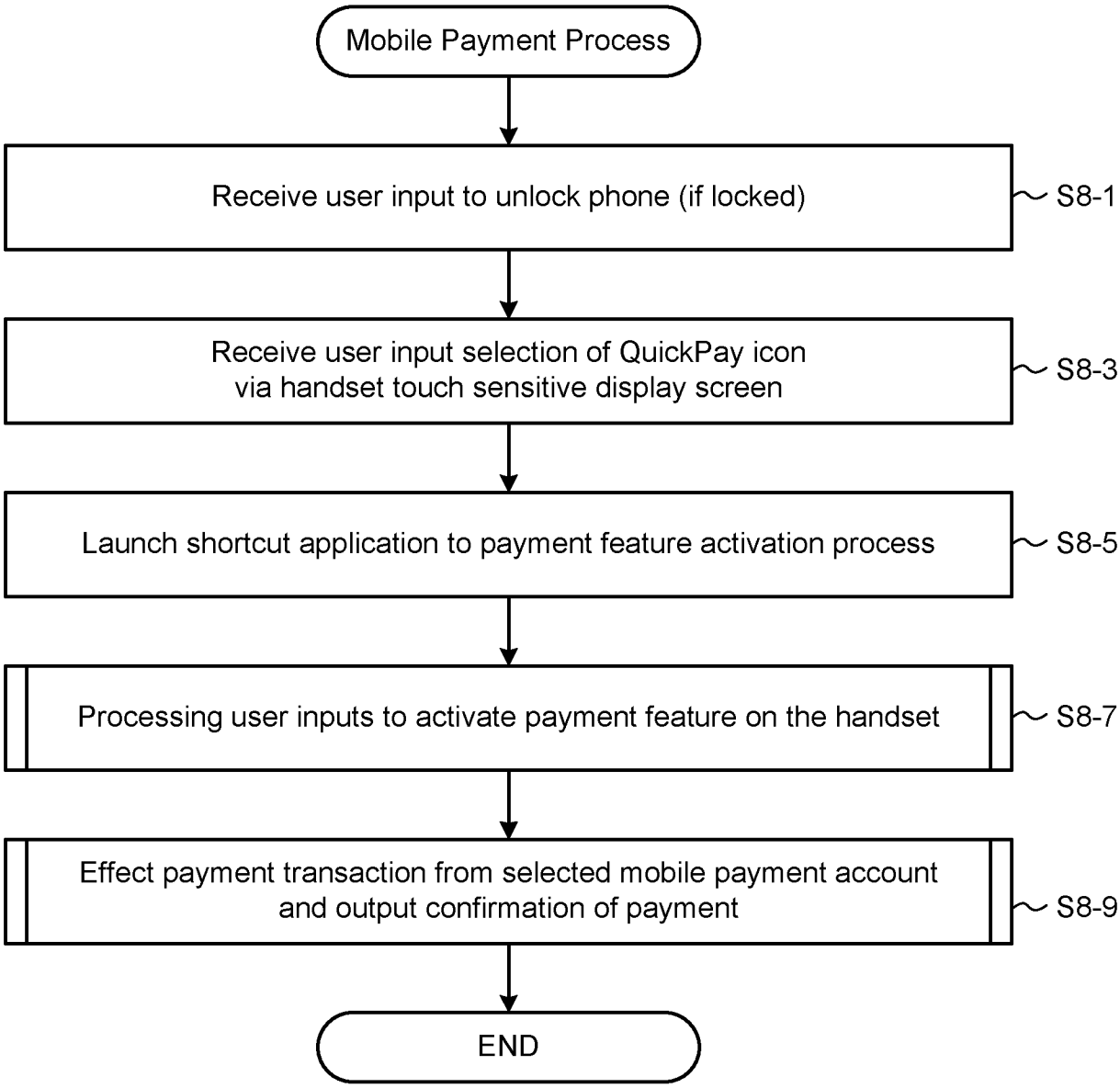

Mobile Payment Process
Receive user input to unlock phone (if locked)
S8-1
Receive user input selection of QuickPay icon via handset touch sensitive display screen
S8-3
Launch shortcut application to payment feature activation process
S8-5
Processing user inputs to activate payment feature on the handset
S8-7
Effect payment transaction from selected mobile payment account and output confirmation of payment
S8-9
END

FIG. 8

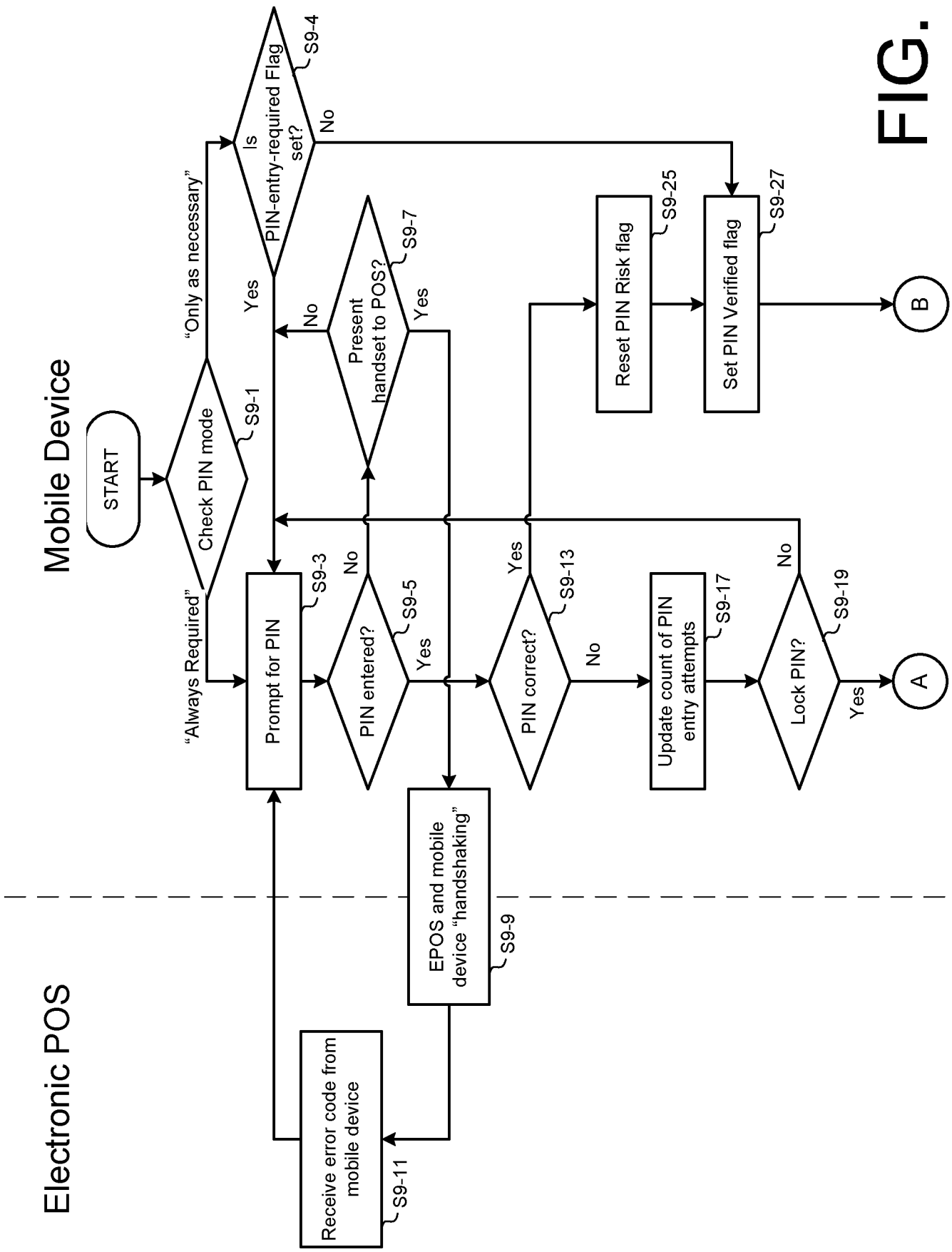

Mobile Device
Electronic POS
START
Check PIN mode
S9-1
"Always Required"
"Only as necessary"
Is PIN-entry-required Flag set?
S9-4
Yes
No
Present handset to POS?
S9-7
Yes
No
Prompt for PIN
S9-3
PIN entered?
S9-5
No
Yes
EPOS and mobile device "handshaking"
S9-9
Receive error code from mobile device
S9-11
PIN correct?
S9-13
Yes
No
Update count of PIN entry attempts
S9-17
Lock PIN?
S9-19
No
Yes
Reset PIN Risk flag
S9-25
Set PIN Verified flag
S9-27
A
B

FIG. 9a

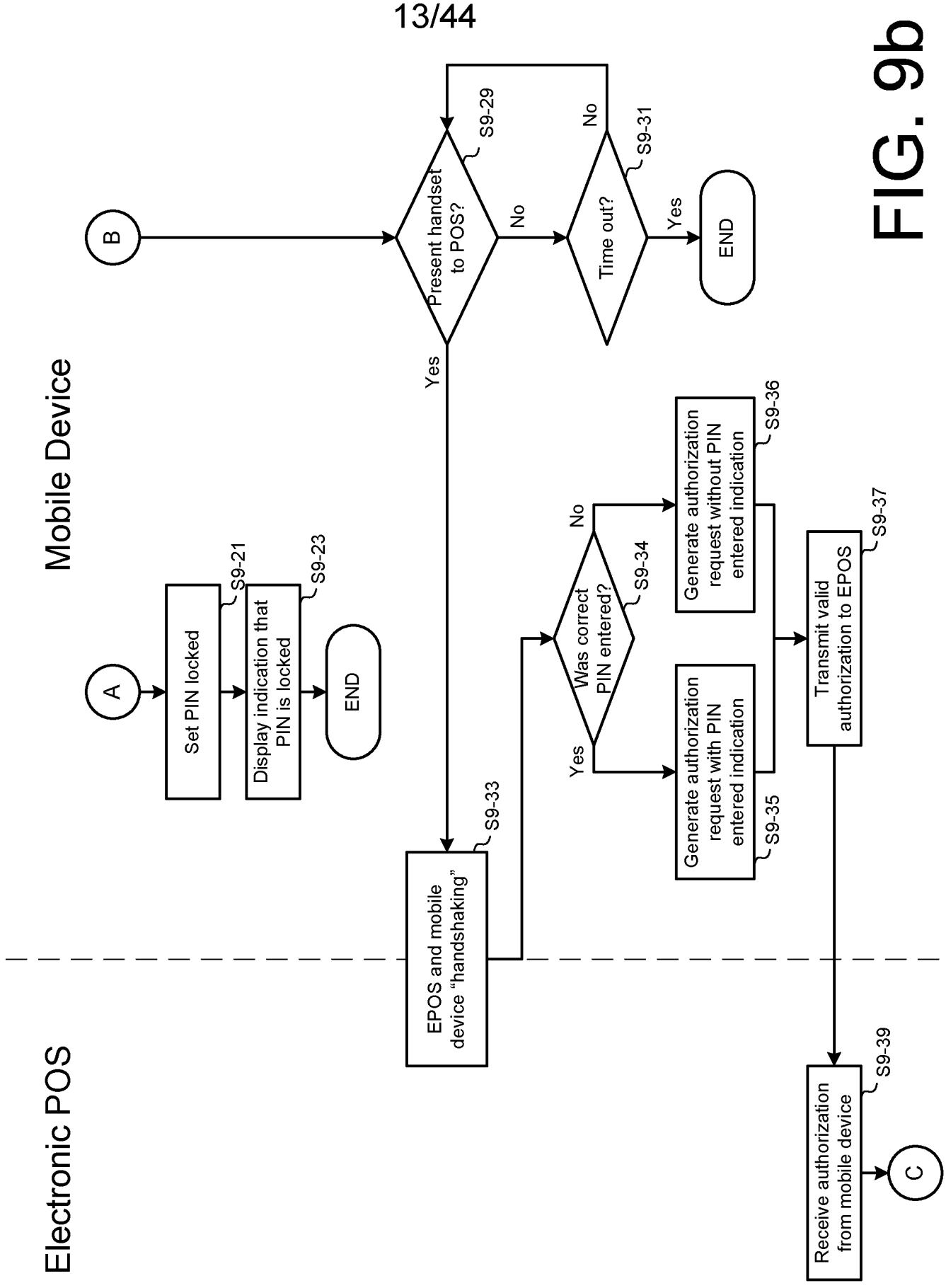

Mobile Device
Electronic POS
A
Set PIN locked
S9-21
Display indication that PIN is locked
S9-23
END
B
Present handset to POS?
S9-29
No
Time out?
S9-31
Yes
END
Yes
EPOS and mobile device "handshaking"
S9-33
Was correct PIN entered?
S9-34
No
Yes
Generate authorization request without PIN entered indication
S9-36
Generate authorization request with PIN entered indication
S9-35
Transmit valid authorization to EPOS
S9-37
Receive authorization from mobile device
S9-39
C

FIG. 9b

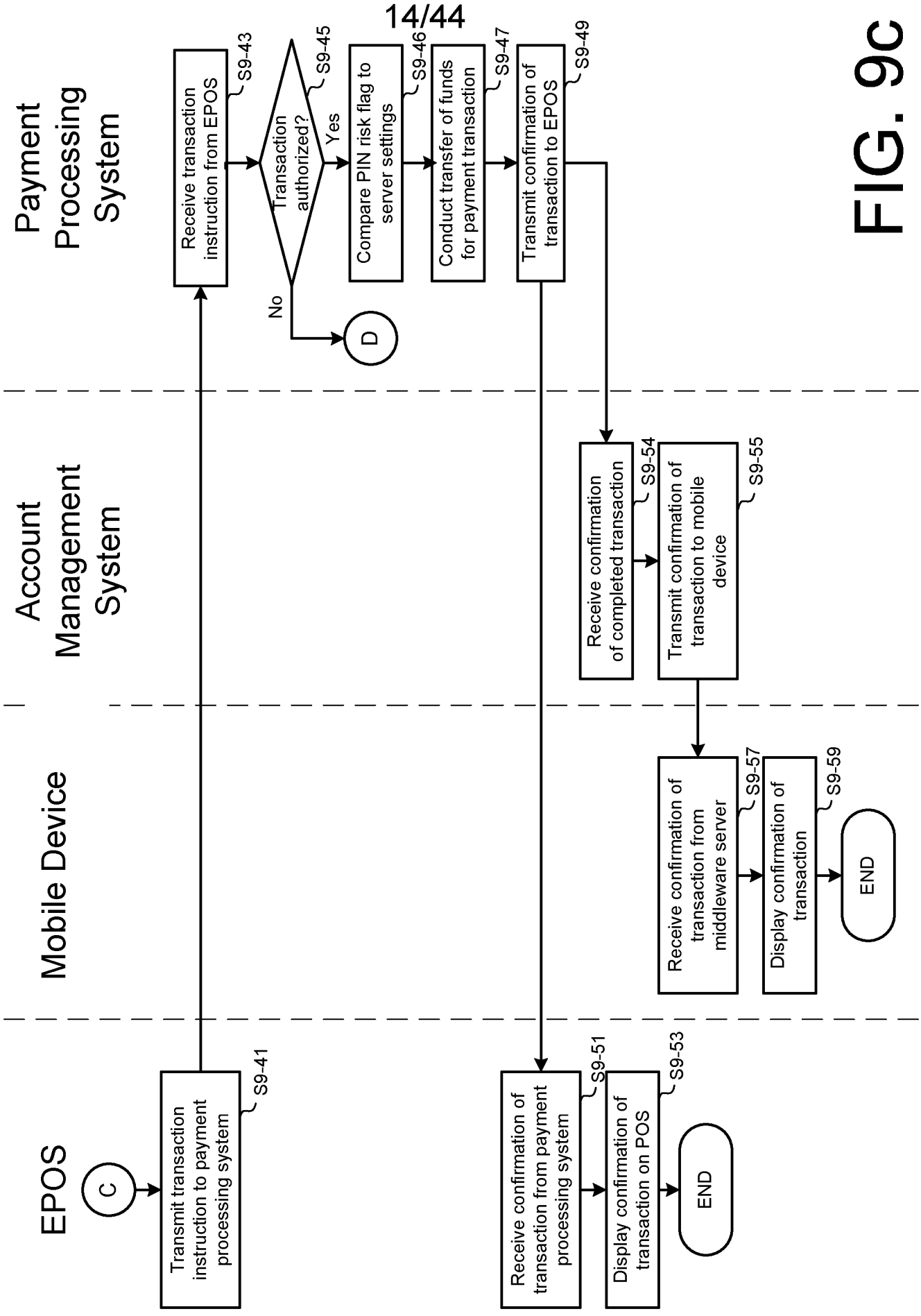

EPOS
Mobile Device
Account Management System
Payment Processing System
C
Transmit transaction instruction to payment processing system
S9-41
Receive transaction instruction from EPOS
S9-43
Transaction authorized?
S9-45
Yes
No
D
Compare PIN risk flag to server settings
S9-46
Conduct transfer of funds for payment transaction
S9-47
Transmit confirmation of transaction to EPOS
S9-49
Receive confirmation of completed transaction
S9-54
Transmit confirmation of transaction to mobile device
S9-55
Receive confirmation of transaction from middleware server
S9-57
Display confirmation of transaction
S9-59
END
Receive confirmation of transaction from payment processing system
S9-51
Display confirmation of transaction on POS
S9-53
END

