



- (51) International Patent Classification:
G06Q 20/36 (2012.01) *H04L 9/32* (2006.01)
G06Q 30/06 (2012.01)
- (21) International Application Number:
PCT/US2015/063315
- (22) International Filing Date:
2 December 2015 (02.12.2015)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:
14/588,335 31 December 2014 (31.12.2014) US
- (63) Related by continuation (CON) or continuation-in-part (CIP) to earlier application:
US 14/588,335 (CON)
Filed on 31 December 2014 (31.12.2014)
- (71) Applicant: PAYPAL, INC. [US/US]; 2211 North First Street, San Jose, California 95131 (US).
- (72) Inventor: MERCILLE, Richard; c/o PAYPAL, INC., 2211 North First Street, San Jose, California 95131 (US).
- (74) Agent: MENCHER, Joseph R.; Haynes And Boone, LLP, 2323 Victory Avenue, Suite 700, Dallas, Texas 75219 (US).
- (81) Designated States (*unless otherwise indicated, for every kind of national protection available*): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, 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, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU,

[Continued on next page]

(54) Title: AUTHENTICATION OF MOBILE DEVICE FOR SECURE TRANSACTION

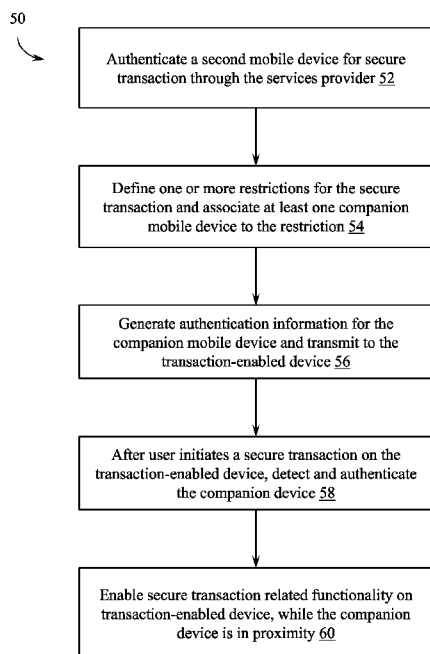


FIG. 1

(57) Abstract: There are provided systems and methods for authenticating a mobile device for use in a secure transaction. A user having a master device authenticated for use in a secure transaction system, such as an electronic payment system, identifies a secondary device to be enabled for use in processing a secure transaction. The secondary device connects to a companion device and shares information associated with the secondary device and companion device with a transaction processing server, which returns authentication information associated with both devices. When the user initiates a secure transaction, the secondary device identifies whether the third device is in proximity. The secure transaction is processed only if the second and third devices are in communication and authenticated during the transaction. If the secondary device is lost or stolen, the device may be disabled until reauthenticated through the master device.



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, KM, ML, MR, NE, SN, TD, TG).

Published:

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

AUTHENTICATION OF MOBILE DEVICE FOR SECURE TRANSACTION

Richard Mercille

CROSS-REFERENCE TO RELATED APPLICATION

[0001] This application is a continuation of and claims priority to U.S. Patent Application No. 14/588,335 filed December 31, 2014, which is incorporated herein by reference in its entirety.

TECHNICAL FIELD

[0002] The present application relates generally to mobile devices and more specifically to systems and methods for authenticating a mobile device for use in a secure transaction.

BACKGROUND

[0003] Mobile devices such as smart phones and smart watches are enjoying widespread popularity. Some of these devices store sensitive personal information and enable functions that could be harmful to the user if the device was stolen, lost or otherwise accessed by an unauthorized user. For example, a smartphone may store the user's online passwords and credit card information used for online purchases. A smartphone may also be used in place of a credit card to make an electronic payment at a merchant through a digital wallet or electronic payment service. Many devices used for secure transactions include specialized hardware known as "secure elements" to protect the confidential payment information. A secure element may be a tamper resistant card or chip that provides for secure storage of sensitive information and is commonly used in devices to secure electronic payment transactions. With the widespread adoption of specialized mobile devices, including wearable technology such as smart watches, fitness trackers and clothing that monitor fitness activity, it is not always necessary or desirable for a user to carry a smartphone. For example, a user may own a variety of mobile devices and desire the convenience and efficiency of wearable electronic technology for certain applications without sacrificing security.