FIG. 9c

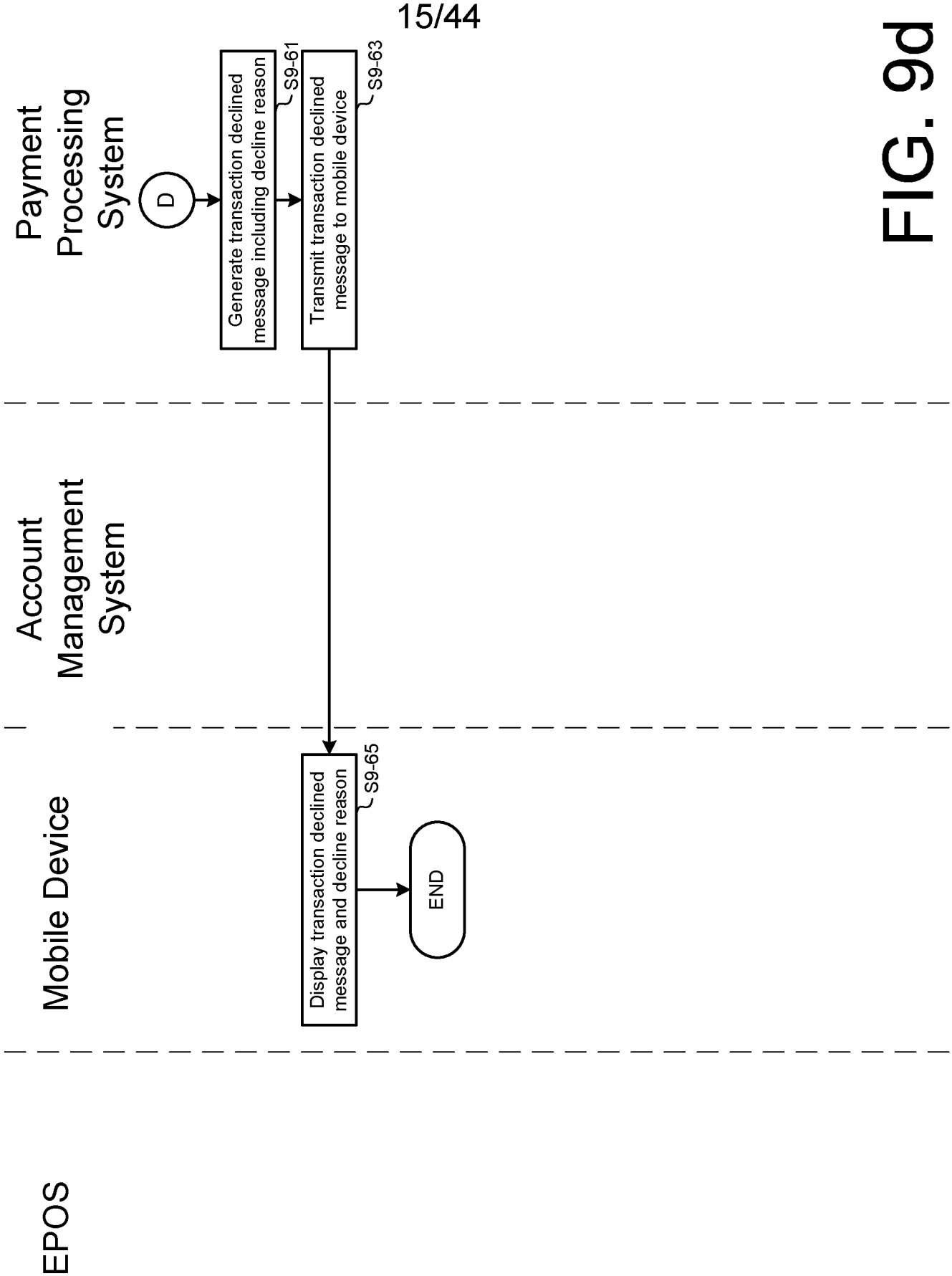

Payment Processing System
Account Management System
Mobile Device
EPOS
D
Generate transaction declined message including decline reason
S9-61
Transmit transaction declined message to mobile device
S9-63
Display transaction declined message and decline reason
S9-65
END

FIG. 9d

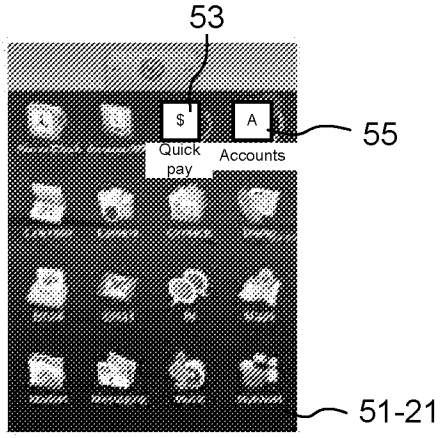


FIG. 10a

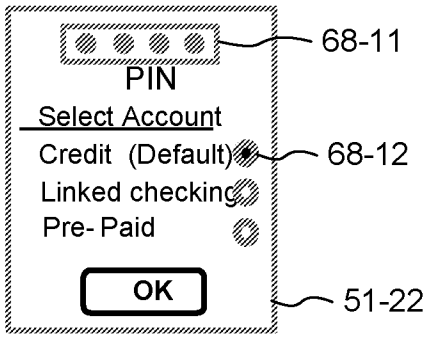


FIG. 10b

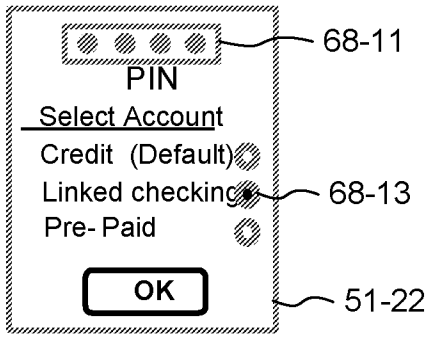


FIG. 10c

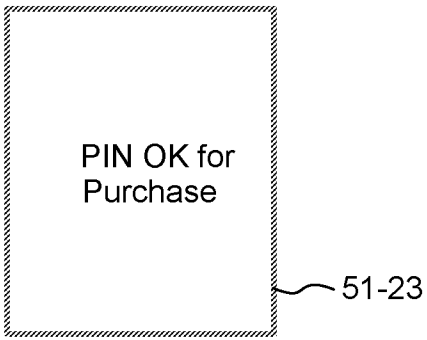


FIG. 10d

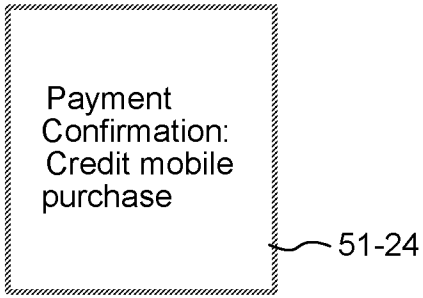


FIG. 10e

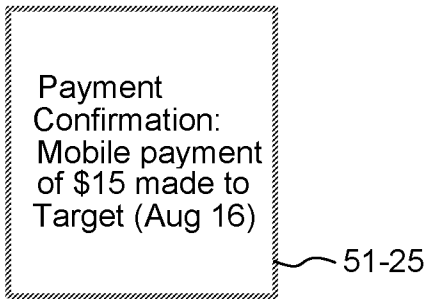


FIG. 10f

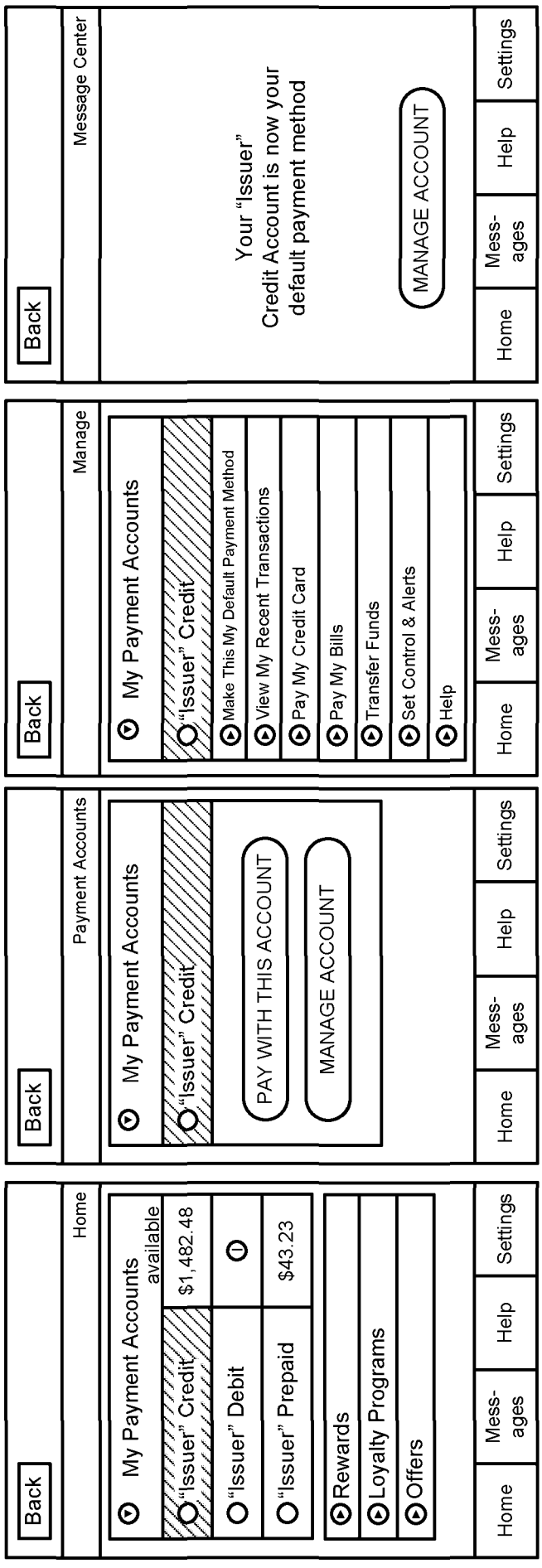


FIG. 11a FIG. 11b FIG. 11c FIG. 11d

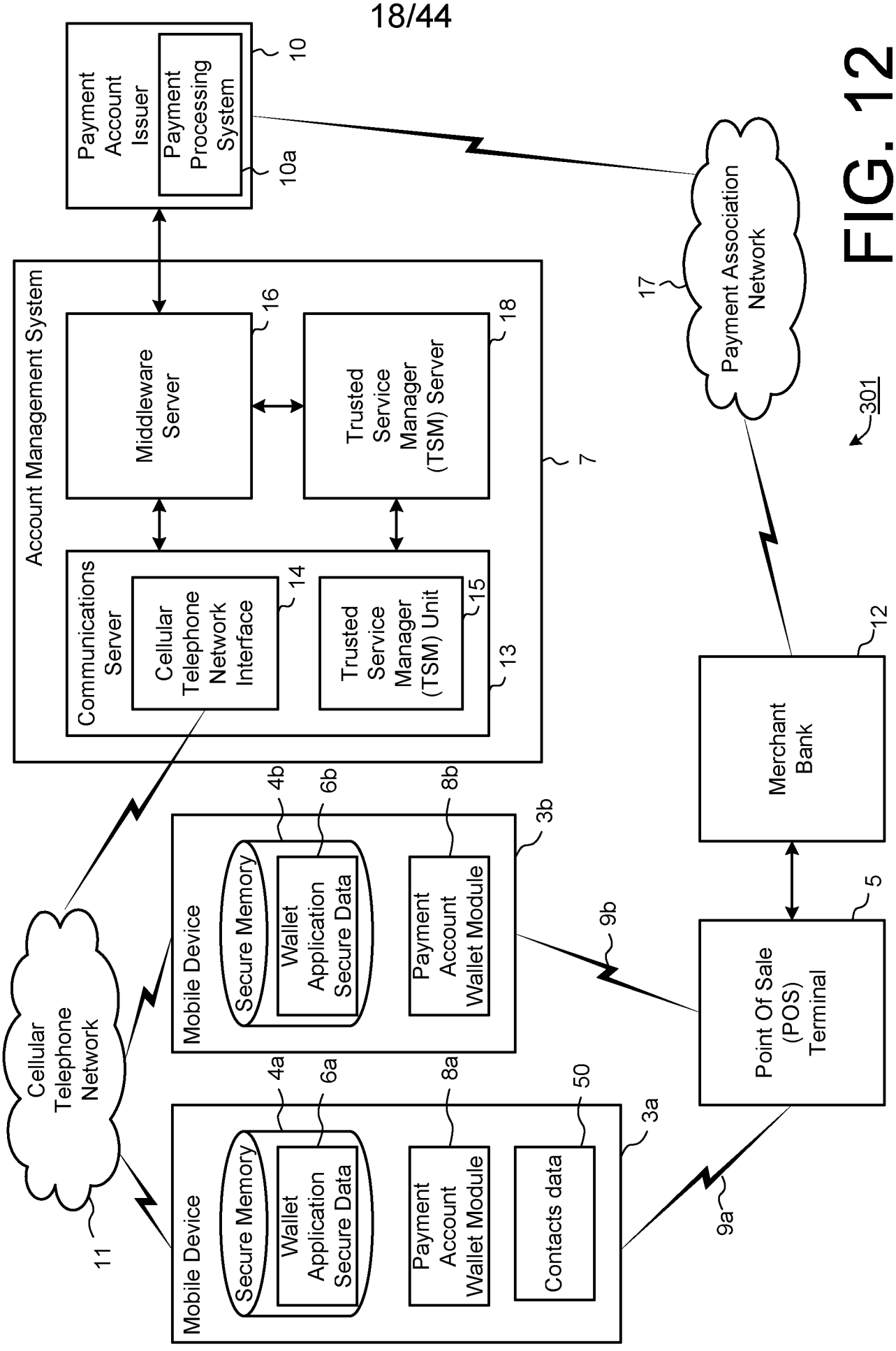

Payment Account Issuer
Payment Processing System
10
10a
Payment Association Network
17
301
Account Management System
Middleware Server
16
Trusted Service Manager (TSM) Server
18
7
Communications Server
Cellular Telephone Network Interface
14
Trusted Service Manager (TSM) Unit
15
13
Merchant Bank
12
Point Of Sale (POS) Terminal
5
9b
9a
Cellular Telephone Network
11
Mobile Device
Secure Memory
Wallet Application Secure Data
4b
6b
Payment Account Wallet Module
8b
3b
Mobile Device
Secure Memory
Wallet Application Secure Data
4a
6a
Payment Account Wallet Module
8a
Contacts data
50
3a

FIG. 12

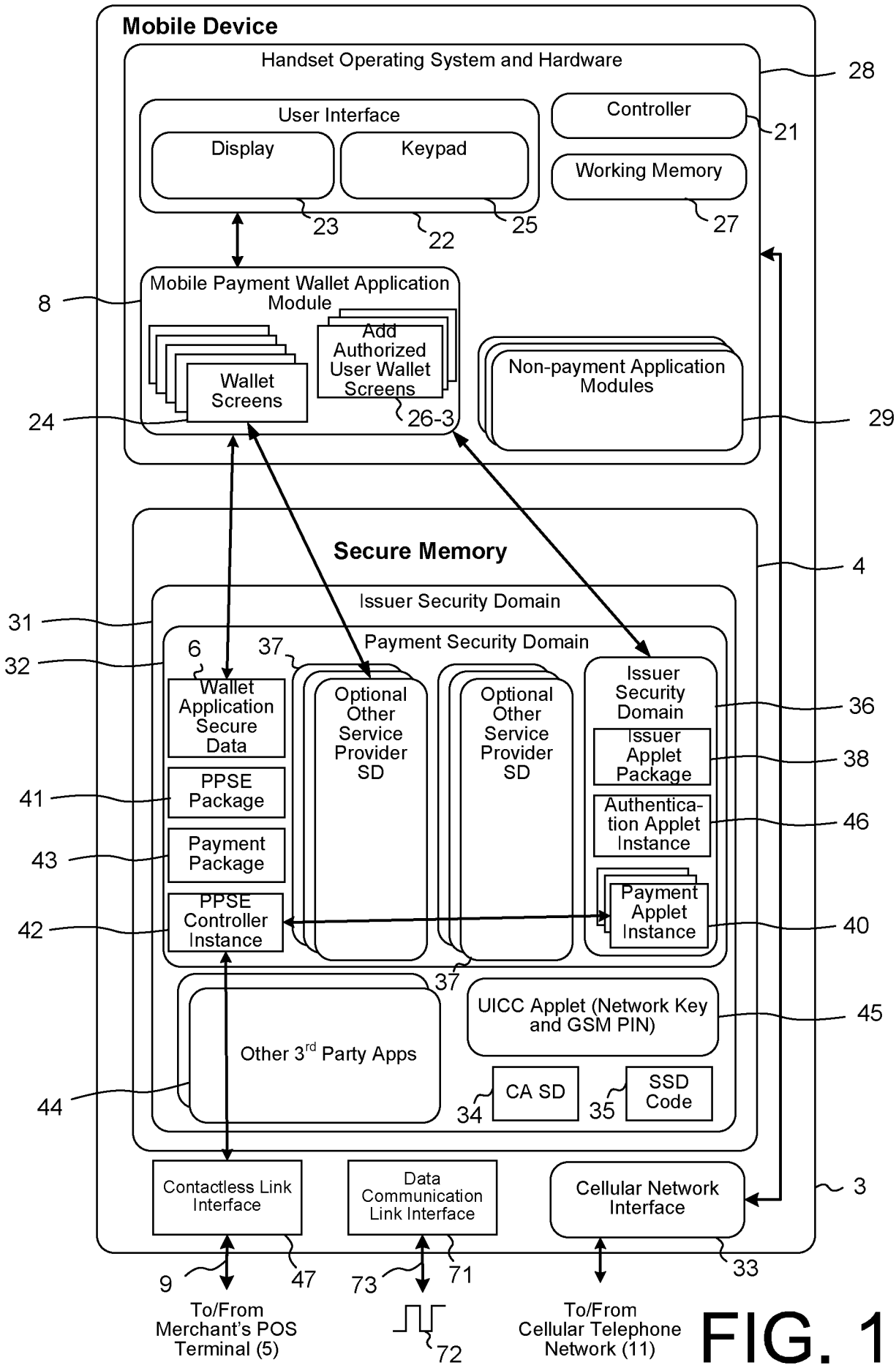

Mobile Device
Handset Operating System and Hardware
28
User Interface
Display
Keypad
23
22
25
Controller
21
Working Memory
27
Mobile Payment Wallet Application Module
8
Wallet Screens
Add Authorized User Wallet Screens
26-3
24
Non-payment Application Modules
29
Secure Memory
4
Issuer Security Domain
31
Payment Security Domain
32
6
37
Wallet Application Secure Data
PPSE Package
41
Payment Package
43
PPSE Controller Instance
42
Optional Other Service Provider SD
Optional Other Service Provider SD
Issuer Security Domain
36
Issuer Applet Package
38
Authentica-tion Applet Instance
46
Payment Applet Instance
40
37
Other 3rd Party Apps
44
UICC Applet (Network Key and GSM PIN)
45
CA SD
34
SSD Code
35
Contactless Link Interface
Data Communication Link Interface
Cellular Network Interface
3
9
47
73
71
33
To/From Merchant's POS Terminal (5)
72
To/From Cellular Telephone Network (11)

FIG. 13

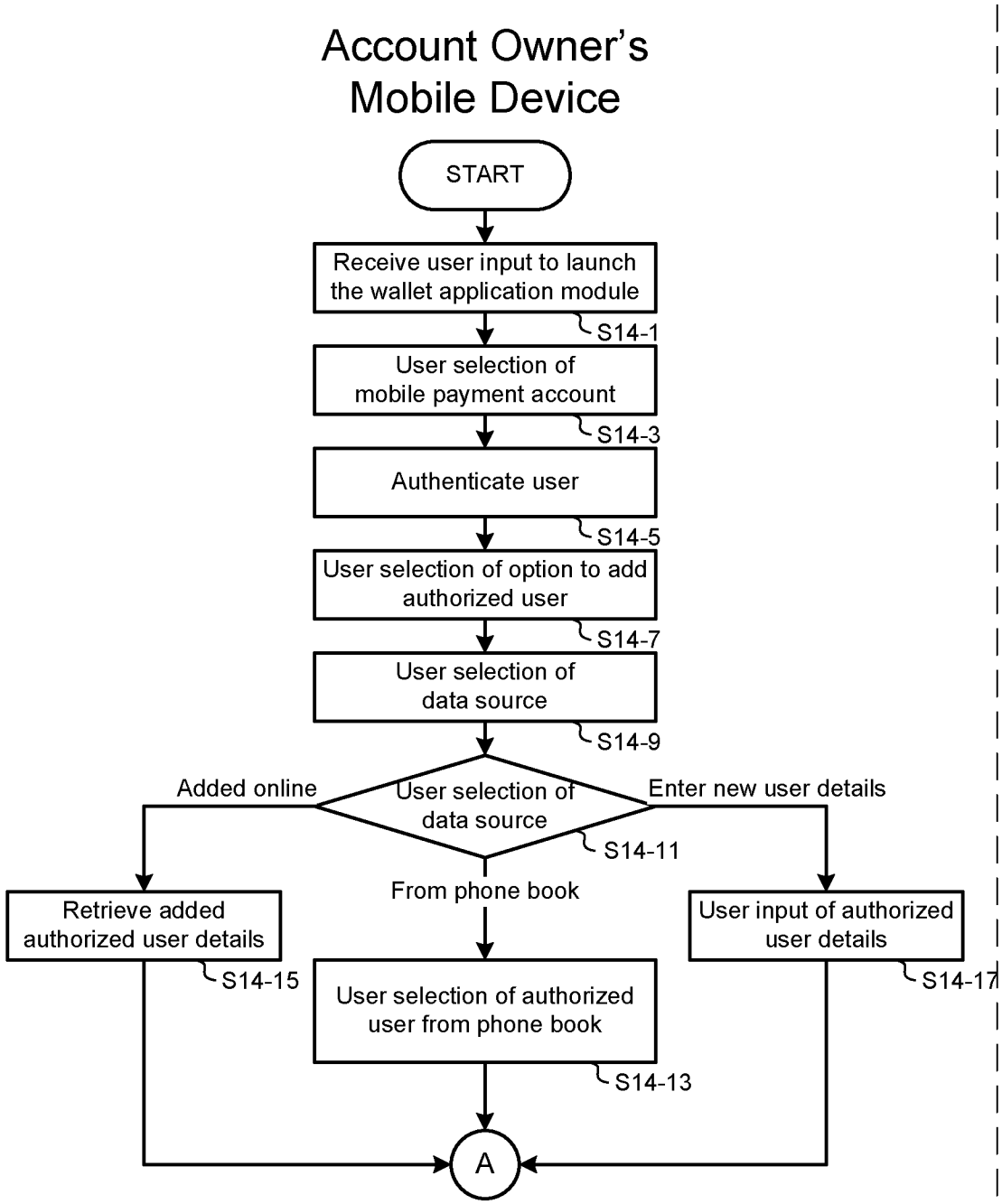

Account Owner's Mobile Device
Middleware Server
Authorized User's Mobile Device
START
Receive user input to launch the wallet application module
S14-1
User selection of mobile payment account
S14-3
Authenticate user
S14-5
User selection of option to add authorized user
S14-7
User selection of data source
S14-9
User selection of data source
S14-11
Added online
Enter new user details
From phone book
Retrieve added authorized user details
S14-15
User input of authorized user details
S14-17
User selection of authorized user from phone book
S14-13
A

FIG. 14a

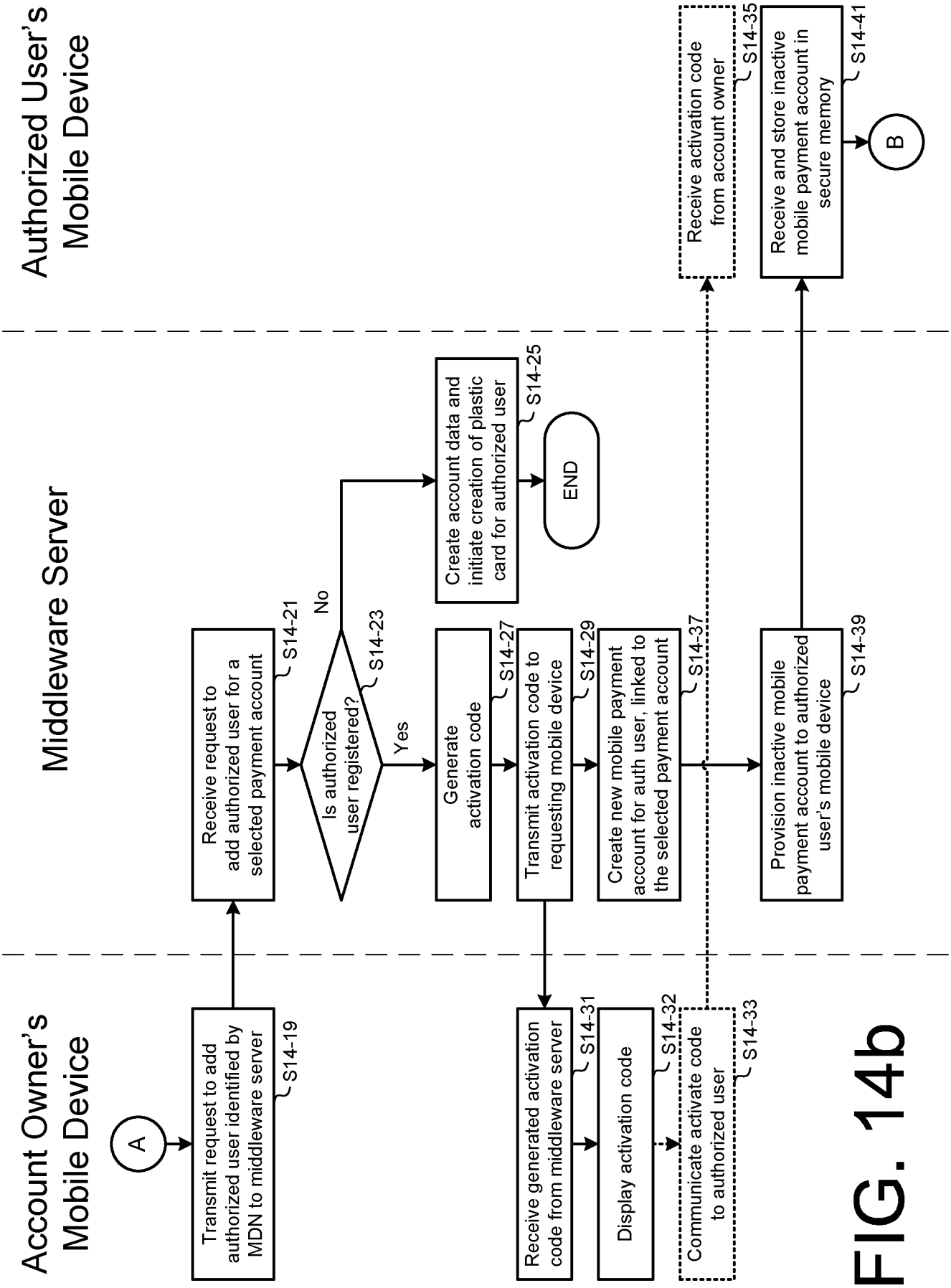

Account Owner's Mobile Device
Middleware Server
Authorized User's Mobile Device
A
Transmit request to add authorized user identified by MDN to middleware server
S14-19
Receive request to add authorized user for a selected payment account
S14-21
Is authorized user registered?
S14-23
No
Yes
Create account data and initiate creation of plastic card for authorized user
S14-25
END
Generate activation code
S14-27
Transmit activation code to requesting mobile device
S14-29
Create new mobile payment account for auth user, linked to the selected payment account
S14-37
Provision inactive mobile payment account to authorized user's mobile device
S14-39
Receive activation code from account owner
S14-35
Receive and store inactive mobile payment account in secure memory
S14-41
B
Receive generated activation code from middleware server
S14-31
Display activation code
S14-32
Communicate activate code to authorized user
S14-33

FIG. 14b

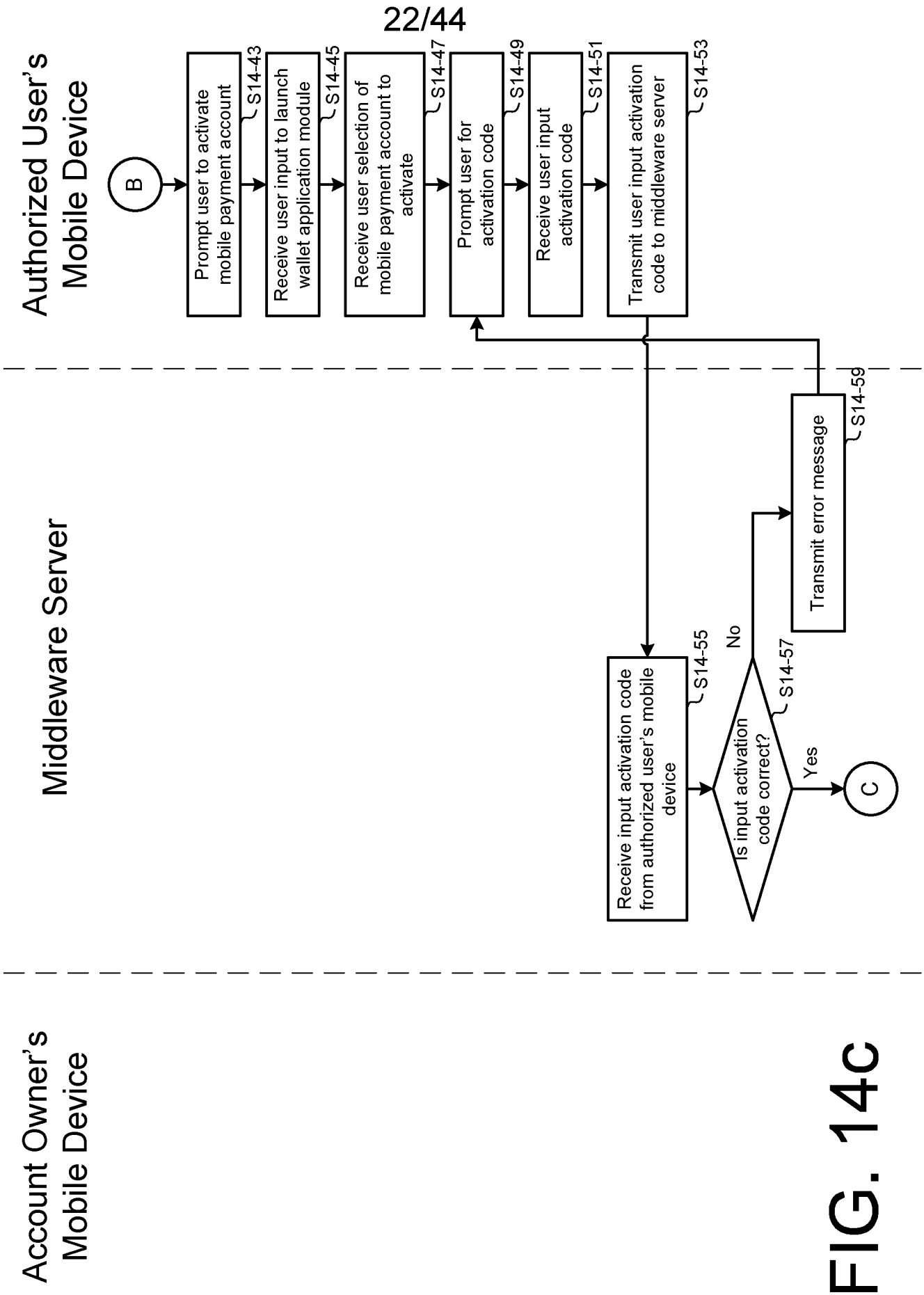

Authorized User's Mobile Device
Middleware Server
Account Owner's Mobile Device
B
Prompt user to activate mobile payment account
S14-43
Receive user input to launch wallet application module
S14-45
Receive user selection of mobile payment account to activate
S14-47
Prompt user for activation code
S14-49
Receive user input activation code
S14-51
Transmit user input activation code to middleware server
S14-53
Receive input activation code from authorized user's mobile device
S14-55
Is input activation code correct?
S14-57
No
Yes
Transmit error message
S14-59
C

FIG. 14c

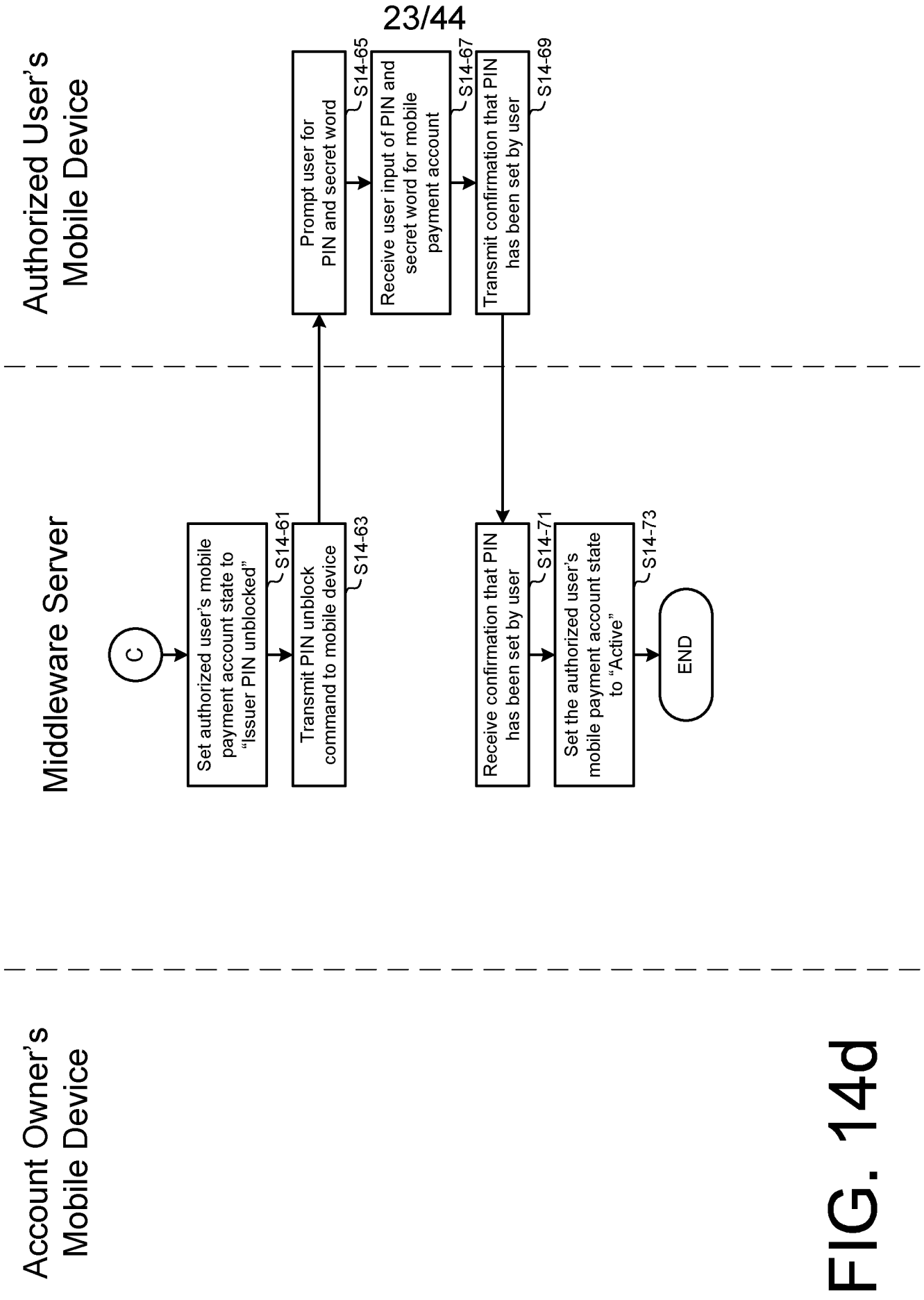

Authorized User's Mobile Device
Middleware Server
Account Owner's Mobile Device
C
Set authorized user's mobile payment account state to "Issuer PIN unblocked"
S14-61
Transmit PIN unblock command to mobile device
S14-63
Prompt user for PIN and secret word
S14-65
Receive user input of PIN and secret word for mobile payment account
S14-67
Transmit confirmation that PIN has been set by user
S14-69
Receive confirmation that PIN has been set by user
S14-71
Set the authorized user's mobile payment account state to "Active"
S14-73
END