BRIEF DESCRIPTION OF THE DRAWINGS

[0004] FIG. 1 is a flow chart illustrating an embodiment of an exemplary secure transaction process;

[0005] FIG. 2 is an embodiment of an exemplary network system suitable for processing a secure transaction;

[0006] FIG. 3 is an embodiment of an exemplary network system suitable for processing a secure transaction;

[0007] FIGs. 4a-b are flow charts illustrating an embodiment of an exemplary device authentication process;

[0008] FIG. 5 is a flow chart illustrating an embodiment of an exemplary electronic payment process;

[0009] FIG. 6 is an embodiment of an exemplary computer system suitable for implementing one or more components in FIGs. 2 and 3; and

[00010] FIGs. 7a-b are exemplary data structures illustrating embodiments of information stored at the transaction-enabled device and transaction processing server, respectively.

[00011] Embodiments of the present disclosure and their advantages are best understood by referring to the detailed description that follows. It should be appreciated that like reference numerals are used to identify like elements illustrated in one or more of the figures, wherein showings therein are for purposes of illustrating embodiments of the present disclosure and not for purposes of limiting the same.

DETAILED DESCRIPTION

[00012] Provided are methods for authenticating a mobile device for secure transactions, such as an electronic payment transaction. Systems suitable for practicing methods of the present disclosure are also provided.

[00013] In various embodiments, a master device, such as a smartphone, is adapted to engage in a secure transaction, such as making an electronic payment at a merchant point of sale terminal. The user of the master device may delegate the authority to enter into the secure transaction to a second mobile device, such as a smart watch. The user may also establish a trust association between the second device and a third mobile device, such as clothing with wearable technology. As used herein, the second device may be referred to as “transaction-enabled device” and the third trusted device may be referred to as a “companion device.”

[00014] When the user of the transaction-enabled device initiates a secure transaction, the device verifies that a companion device is in communication with the transaction-enabled device. Access to the secure transaction is allowed only if, and while, the companion device

is in communication with the transaction-enabled device. If the companion device is not detected, access to the secured transaction on the transaction-enabled device may be either denied or restricted. In one embodiment, an attempt to access the secure function without the companion device (for example, if the transaction-enabled device is lost or stolen), may result in the secured function being disabled and/or confidential information being purged from the transaction-enabled device. The secure transaction can then be restored on the device by reauthenticating the device through the master device. In various embodiments, the user may allow restricted use of the secure transaction when the companion device is absent, for example, by establishing a spending limited (\$20 per transaction), or setting geographic or other restrictions.

[00015] FIG 1 is a flow chart 50 illustrating an embodiment of an exemplary secure transaction process. A user operates a master device (e.g., a smart phone), which is authenticated for secure transactions through a service provider. In this embodiment, the user accesses a corresponding account managed by the service provider and identifies a second mobile device (e.g., a smart watch) to which the user desires to delegate authority for the secure transaction. In step, 52, the user authenticates the second mobile device for secure transactions through the service provider. In various embodiments, authentication may include user and device authentication. User authentication may include a username and password combination, biometric authentication (e.g., fingerprint scan) or other user authentication as available through the second device. Device authentication may include a unique device identifier, shared encryption keys, a unique token and other authentication techniques and protocols. The service provider generates unique authentication information for the second device, which is transmitted to and stored on the transaction-enabled device. In one embodiment, the second device is adapted to facilitate an electronic payment and receives a payment token from the master device which is associated with the master account and second device. In various embodiments, one or more tokens may be used, and the tokens may be single use or multi-use. The tokens may be generated and transmitted to the second device by the master device, the service provider or a third party token service. In various embodiments, the service provider may communicate with the transaction-enabled device or communicate with the master device, which forwards the authentication information to the transaction-enabled device.