FIG. 14d

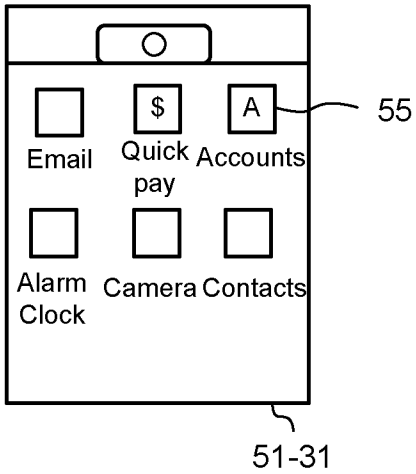


FIG. 15a

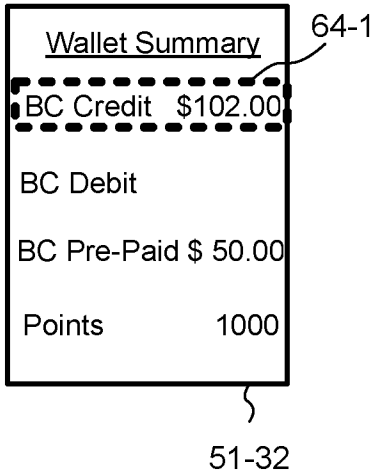


FIG. 15b

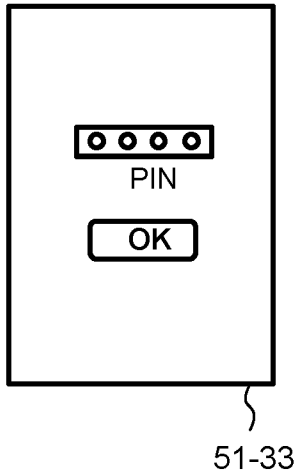


FIG. 15c

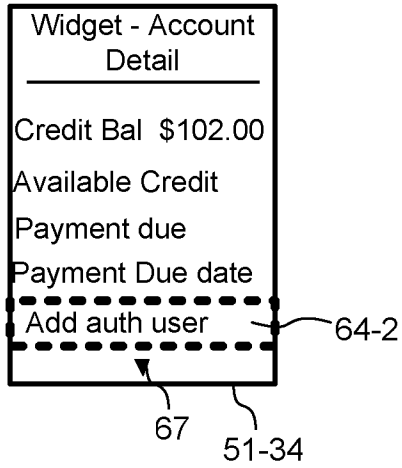


FIG. 15d

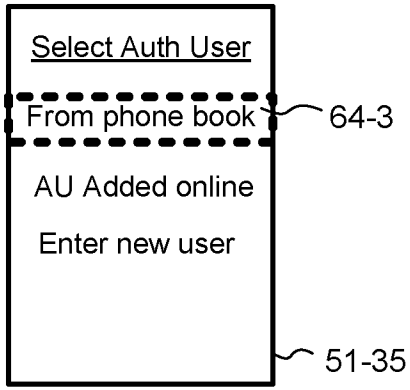


FIG. 15e

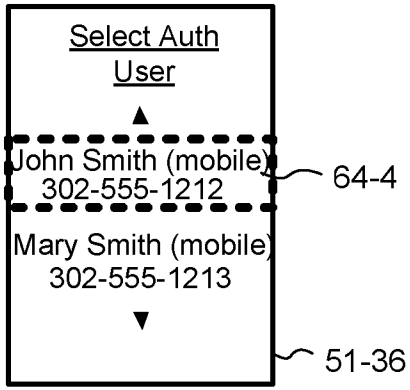


FIG. 15f

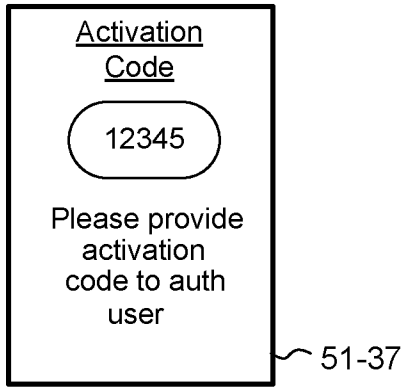


FIG. 15g

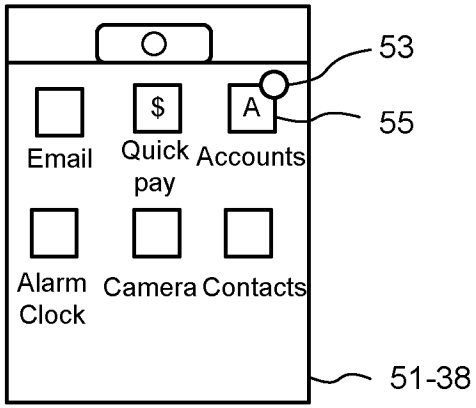


FIG. 16a

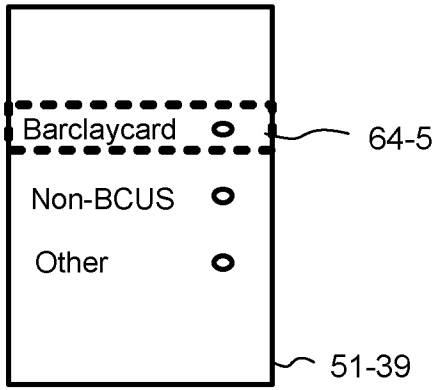


FIG. 16b

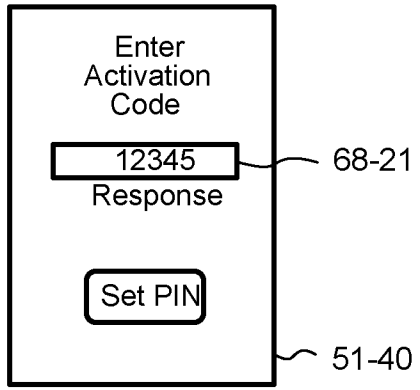


FIG. 16c

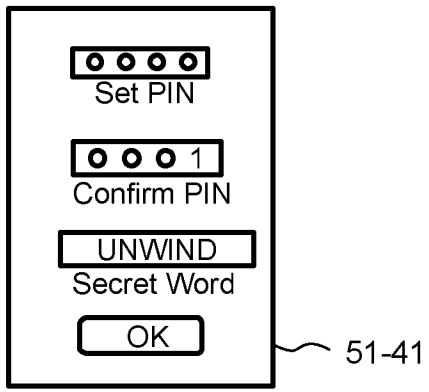


FIG. 16d

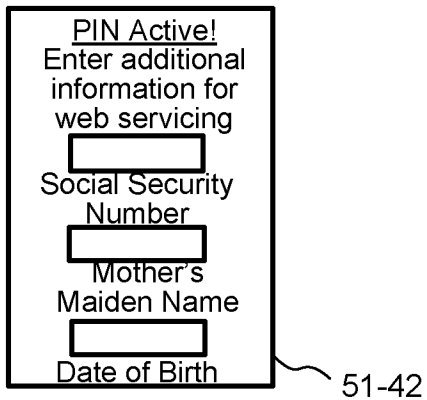


FIG. 16e

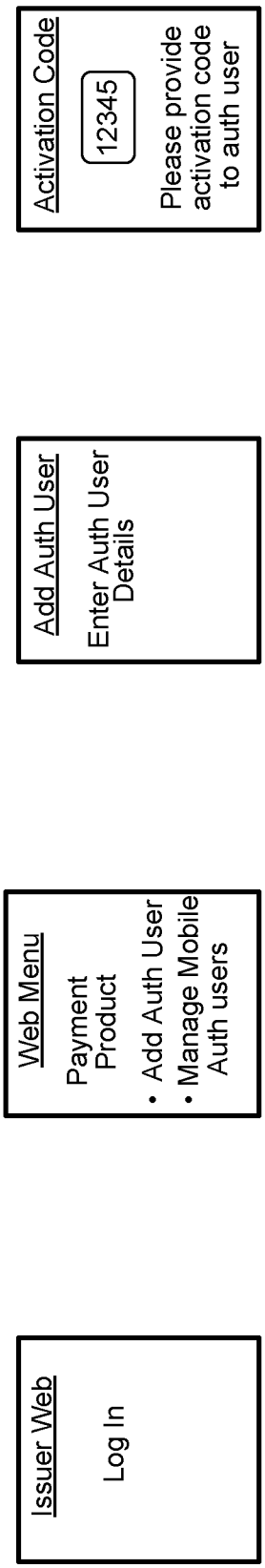


FIG. 17a

FIG. 17b

FIG. 17c

FIG. 17d

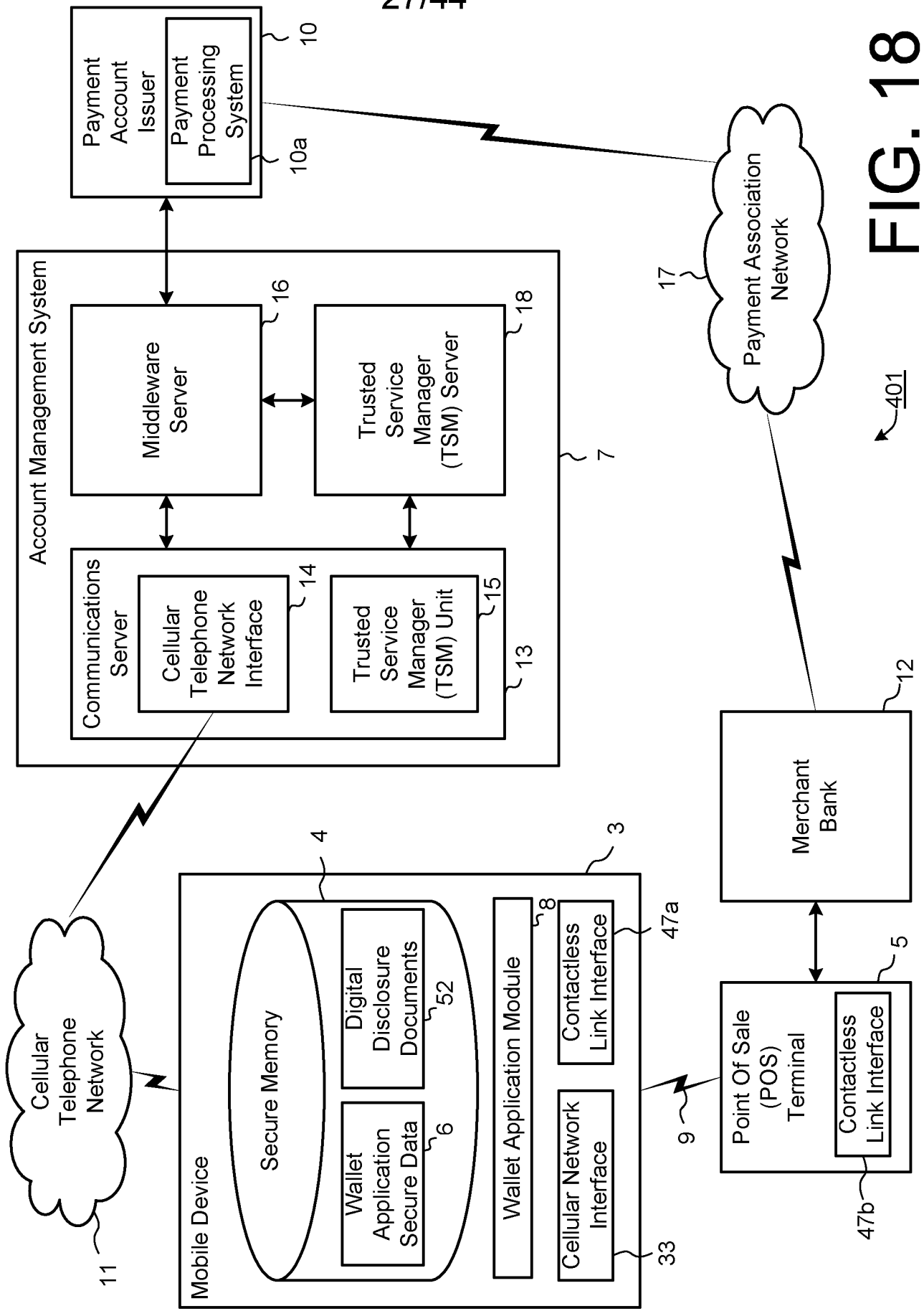

Payment Account Issuer
Payment Processing System
10
10a
Account Management System
Middleware Server
16
Trusted Service Manager (TSM) Server
18
7
Communications Server
Cellular Telephone Network Interface
14
Trusted Service Manager (TSM) Unit
15
13
Payment Association Network
17
401
Merchant Bank
12
Cellular Telephone Network
11
Mobile Device
4
Secure Memory
Digital Disclosure Documents
52
Wallet Application Secure Data
6
Wallet Application Module
8
Contactless Link Interface
47a
3
Cellular Network Interface
33
9
Point Of Sale (POS) Terminal
Contactless Link Interface
5
47b

FIG. 18

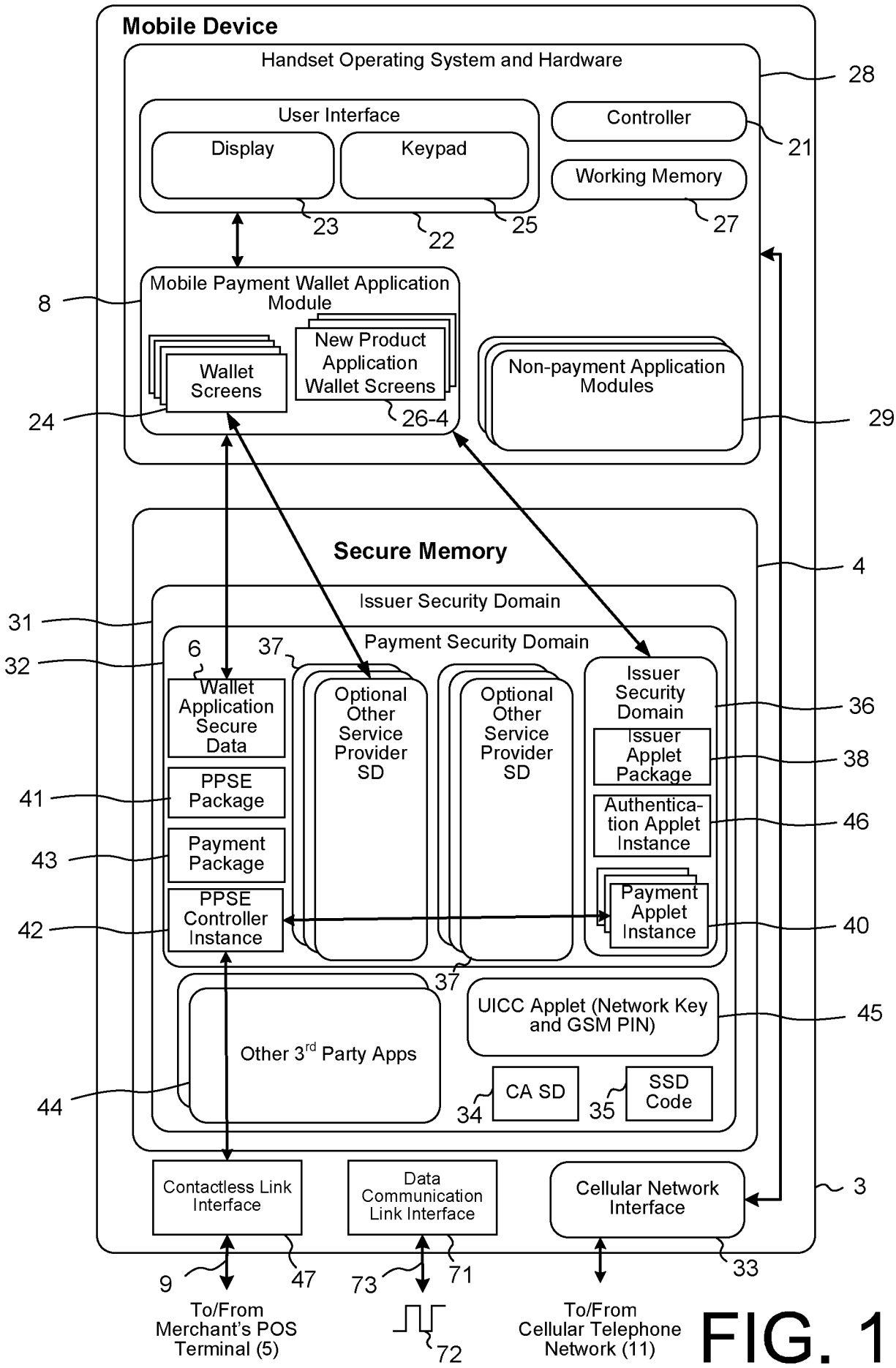

Mobile Device
Handset Operating System and Hardware
28
User Interface
Display
Keypad
23
22
25
Controller
21
Working Memory
27
Mobile Payment Wallet Application Module
8
Wallet Screens
New Product Application Wallet Screens
26-4
24
Non-payment Application Modules
29
Secure Memory
4
Issuer Security Domain
31
Payment Security Domain
32
6
37
Wallet Application Secure Data
PPSE Package
41
Payment Package
43
PPSE Controller Instance
42
Optional Other Service Provider SD
Optional Other Service Provider SD
Issuer Security Domain
36
Issuer Applet Package
38
Authentica-tion Applet Instance
46
Payment Applet Instance
40
37
Other 3rd Party Apps
44
UICC Applet (Network Key and GSM PIN)
45
CA SD
34
SSD Code
35
Contactless Link Interface
Data Communication Link Interface
Cellular Network Interface
3
9
47
73
71
33
To/From Merchant's POS Terminal (5)
72
To/From Cellular Telephone Network (11)

FIG. 19

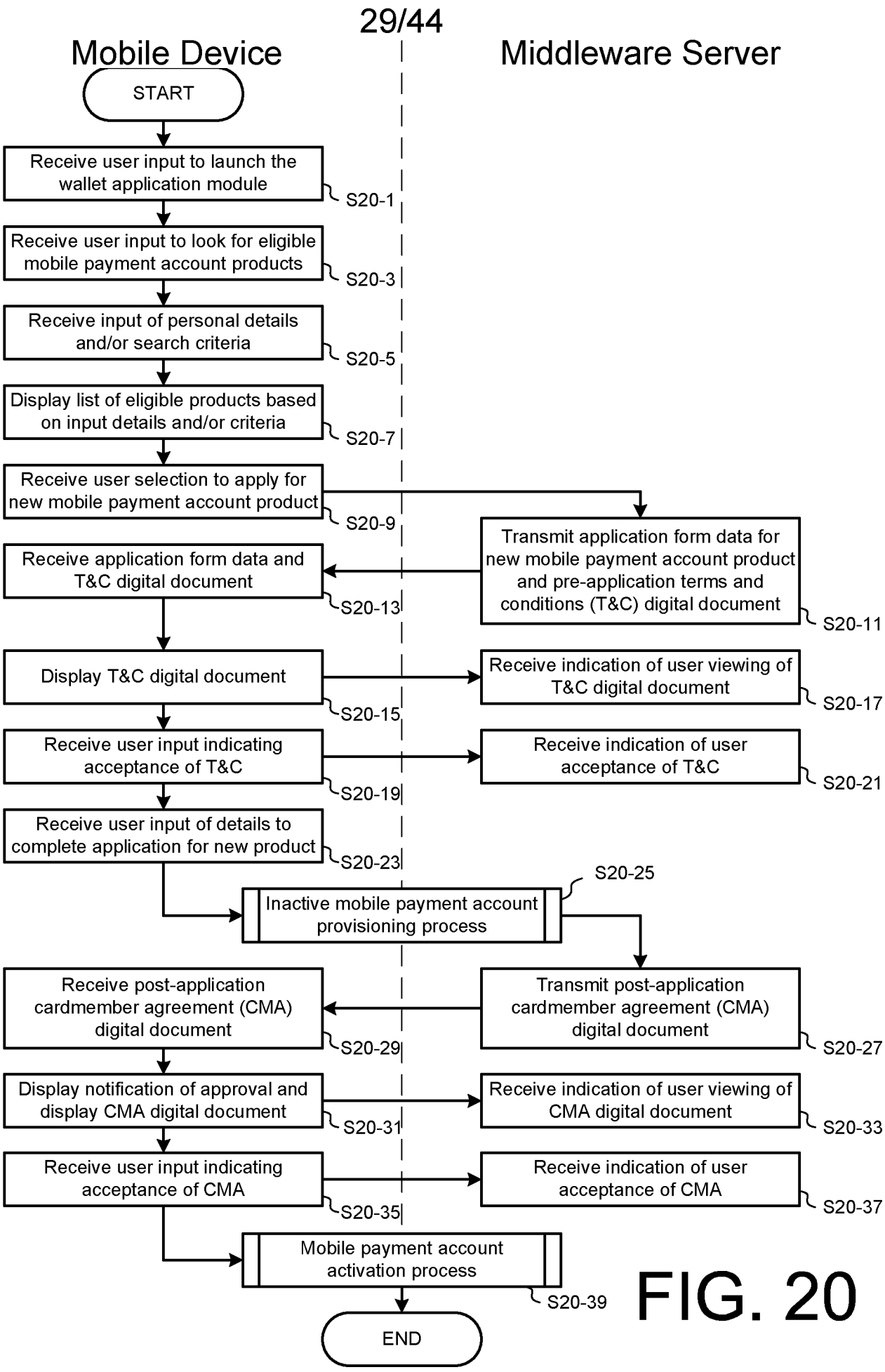

Mobile Device
Middleware Server
START
Receive user input to launch the wallet application module
S20-1
Receive user input to look for eligible mobile payment account products
S20-3
Receive input of personal details and/or search criteria
S20-5
Display list of eligible products based on input details and/or criteria
S20-7
Receive user selection to apply for new mobile payment account product
S20-9
Transmit application form data for new mobile payment account product and pre-application terms and conditions (T&C) digital document
S20-11
Receive application form data and T&C digital document
S20-13
Display T&C digital document
S20-15
Receive indication of user viewing of T&C digital document
S20-17
Receive user input indicating acceptance of T&C
S20-19
Receive indication of user acceptance of T&C
S20-21
Receive user input of details to complete application for new product
S20-23
S20-25
Inactive mobile payment account provisioning process
Receive post-application cardmember agreement (CMA) digital document
S20-29
Transmit post-application cardmember agreement (CMA) digital document
S20-27
Display notification of approval and display CMA digital document
S20-31
Receive indication of user viewing of CMA digital document
S20-33
Receive user input indicating acceptance of CMA
S20-35
Receive indication of user acceptance of CMA
S20-37
Mobile payment account activation process
S20-39
END

FIG. 20

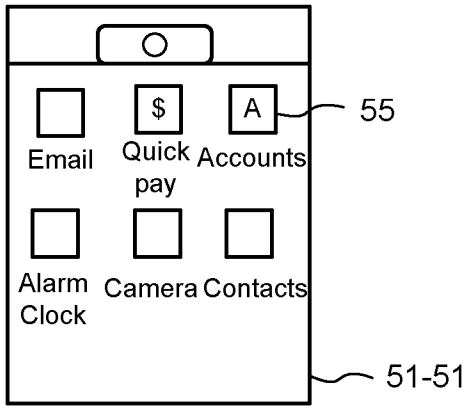


FIG. 21a

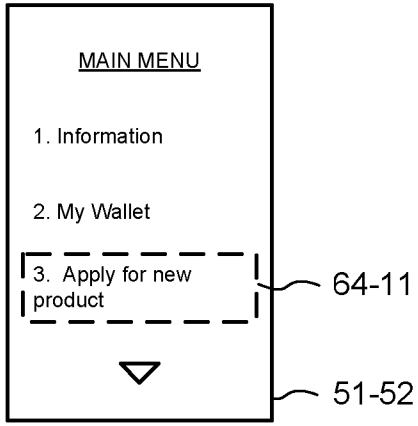


FIG. 21b

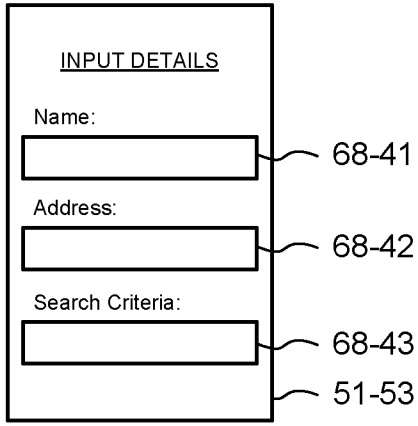


FIG. 21c

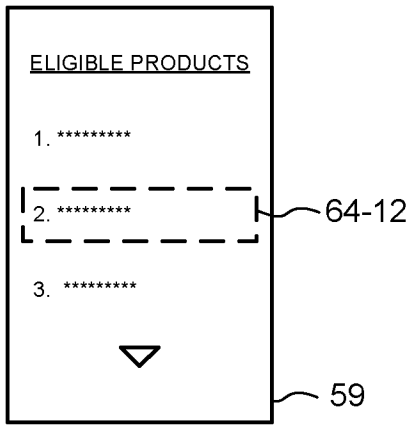


FIG. 21d

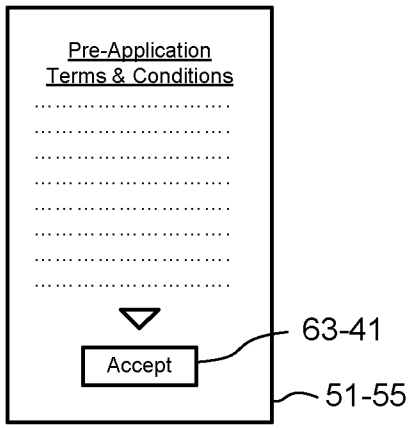


FIG. 21e

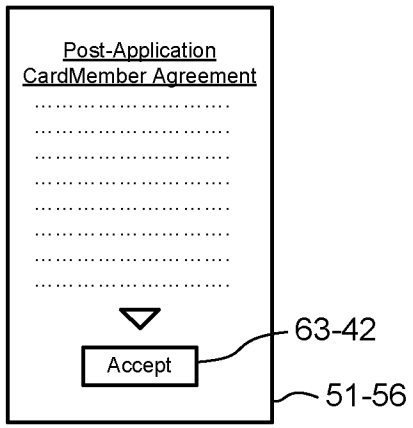


FIG. 21f

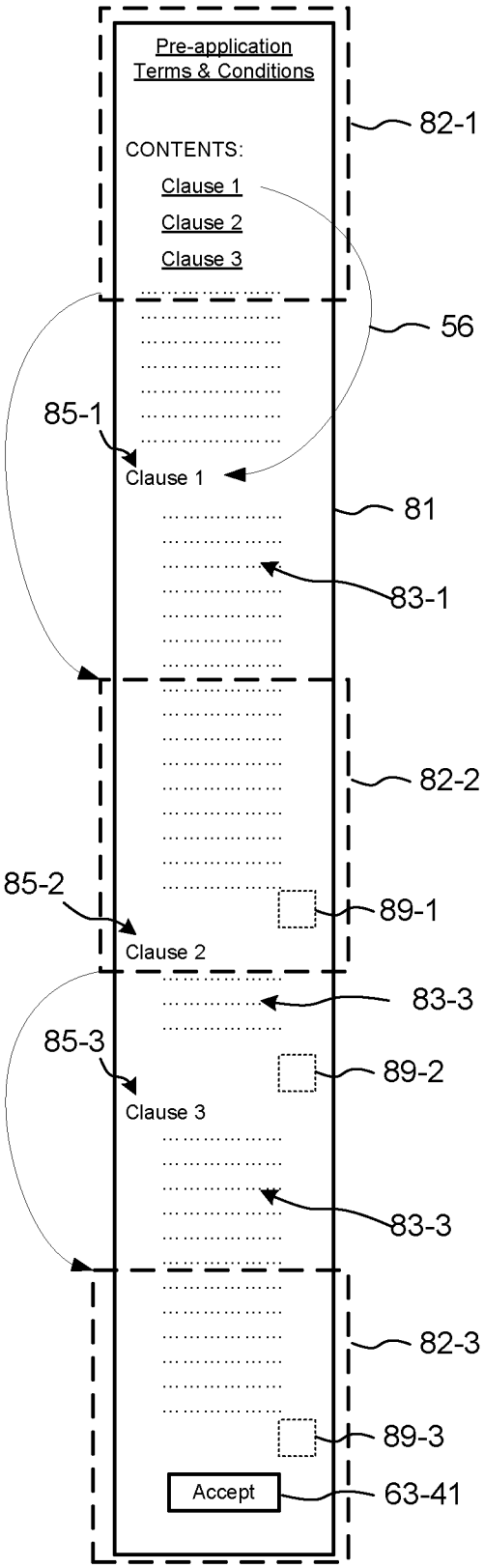

Pre-application
Terms & Conditions
CONTENTS:
Clause 1
Clause 2
Clause 3
82-1
56
85-1
Clause 1
81
83-1
82-2
85-2
89-1
Clause 2
83-3
85-3
89-2
Clause 3
83-3
82-3
89-3
Accept
63-41

FIG. 22

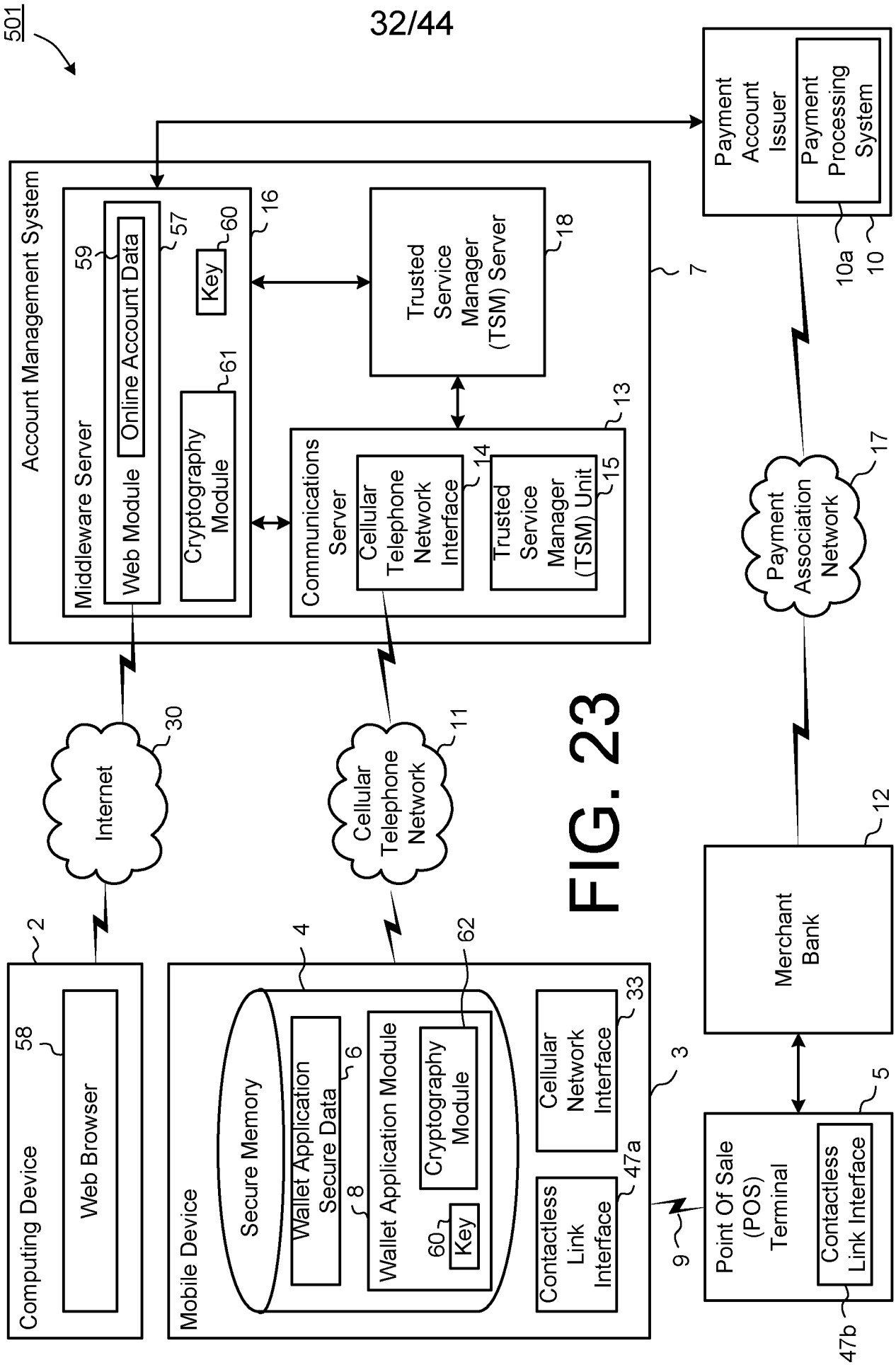

501
Account Management System
Middleware Server
59
Web Module
Online Account Data
57
Cryptography Module
61
Key
60
16
Trusted Service Manager (TSM) Server
18
Communications Server
13
Cellular Telephone Network Interface
14
Trusted Service Manager (TSM) Unit
15
7
Payment Account Issuer
Payment Processing System
10a
10
Payment Association Network
17
Internet
30
Cellular Telephone Network
11
Computing Device
2
58
Web Browser
Mobile Device
4
Secure Memory
Wallet Application Secure Data
6
8
Wallet Application Module
Cryptography Module
62
60
Key
Cellular Network Interface
33
Contactless Link Interface
47a
3
Merchant Bank
12
9
Point Of Sale (POS) Terminal
Contactless Link Interface
5
47b