[00016] In step 54, the user defines one or more restrictions on the use of and/or access to the secure transaction on the transaction-enabled device and associates at least one

companion device to the restriction. In one embodiment, the user associates a companion device which must be in proximity to the transaction-enabled device to enable the secure transaction. The service provider generates authentication information for the companion device and transfers the information to the transaction-enabled device in step 56. In various embodiments, the restrictions may include denying access to the secure transaction unless the companion device is in proximity to the transaction-enabled device, limiting access to certain secured features or restricting secure transaction parameters. For example, if the transaction-enabled device is a fitness watch that the user wears while jogging, the secure transaction features may be limited to allow the user to make a purchase up to a limited amount (e.g., \$20) within a certain geographic area associated with the activity.

[00017] In step 58, the user initiates a secure transaction through the transaction-enabled device, searches for the companion device and attempts to authenticate the companion device if found. In one embodiment, the secure transaction is disabled unless the transaction-enabled device locates and authenticates a companion device. The transaction-enabled device may search for a companion device using a short range wireless protocol (e.g., Bluetooth) and if communication is established with the companion device, the transaction-enabled device initiates an authentication protocol with the companion device. Through the authentication protocol, the companion device transmits authentication information to the transaction-enabled device which is then verified by the transaction-enabled device. If the companion device is authenticated, the secure transaction is enabled in step 60, and the user will have access to the secure transaction for as long as the companion device remains in communication with the transaction-enabled device.

[00018] In one embodiment, the secure transaction is an electronic purchase from a merchant and the transaction-enabled device prepares and transmits encrypted transaction data, a payment token and a digital signature to a merchant's point-of-sale terminal, which forwards the information to the service provider for processing. The encrypted transaction information and digital signature may include a timestamp and unique devices identifiers for each of the transaction-enabled device and companion device.

[00019] Referring to FIG. 2, an exemplary embodiment of a network system 100 suitable for implementing the processes described herein is illustrated. As shown, system 100 may comprise or implement a plurality of devices, servers, and/or software components that operate to perform various methodologies in accordance with the described embodiments. Exemplary devices and servers may include device, stand-alone, and enterprise-class servers,

operating an OS such as a MICROSOFT® OS, a UNIX® OS, a LINUX® OS, or other suitable device and/or server based OS. It can be appreciated that the devices and/or servers illustrated in FIG. 2 may be deployed in other ways and that the operations performed and/or the services provided by such devices and/or servers may be combined or separated for a given embodiment and may be performed by a greater number or fewer number of devices and/or servers. One or more devices and/or servers may be operated and/or maintained by the same or different entities.

[00020] System 100 comprises a user 102, a master device 110, a transaction-enabled device 160, a companion device 170 and a transaction processing server 130 in communication over a network 150. Master device 110, transaction processing server 130, transaction-enabled device 160 and companion device 170 may each include one or more processors, memories, and other appropriate components for executing instructions such as program code and/or data stored on one or more computer readable mediums to implement the various applications, data, and steps described herein. For example, such instructions may be stored in one or more computer readable media such as memories or data storage devices internal and/or external to various components of system 100, and/or accessible over network 150.

[00021] Master device 110 may be implemented using any appropriate hardware and software configured for wired and/or wireless communication with transaction processing server 130 and transaction-enabled device 160. In various embodiments, master device 110 may be implemented as a smart phone, tablet, laptop computer, wristwatch with appropriate computer hardware resources, eyeglasses with appropriate computer hardware, clothing with wearable technology with appropriate computer hardware, and/or other types of computing devices capable of transmitting and/or receiving data as described herein. Although a single master device is shown, the master device may be managed or controlled by any suitable processing device, and may include a plurality of devices that function similarly. Moreover, in various embodiments, one or more of the applications, processes, and/or features discussed below in reference to master device 110 may be included in a communication device connected to master device 110.