FIG. 23

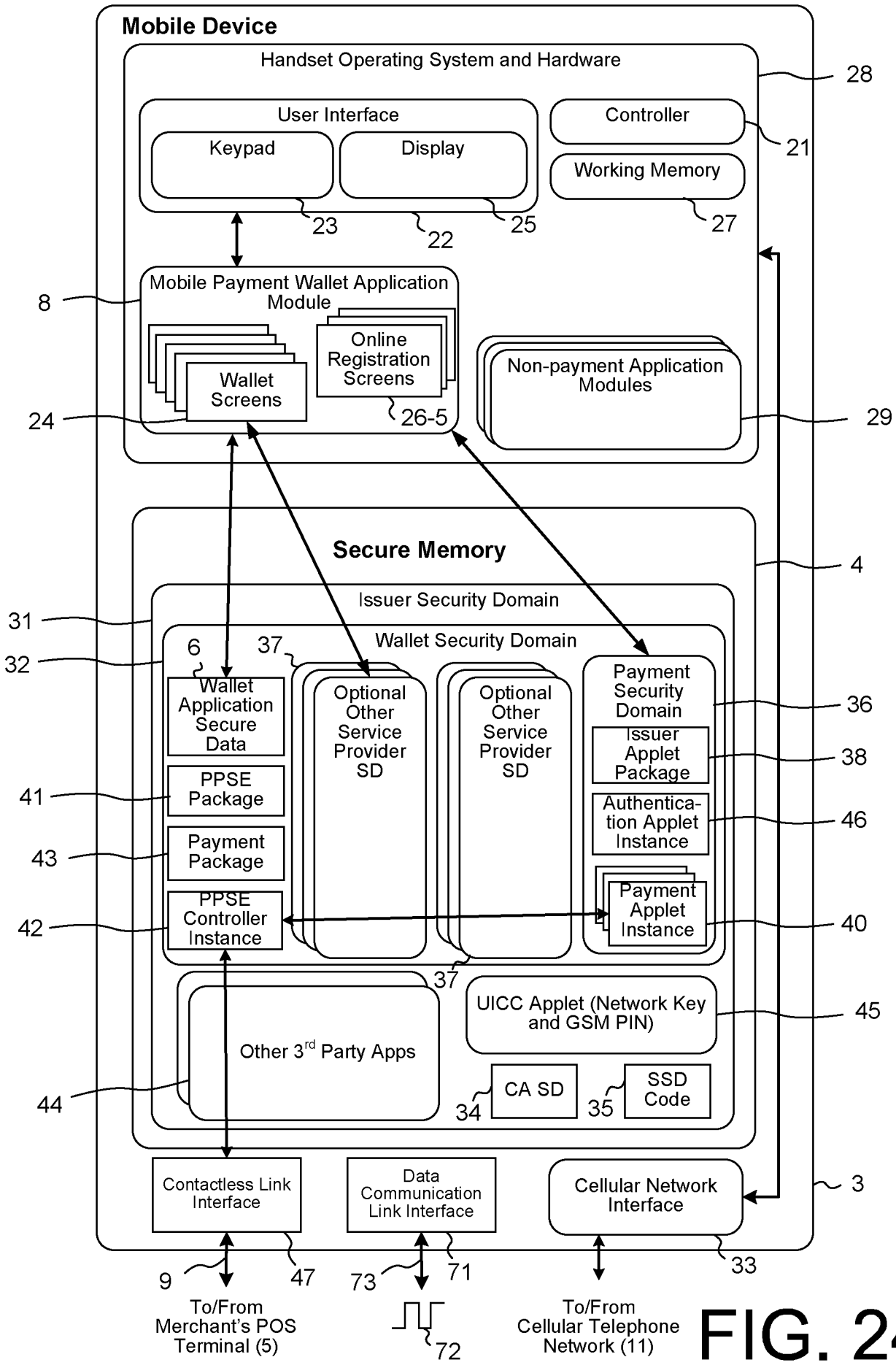

Mobile Device
Handset Operating System and Hardware
28
User Interface
Keypad
Display
23
22
25
Controller
21
Working Memory
27
Mobile Payment Wallet Application Module
8
Wallet Screens
Online Registration Screens
26-5
24
Non-payment Application Modules
29
Secure Memory
4
Issuer Security Domain
31
Wallet Security Domain
32
6
37
Wallet Application Secure Data
PPSE Package
41
Payment Package
43
PPSE Controller Instance
42
Optional Other Service Provider SD
Optional Other Service Provider SD
Payment Security Domain
36
Issuer Applet Package
38
Authentica-tion Applet Instance
46
Payment Applet Instance
40
37
Other 3rd Party Apps
44
UICC Applet (Network Key and GSM PIN)
45
CA SD
34
SSD Code
35
Contactless Link Interface
Data Communication Link Interface
Cellular Network Interface
3
9
47
73
71
33
To/From Merchant's POS Terminal (5)
72
To/From Cellular Telephone Network (11)

FIG. 24

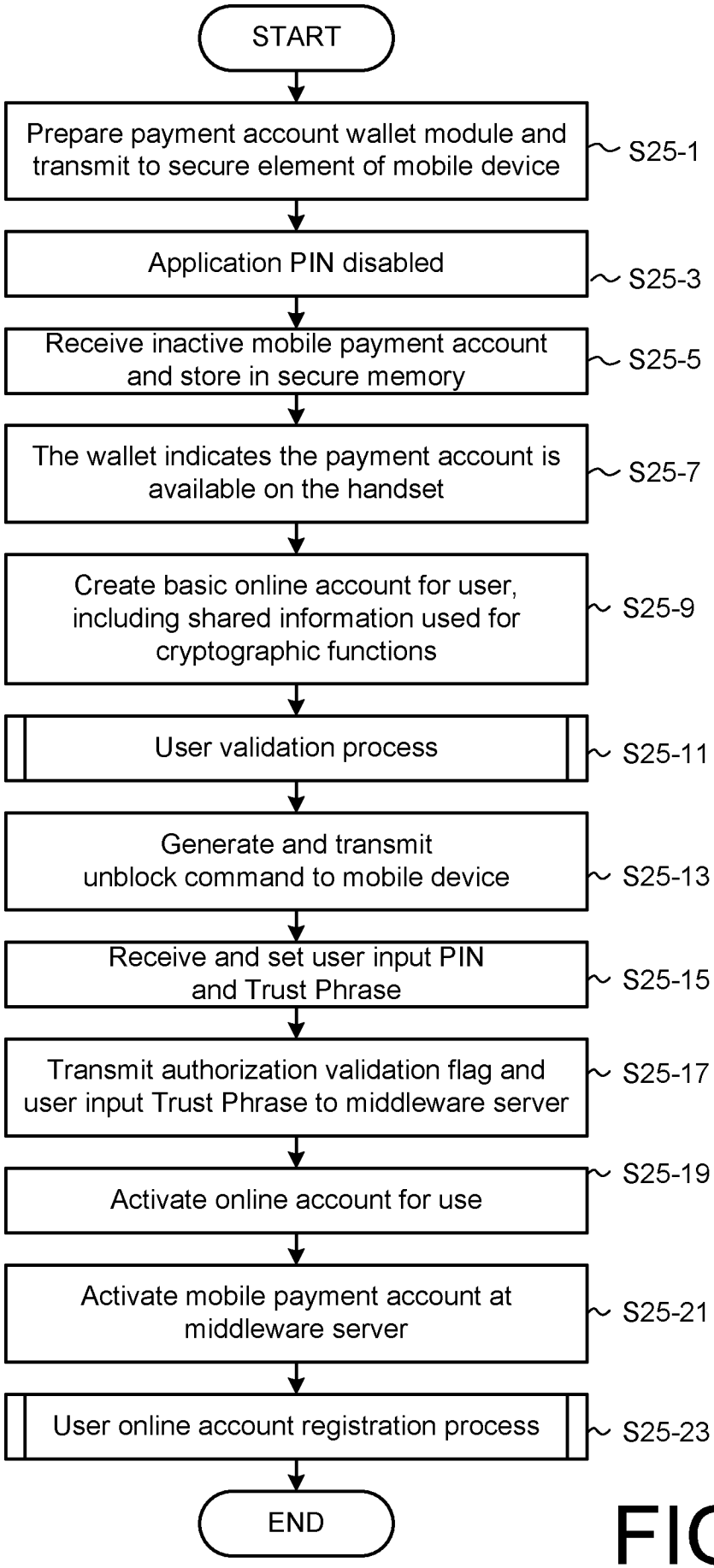

START
Prepare payment account wallet module and transmit to secure element of mobile device
S25-1
Application PIN disabled
S25-3
Receive inactive mobile payment account and store in secure memory
S25-5
The wallet indicates the payment account is available on the handset
S25-7
Create basic online account for user, including shared information used for cryptographic functions
S25-9
User validation process
S25-11
Generate and transmit unblock command to mobile device
S25-13
Receive and set user input PIN and Trust Phrase
S25-15
Transmit authorization validation flag and user input Trust Phrase to middleware server
S25-17
Activate online account for use
S25-19
Activate mobile payment account at middleware server
S25-21
User online account registration process
S25-23
END

FIG. 25

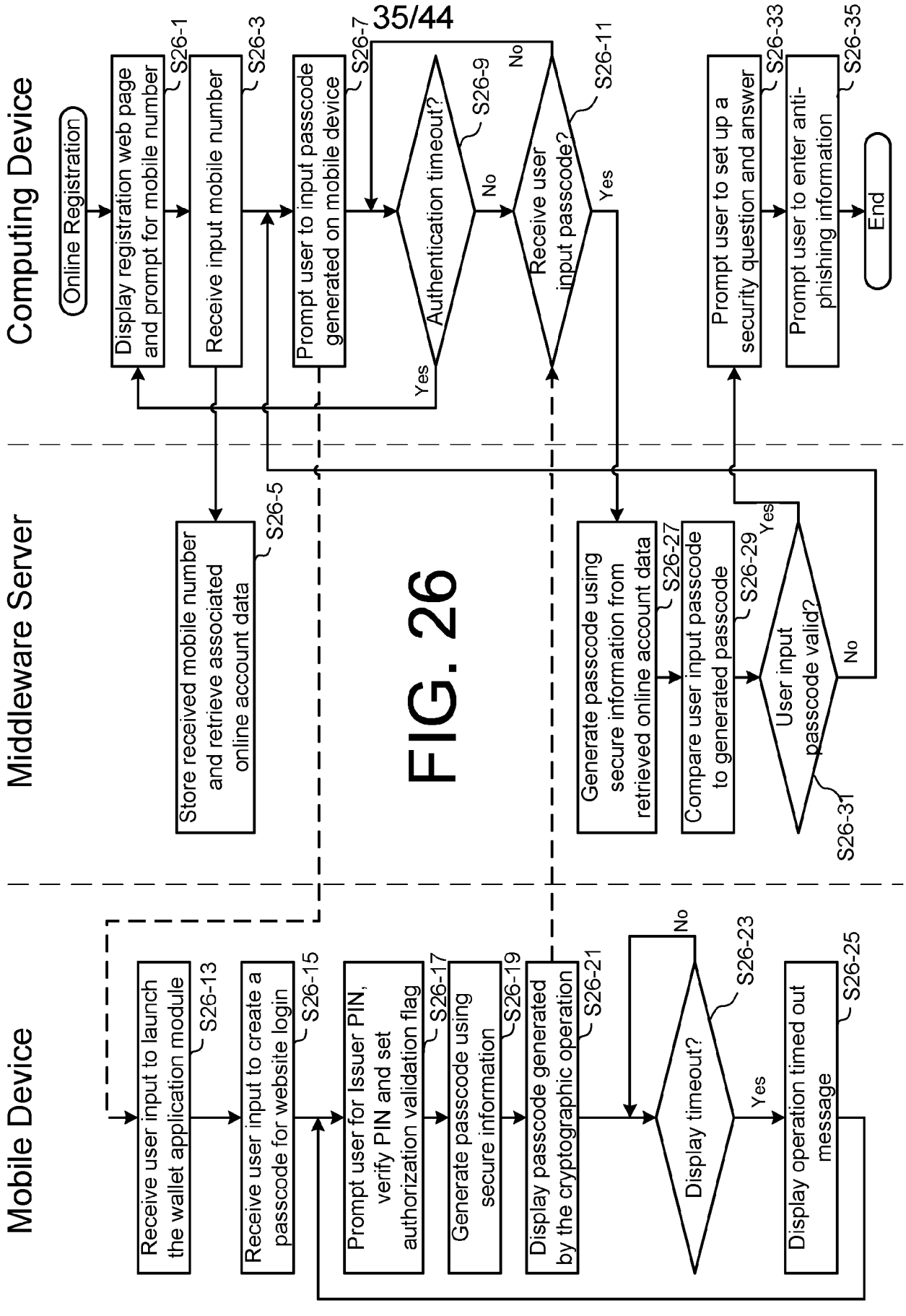
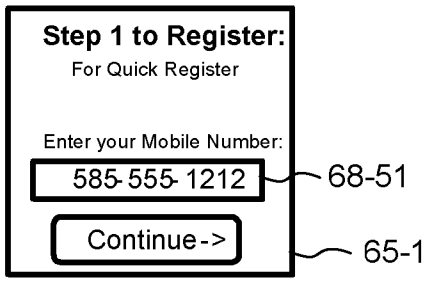
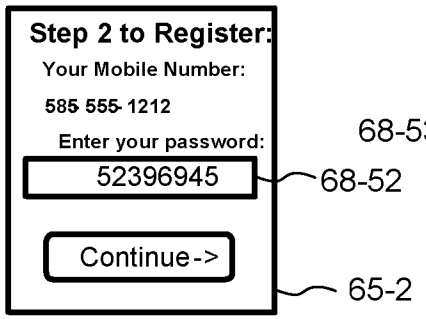
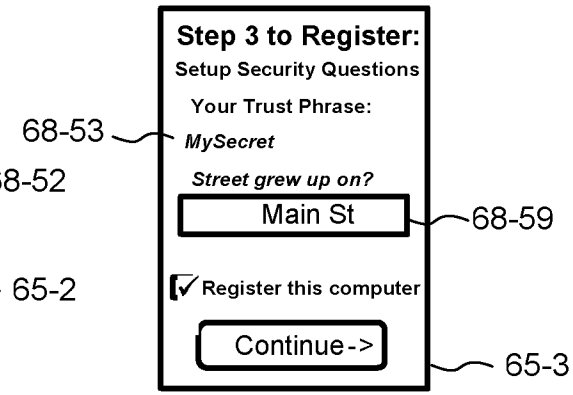

Computing Device
Middleware Server
Mobile Device
Online Registration
Display registration web page and prompt for mobile number
S26-1
Receive input mobile number
S26-3
Prompt user to input passcode generated on mobile device
S26-7
Authentication timeout?
S26-9
Yes
No
Receive user input passcode?
S26-11
No
Yes
Prompt user to set up a security question and answer
S26-33
Prompt user to enter anti-phishing information
S26-35
End
Store received mobile number and retrieve associated online account data
S26-5
Generate passcode using secure information from retrieved online account data
S26-27
Compare user input passcode to generated passcode
S26-29
User input passcode valid?
S26-31
Yes
No
Receive user input to launch the wallet application module
S26-13
Receive user input to create a passcode for website login
S26-15
Prompt user for Issuer PIN, verify PIN and set authorization validation flag
S26-17
Generate passcode using secure information
S26-19
Display passcode generated by the cryptographic operation
S26-21
Display timeout?
S26-23
No
Yes
Display operation timed out message
S26-25

FIG. 26







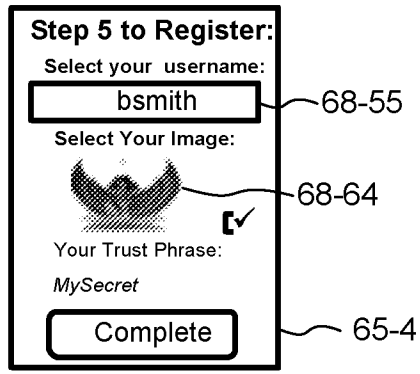
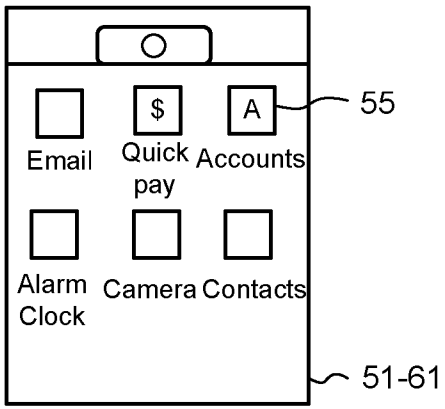
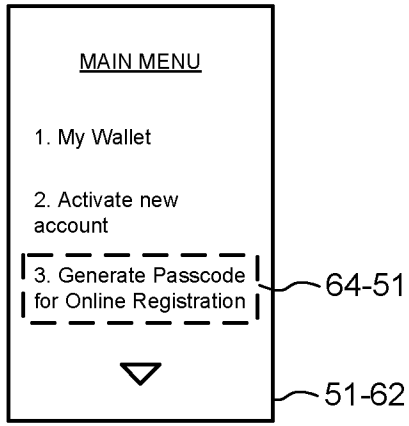
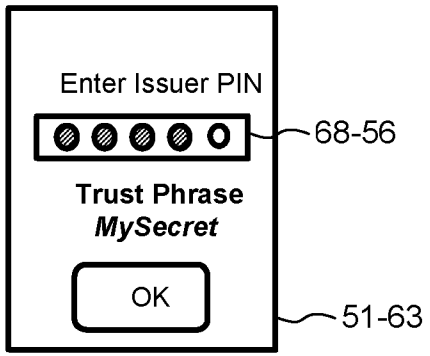


FIG. 27a FIG. 27b FIG. 27c FIG. 27d







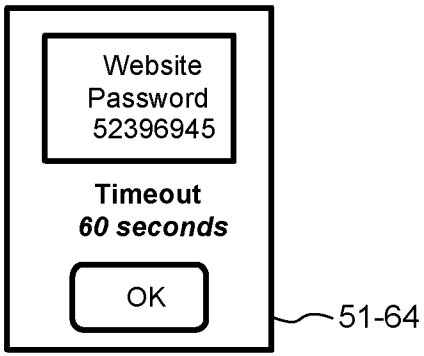


FIG. 28a FIG. 28b FIG. 28c FIG. 28d

FIG. 29a FIG. 29b FIG. 29c FIG. 29d

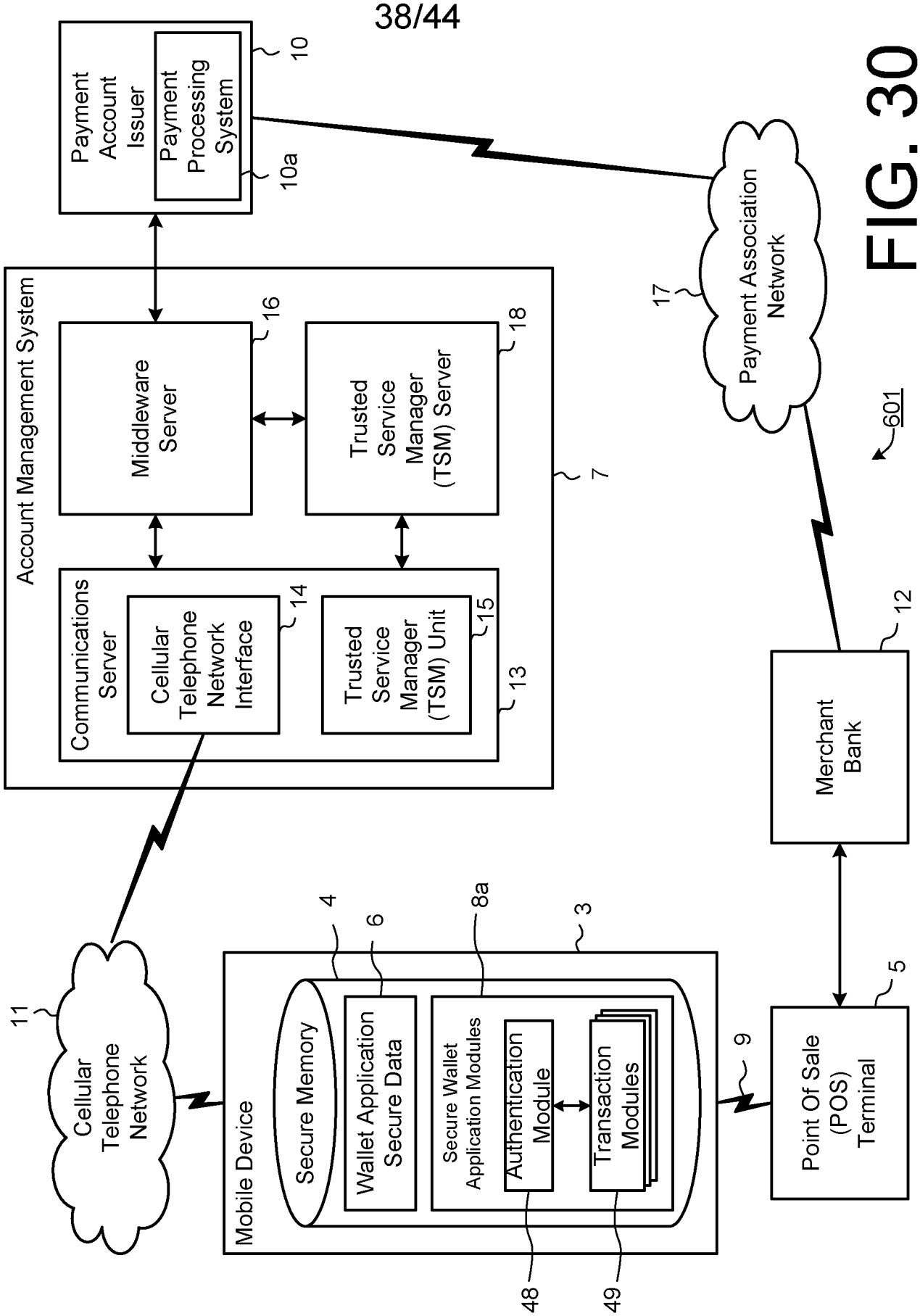

Payment Account Issuer
Payment Processing System
10
10a
Payment Association Network
17
601
Account Management System
Middleware Server
16
Trusted Service Manager (TSM) Server
18
7
Communications Server
Cellular Telephone Network Interface
14
Trusted Service Manager (TSM) Unit
15
13
Merchant Bank
12
Cellular Telephone Network
11
Mobile Device
4
6
8a
3
Secure Memory
Wallet Application Secure Data
Secure Wallet Application Modules
Authentication Module
Transaction Modules
48
49
9
Point Of Sale (POS) Terminal
5

FIG. 30

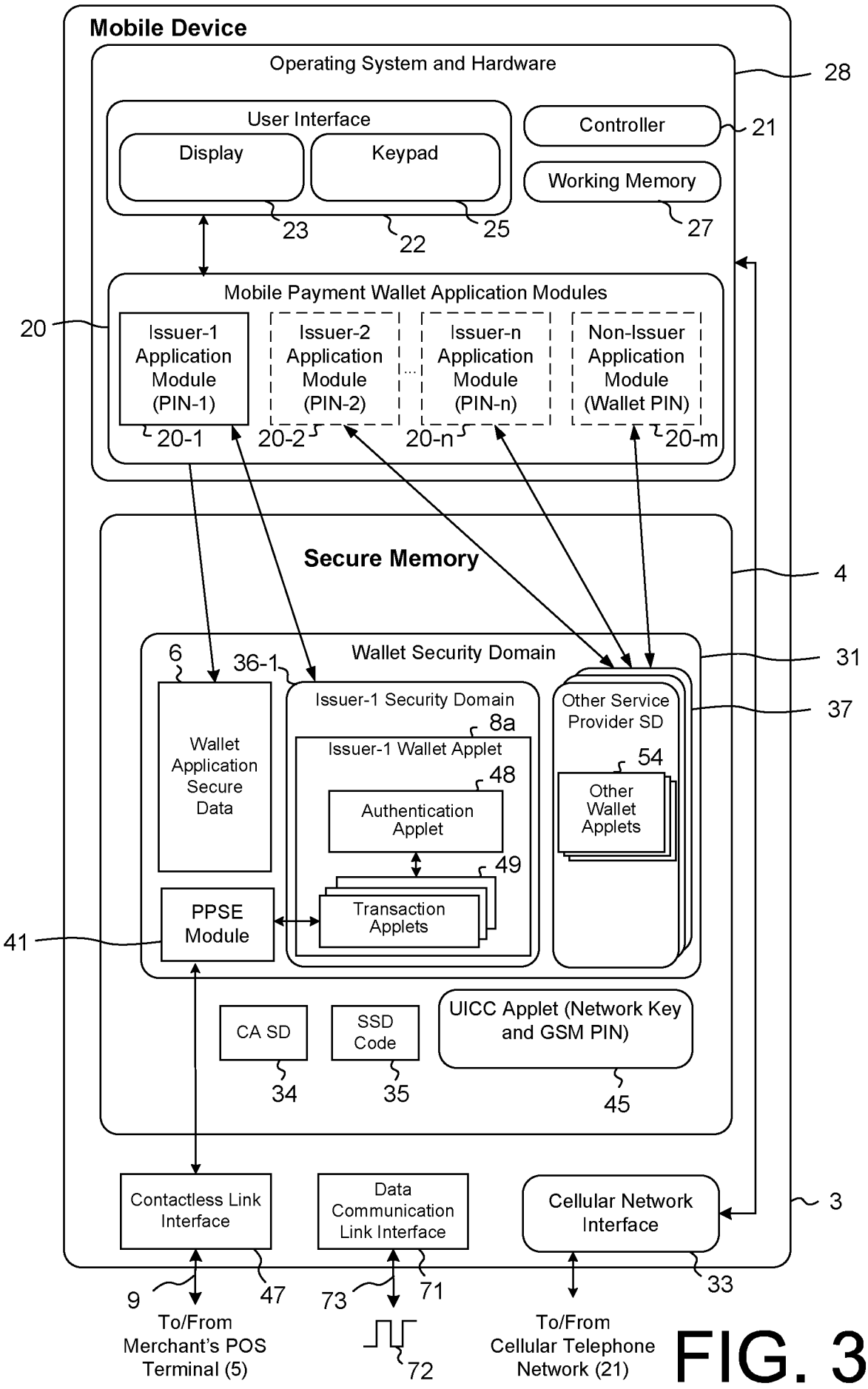

Mobile Device
Operating System and Hardware
28
User Interface
Display
Keypad
23
22
25
Controller
21
Working Memory
27
Mobile Payment Wallet Application Modules
20
Issuer-1 Application Module (PIN-1)
Issuer-2 Application Module (PIN-2)
Issuer-n Application Module (PIN-n)
Non-Issuer Application Module (Wallet PIN)
20-1
20-2
20-n
20-m
Secure Memory
4
6
36-1
Wallet Security Domain
31
Wallet Application Secure Data
Issuer-1 Security Domain
8a
Issuer-1 Wallet Applet
48
Authentication Applet
49
Transaction Applets
Other Service Provider SD
37
54
Other Wallet Applets
PPSE Module
41
CA SD
34
SSD Code
35
UICC Applet (Network Key and GSM PIN)
45
Contactless Link Interface
Data Communication Link Interface
Cellular Network Interface
3
9
47
73
71
33
To/From Merchant's POS Terminal (5)
72
To/From Cellular Telephone Network (21)

FIG. 31

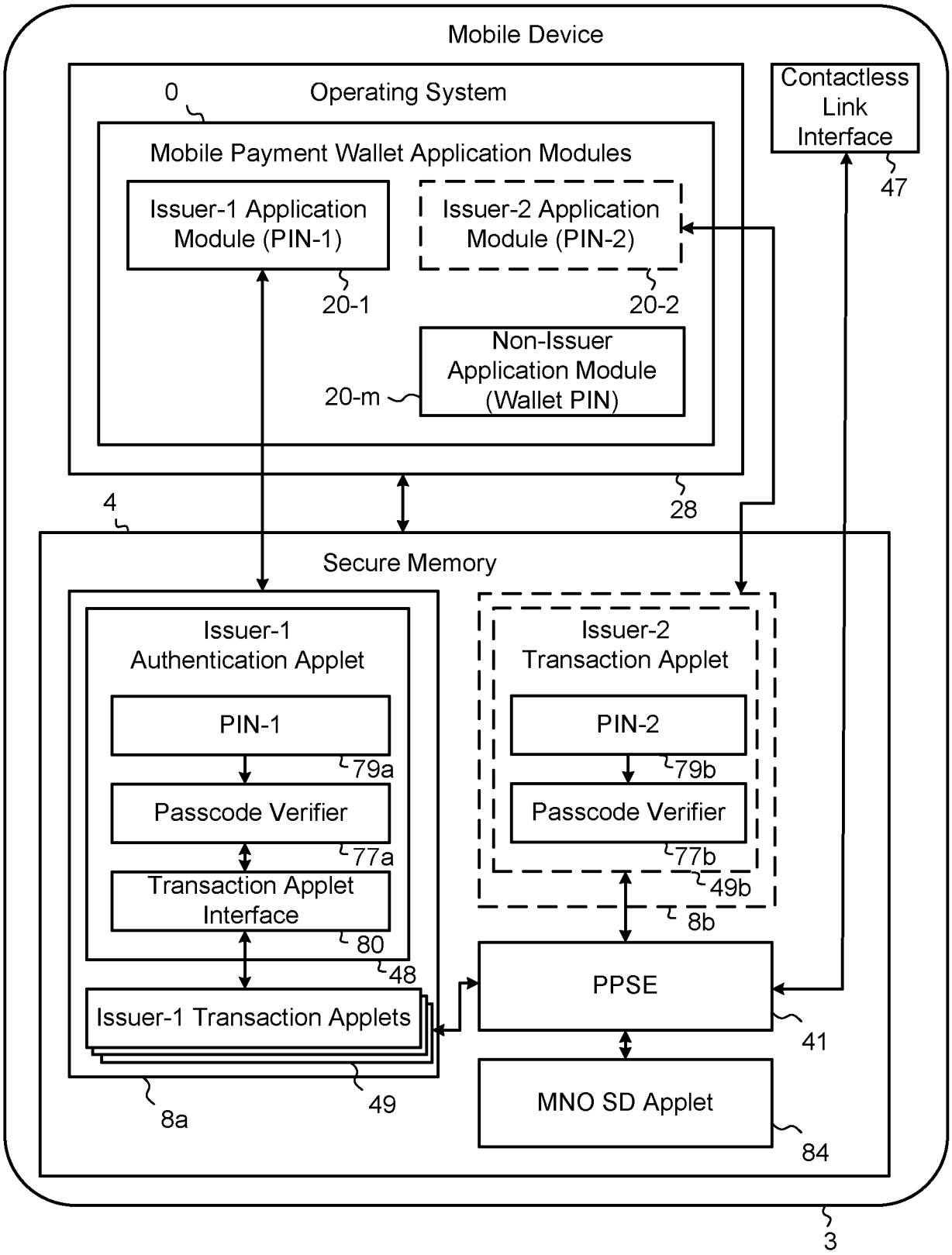

Mobile Device
0
Operating System
Mobile Payment Wallet Application Modules
Issuer-1 Application Module (PIN-1)
20-1
Issuer-2 Application Module (PIN-2)
20-2
Non-Issuer Application Module (Wallet PIN)
20-m
Contactless Link Interface
47
28
4
Secure Memory
Issuer-1 Authentication Applet
PIN-1
79a
Passcode Verifier
77a
Transaction Applet Interface
80
48
Issuer-1 Transaction Applets
8a
49
Issuer-2 Transaction Applet
PIN-2
79b
Passcode Verifier
77b
49b
8b
PPSE
41
MNO SD Applet
84
3