[00022] Master device 110 of FIG. 2 comprises a secure transaction module 114 and a communication module 116. In other embodiments, master device 110 may include additional or different modules having specialized hardware and/or software as required. Secure transaction module 114 comprises one or more hardware and software processes to

facilitate a secure transaction through the transaction processing server 130. In one embodiment, the secure transaction module 114 facilitates an electronic payment and includes corresponding hardware and software which may comprise secure storage for maintaining data for authenticating the master device 110 to the transaction processing server 130.

[00023] The secure transaction module 114 comprises an administration module 120 and a secure element 122. The administration module 120 provides the user 102 with an interface to manage transactions, interface with the transaction processing server 130 and administer the delegation of secure transactions to other devices as described herein. Through the administration module 120, the user 102 sets, accesses, and/or determines appropriate restrictions for entering into secure transactions through the transaction-enabled device 160.

[00024] The communications module 116 is adapted to communicate with the service provider server 130 over the network 150 and transaction-enabled device 160. In one embodiment, the communications module 116 is further adapted to communicate with merchant point-of-sale devices to facilitate an electronic transaction. In various embodiments, communications module 118 may include a DSL (e.g., Digital Subscriber Line) modem, a PSTN (Public Switched Telephone Network) modem, an Ethernet device, a broadband device, a satellite device and/or various other types of wired and/or wireless network communication devices including microwave, radio frequency, infrared, Bluetooth, and near field communication devices. Communications module 116 may communicate directly with the transaction-enabled device 160 using short range wireless communications, such as Bluetooth Low Energy, LTE Direct, radio frequency, infrared, Bluetooth, and near field communications.

[00025] Transaction-enabled device 160 may be implemented using any appropriate hardware and software and includes a communications module 168 configured for wired and/or wireless communication with master device 110, companion device 170 and transaction processing server 130. In various embodiments, transaction-enabled device 160 may be implemented as a smart phone, tablet, laptop computer, wristwatch with appropriate computer hardware resources, eyeglasses with appropriate computer hardware, clothing with wearable technology with appropriate computer hardware, and/or other types of computing devices capable of transmitting and/or receiving data as described herein. Although only one transaction-enabled device 160 is shown, a plurality of primary devices 160 may be implemented within the spirit of this embodiment. Moreover, in various embodiments, one or

more of the applications, processes, and/or features discussed below in reference to transaction-enabled device 160 may be included in a communication device connected to transaction-enabled device 160.

[00026] The transaction-enabled device 160 also comprises a secure transaction module 162 which is adapted to facilitate a secure transaction with the transaction processing server 130, and may correspond to specialized hardware and/or software utilized by transaction-enabled device 160. The secure transaction module 162 comprises a companion detection module 164 and a secure element 166. When user 102 initiates a secure transaction using the secure transaction module 162, the companion detection module 166 attempts to pair with a companion device 170. If the companion detection module 166 detects a companion device 170, the transaction proceeds and transaction information, unique device information received from the companion device 170, unique device information of the transaction-enabled device 160 and encryption parameters received from transaction processing server 130 are used to create a transaction message for delivery to transaction processing server 130. In one embodiment, the transaction-enabled device 160 provides the transaction message to a point-of-sale terminal and the transaction message is forwarded to the transaction processing server 130 by a corresponding merchant. In another embodiment, the transaction message is forwarded to transaction processing server 130 over the network 150. The transaction processing server 130 deconstructs the transaction message to authenticate the user 102, transaction-enabled device 160 and companion device 170 to authorize the transaction.

[00027] If the companion detection module 166 loses connection with the companion device 170, then the secure transaction module 162 will be disabled from further processing of the secure transaction until another companion device is detected and authenticated. In one embodiment, secure element 166 is a tamper resistant secure storage for storing one or more tokens and other authentication data to authenticate the transaction-enabled device to the service provider 130. In other embodiments, secure element 166 can be any suitable storage element, with different levels or types of security, including a non-secure storage element. In various embodiments, one or more features of the transaction-enabled device 160 may be combined so as to provide their respective features in one module.