FIG. 32

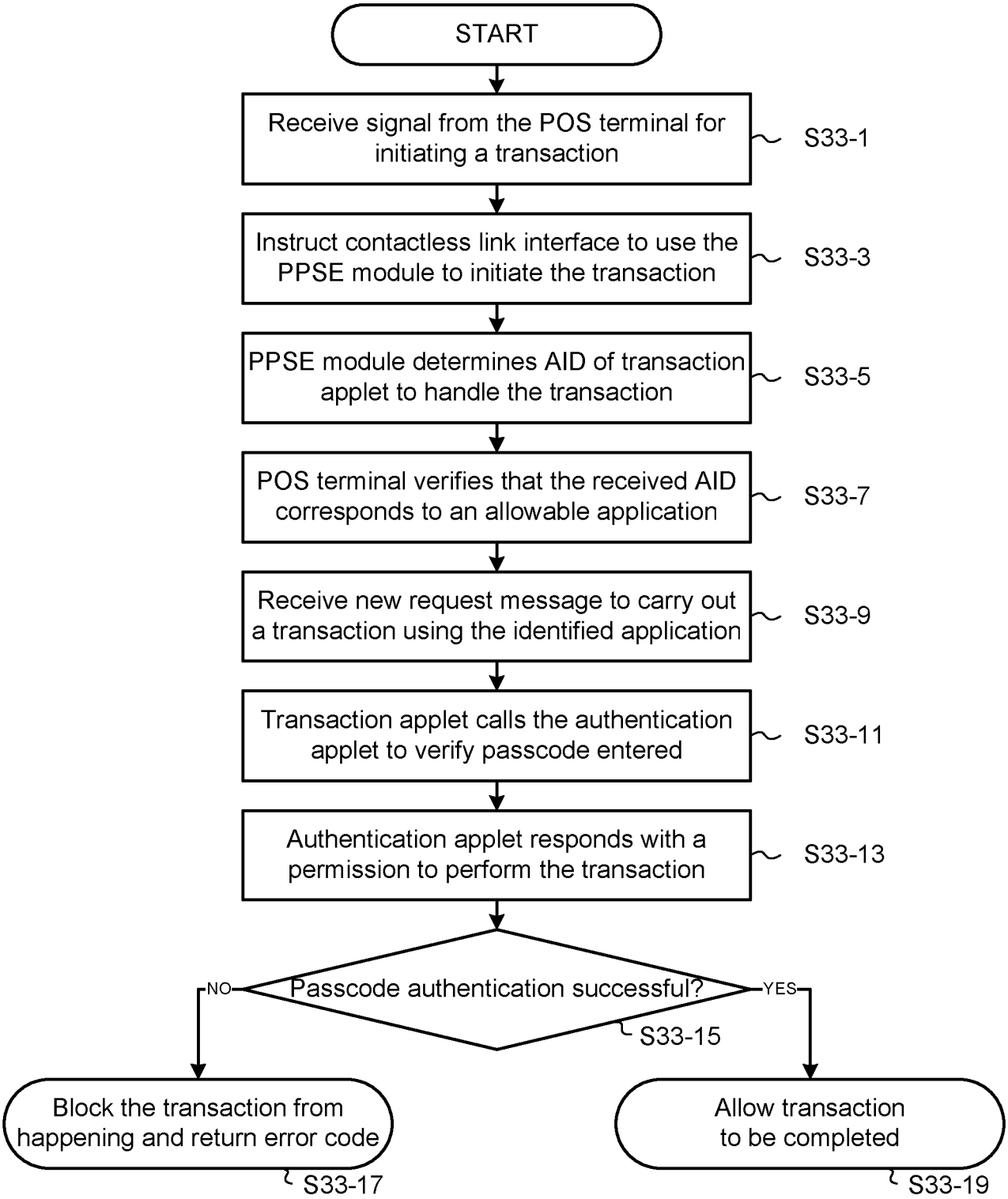

START
Receive signal from the POS terminal for initiating a transaction
S33-1
Instruct contactless link interface to use the PPSE module to initiate the transaction
S33-3
PPSE module determines AID of transaction applet to handle the transaction
S33-5
POS terminal verifies that the received AID corresponds to an allowable application
S33-7
Receive new request message to carry out a transaction using the identified application
S33-9
Transaction applet calls the authentication applet to verify passcode entered
S33-11
Authentication applet responds with a permission to perform the transaction
S33-13
Passcode authentication successful?
S33-15
NO
YES
Block the transaction from happening and return error code
S33-17
Allow transaction to be completed
S33-19

FIG. 33

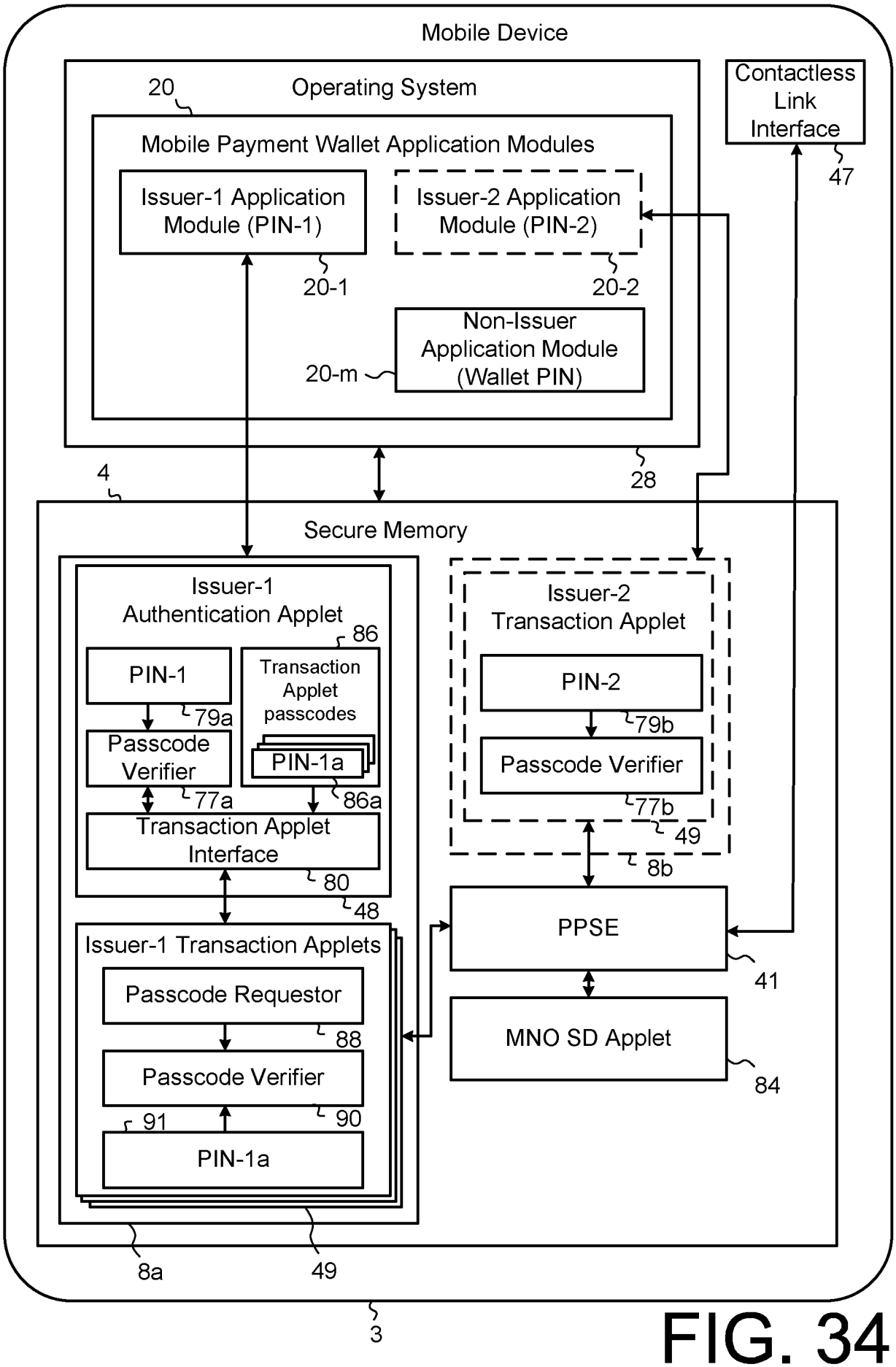

Mobile Device
20
Operating System
Mobile Payment Wallet Application Modules
Issuer-1 Application Module (PIN-1)
20-1
Issuer-2 Application Module (PIN-2)
20-2
Non-Issuer Application Module (Wallet PIN)
20-m
Contactless Link Interface
47
4
28
Secure Memory
Issuer-1 Authentication Applet
86
PIN-1
79a
Passcode Verifier
77a
Transaction Applet passcodes
PIN-1a
86a
Transaction Applet Interface
80
48
Issuer-1 Transaction Applets
Passcode Requestor
88
Passcode Verifier
91
90
PIN-1a
Issuer-2 Transaction Applet
PIN-2
79b
Passcode Verifier
77b
49
8b
PPSE
41
MNO SD Applet
84
8a
49
3

FIG. 34

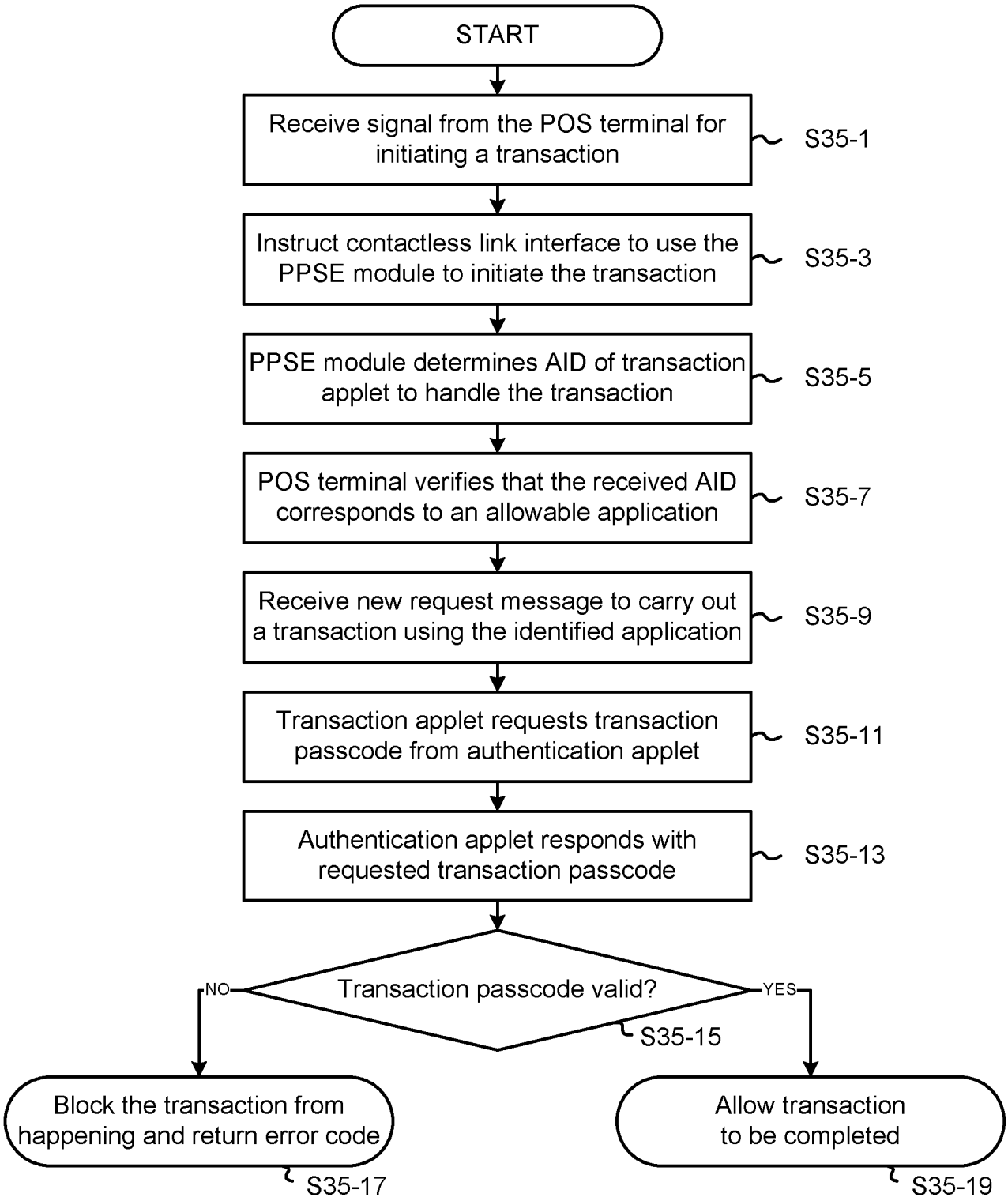

START
Receive signal from the POS terminal for initiating a transaction
S35-1
Instruct contactless link interface to use the PPSE module to initiate the transaction
S35-3
PPSE module determines AID of transaction applet to handle the transaction
S35-5
POS terminal verifies that the received AID corresponds to an allowable application
S35-7
Receive new request message to carry out a transaction using the identified application
S35-9
Transaction applet requests transaction passcode from authentication applet
S35-11
Authentication applet responds with requested transaction passcode
S35-13
Transaction passcode valid?
S35-15
NO
YES
Block the transaction from happening and return error code
S35-17
Allow transaction to be completed
S35-19

FIG. 35

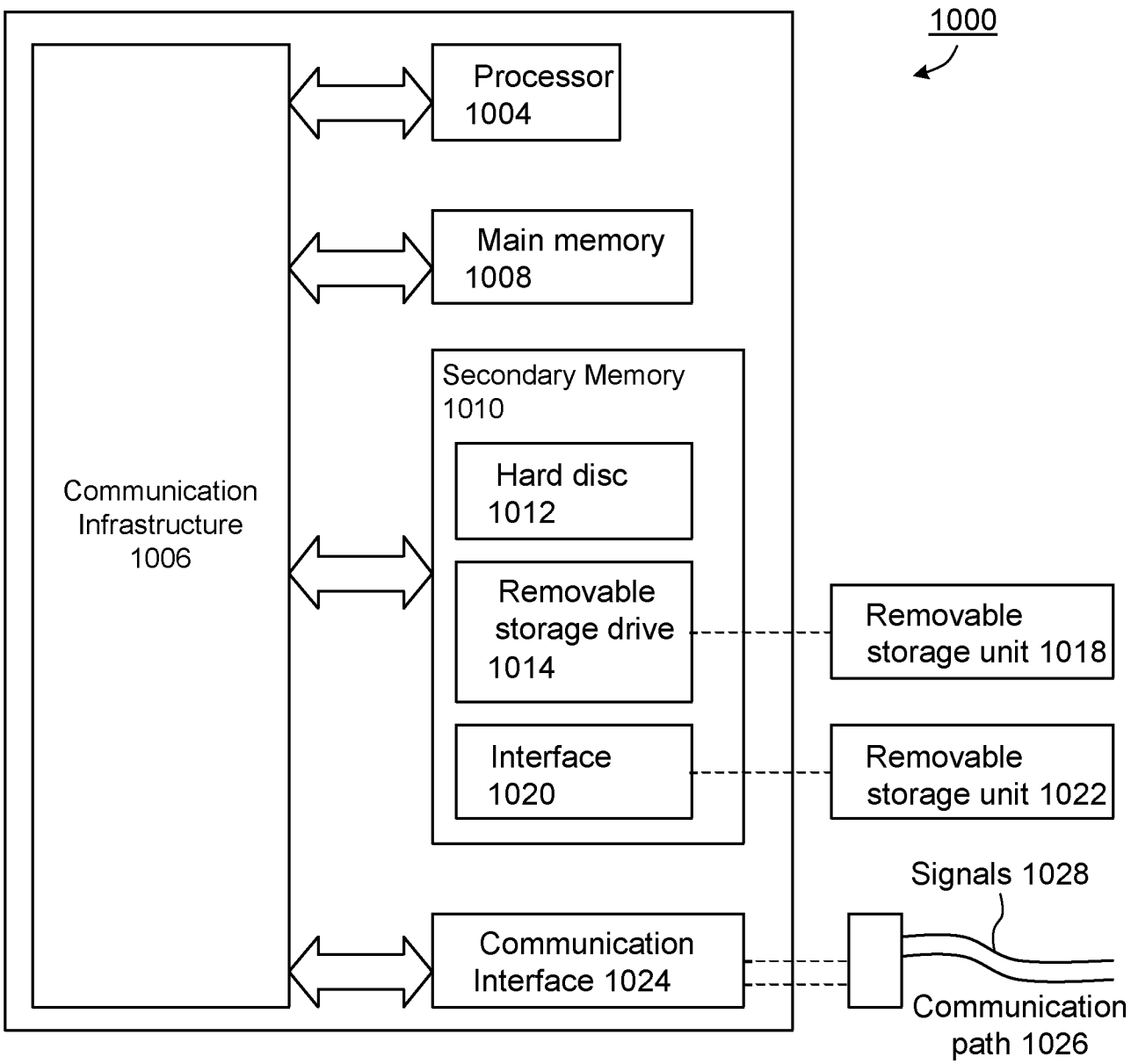

1000
Processor 1004
Main memory 1008
Secondary Memory 1010
Hard disc 1012
Removable storage drive 1014
Interface 1020
Communication Infrastructure 1006
Removable storage unit 1018
Removable storage unit 1022
Signals 1028
Communication Interface 1024
Communication path 1026

FIG. 36

INTERNATIONAL SEARCH REPORT

International application No
PCT/GB2011/051839

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06Q20/00
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 2010/051339 A2 (VISA INT SERVICE ASS [US]; DOMINGUEZ BEN [US]; FISHER DOUGLAS [US]; CH) 6 May 2010 (2010-05-06) the whole document	1-135
X	WO 2007/136277 A1 (FRONDE ANYWHERE LTD [NZ]; PARFENE HORATIU NICOLAE [NZ]; WILLIAMS ANTON) 29 November 2007 (2007-11-29) abstract	1-135
X	US 2009/234751 A1 (CHAN ERIC [CA] ET AL) 17 September 2009 (2009-09-17) abstract	1-135
X	US 2006/200427 A1 (MORRISON ROBERT A [US] ET AL) 7 September 2006 (2006-09-07) abstract the whole document	1-135

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
4 January 2012	12/01/2012

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Verhoef, Peter

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/GB2011/051839

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2010051339 A2	06-05-2010	US 2010114740 A1	06-05-2010
		WO 2010051339 A2	06-05-2010
WO 2007136277 A1	29-11-2007	AU 2007252340 A1	29-11-2007
		CA 2649711 A1	29-11-2007
		CN 101438530 A	20-05-2009
		EP 2018733 A1	28-01-2009
		JP 2009537893 A	29-10-2009
		KR 20090031672 A	27-03-2009
		NZ 547322 A	28-03-2008
		US 2009228966 A1	10-09-2009
		WO 2007136277 A1	29-11-2007
		ZA 200704044 A	29-04-2009
US 2009234751 A1	17-09-2009	CA 2718514 A1	17-09-2009
		EP 2263201 A1	22-12-2010
		US 2009234751 A1	17-09-2009
		WO 2009111856 A1	17-09-2009
US 2006200427 A1	07-09-2006	NONE	