[00028] In one embodiment, companion detection module 164 authenticates the identity of the user 102 by detecting and connecting with a companion device 170 associated with user 102 and receiving additional identification information and authentication information from the companion device 170. The companion device 170 comprises an identification element

172 and a communications module 174. The connection between the transaction-enabled device 160 and the companion device 170 may utilize short range wireless communications. For example, companion detection module 164 may pair with the companion device 170 and request a unique device identifier of secondary device 170. The identification element 172 transmits a universally unique identifier associated with the companion device 170 to the primary device 160. In various embodiments, the identification element 172 may include an RFID, a code stored in a volatile memory, a hardware device identifier and a secure element.

[00029] The companion detection module 164 may transmit the request to establish the connection with companion device 170 as a short range wireless communication (e.g. a BLE protocol communication) including a “wake up” process for the companion device 170. In other embodiments, the request and/or connection may utilize near field communication, radio communication, infrared communication, or Bluetooth communication. Additionally, although transaction-enabled device 160 may utilize BLE protocol communications to effectuate an “always on” type service where the unique device identifier and “wake up” process are transmitted continuously by transaction-enabled device 160 during the secure transaction, other communication protocols used to provide an “always on” service may include LTE Direct or similar device-to-device communication technology. BLE and LTE Direct may both be utilized to provide discovery of nearby devices to transaction-enabled device 160.

[00030] In various embodiments, secure transaction module 162 also requests a log in or other identifier from user 102 that authenticates user 102. In such embodiments, user 102 may provide an identifier, user account name, password, and/or PIN directly to transaction-enabled device 160 or companion device 170. User 102 may also be identified using biometrics and biometric reading devices such as a fingerprint scanner or eye/retinal scanner. The identification information may be entered to either device using an interactive touch screen, a keyboard, a mouse, a biometric reader, or other input device available on either transaction-enabled device 160 or companion device 170. The user 102 authentication information may be stored in the secure element 166 or transaction processing server 130 as appropriate for authenticating the identity of user 102.

[00031] In various embodiments, the master device 110, transaction-enabled device 160 and companion device 170 may include other applications and features as may be desired to provide features to user 102. For example, the devices may include security applications for implementing client-side security features, programmatic client applications for interfacing

with appropriate application programming interfaces (APIs) over network 150, games, fitness tracking applications, email, texting, voice and IM applications, and other application and features. The communications modules 116, 168 and 174 may also correspond to mobile, satellite, wireless Internet, and/or radio communication applications. The applications may further include payment applications and/or services, for example, applications/services that may provide payments, purchases made by a user of the device (e.g., user 102 and/or a person/entity exerting control over the device), and/or other payments during use of the device, or GPS applications configured to display location information to user 102. The devices may also include financial applications, such as banking, online payments, money transfer, or other financial applications, software programs, executable by a processor, including a graphical user interface (GUI) configured to provide an interface for user 102. Any application can be implemented in a secure transaction module described herein to provide restrictions and authentication as described herein.

[00032] The transaction processing server 130 may be maintained, for example, by a service provider offering the secure transaction services, and is accessed by the user to administer user accounts, to authenticate devices and enable secure transactions. For example, transaction processing server 130 may correspond to or be associated with an electronic payment service. In this regard, transaction processing server 130 includes one or more processing applications which may be configured to interact with master device 110, transaction-enabled device 160 and a merchant 180 to authorize devices and communications for a secure transaction. Although only one server is shown, a plurality of servers and/or associated devices may function similarly.

[00033] Transaction processing server 130 includes a secure transaction module 132, an authentication module 134, a restrictions module 136, a network interface 138 and a database 140. In other embodiments, the transaction processing server 130 may include additional or different modules having specialized hardware and/or software as required.

[00034] The transaction processing server 130 may be controlled by a service provider which provides a service over the network 150 associated with the secure transaction modules 114 and 162. For example, the transaction processing server 130 may correspond to a payment service provider, a merchant, a transportation service provider, a media provider, or other type of service provider. In this regard, transaction processing server 130 includes one or more servers incorporating one or more processing applications which may be configured to interact with master device 110, transaction-enabled device 160 and/or

merchant 180. In one example, transaction processing server 130 may be provided by PAYPAL®, Inc. of San Jose, CA, USA. Although only one server is shown, a plurality of servers and/or associated devices may function similarly. Other applications may also be included that correspond to processes, procedures, and/or applications, for example, a software program, executable by a hardware processor. In other embodiments, transaction processing server 130 may include additional or different modules having specialized hardware and/or software as required.

[00035] Secure transaction module 132 may correspond to one or more processes and associated devices to process some action taken with regard to use of the secure transaction module 114 or 162. Secure transaction module 132 may correspond to specialized hardware and/or software utilized by transaction processing server 130 to receive a request to process an action by user 102 when user 102 is utilizing the secure transaction module 162 of transaction-enabled device 160. For example, an action processed by secure transaction module 132 may correspond to a payment to the merchant 180.

[00036] Secure transaction module 132 may also enforce authentication and restriction requirements on the use and performance of the transaction-enabled device 160. Thus, if the action is received from transaction-enabled device 160 by secure transaction module 132, secure transaction module 132 may authenticate the user and device using the authentication module 134 or determine if a restriction is placed on the action via restriction module 136 prior to processing the transaction. Secure transaction module 142 may then proceed with the requested transaction if the authentication and restriction requirements are satisfied. The transaction processing server 130 may include other applications as desired to provide additional services and features to user 102, such as security applications for implementing server-side security features, programmatic server applications for interfacing with appropriate application programming interfaces (APIs) over network 150, or software programs, executable by a processor, including a graphical user interface (GUI), configured to provide an interface to a user.

[00037] Additionally, transaction processing server 130 includes database 140 storing user accounts and related transaction and configuration information, including the transaction-enabled devices, companion devices, restrictions and authentication information. User accounts in database 140 may include user information, such as name, address, birthdate, payment/funding information, additional user financial information, and/or other desired user data. Account holders may link to their respective accounts through a user, device identifier

and other authentication information. For example, when a device identifier is transmitted to transaction processing server 130, e.g. from transaction-enabled device 160, an account may be found. Database 140 may store received information, such as actions for processing, and user identification information.

[00038] In various embodiments, transaction processing server 140 includes at least one network interface 138 adapted to communicate with master device 110, transaction-enabled device 160 and/or merchant 180 over network 150. In various embodiments, network interface component 148 may comprise a DSL (e.g., Digital Subscriber Line) modem, a PSTN (Public Switched Telephone Network) modem, an Ethernet device, a broadband device, a satellite device and/or various other types of wired and/or wireless network communication devices including microwave, radio frequency (RF), and infrared (IR) communication devices.

[00039] Restrictions module 132 may correspond to one or more processes to execute modules and associated devices of transaction processing server 130 to set, manage, and/or access/determine restrictions. In this regard, restrictions module 132 may correspond to specialized hardware and/or software utilized by transaction processing server 130 with master device 110 to set and/or manage restrictions for user 102 and/or a transaction-enabled device 160. Restrictions for user 102 and/or the devices associated with the user 102 may be set and managed by user 102, a person/entity associated with user 102 (e.g., a guardian for user 102, a workplace for user 102 providing one or more vehicles to user 102, etc.), and/or a person/entity exerting control over the devices associated with user 102. In one embodiment, the restrictions module 132 communicates with the secure transaction module 132 on the master device 110.

[00040] Authentication module 134 may correspond to one or more processes to execute module and associated devices of transaction processing server 140 to generate, store and exchange authentication information and authenticate devices and transactions.

Authentication module 134 uses database 140 to store device, user and authentication information which may include devices identifiers, user identification, user account information and authentication information such as encryption keys and tokens.

[00041] Network 150 may be implemented as a single network or a combination of multiple networks. For example, in various embodiments, network 150 may include the Internet or one or more intranets, landline networks, wireless networks, and/or other appropriate types of networks. Network 150 may correspond to small scale communication

networks, such as a private or local area network, or a larger scale network, such as a wide area network or the Internet, accessible by the various components of system 100.

[00042] Referring to FIG. 3, an embodiment of an exemplary network system suitable for processing a secure transaction is illustrated. Environment 200 includes a user 202 corresponding generally to user 102 of FIG. 2, with a transaction-enabled device 204 and a companion device 206, that correspond generally to the transaction-enabled device 160 and companion device 170 of Fig. 2. As illustrated, the transaction-enabled device 204 is a fitness watch, which may be used to track user 202's performance activity during exercise such as heart rate, exercise time, and distance via GPS. Companion device 206 is a body monitoring shirt 206 that include circuitry for measuring user 202's biometric characteristics during exercise, such as heart rate, and transmitting the data to the watch 204.

[00043] In environment 200, user 202 desires to purchase a good or service (e.g., food and drink) from a merchant 210 using the watch 204, which has been authenticated as a transaction-enabled device through service provider 240. The user 202 activates a secure payment application on the watch 204, and the watch 204 searches for the shirt 206 as a companion device and requests authentication information. In one embodiment, the watch 204 establishes a secure wireless communication with network 150 to access service provider 240 and transmits unique identification information from the shirt 206 (secondary device) and watch 204 (primary device) to the service provider 240 to authenticate the watch 204 for payment. If service provider 240 authenticates the two devices, then the secure payment application on the watch is enabled and user 202 can use the watch 204 to make an electronic payment through the merchant 210's point of sale terminal 212, such as through near field communication. As illustrated in environment 200, the watch 204 will only be enabled for payment at merchant 210 if the watch 204 is in communication with shirt 206. In an alternate embodiment, after the watch 204 receives authentication information from the shirt 206, the watch 204 prepares an electronic message including a timestamp, transaction information, and authentication information for both the watch 204 and the shirt 206, and the electronic message is transmitted to the merchant 210 through the point-of-sale terminal 212. The merchant 210 forwards the transaction message to the service provider 240, which verifies the watch 204 and shirt 206 before proceeding to authorize the transaction.

[00044] Referring to FIGs. 4a-b, exemplary flow charts for an embodiment of delegating a secure transaction from a trusted user device to a second device is illustrated. Note that one or

more steps, processes, and methods described herein may be omitted, performed in a different sequence, or combined as desired or appropriate.

[00045] In one embodiment, a user accesses a master device to execute the steps of the process 400. In step 402, the user launches the secure transaction module on the trusted master device and establishes a secure communication session with the secure transaction server. In an exemplary embodiment, the secure transaction module is an electronic payment application accessible through the user interface of the master user device. In one embodiment, the user is prompted to enter identifying information, such as a username and password, personal identification number, fingerprint scan, retinal scan, or facial or voice recognition. As a trusted device, the master device also exchanges authentication information to authenticate the device, such as device identifiers, tokens and one or more encryption keys.

[00046] In step 404, the user selects a second device that will operate as a transaction-enabled device, and the master device establishes a communication with a secure transaction module of the second device. The second device searches for available companion devices that are in proximity, the user selects an available companion device and the second device requests device authentication information. The second device returns unique device identifiers for the second device and the selected companion device to the master device.

[00047] The master device receives the device identifiers for the second device and the companion device and in step 406, transmits the second device information and companion device information to the service provider. In step 408, the master device receives authentication information from the service provider, which may include a token and one or more encryption keys for each device, and the master device transmits the authentication information to the secure transaction module on the secondary device for storage in the secure element. In one embodiment, the service provider generates a public-private key pair (e.g., using SRP or RSA public-key encryption techniques) for each device to be authenticated, with the service provider storing the public key and the private key being stored on an associated user device.

[00048] FIG. 4b is a flow chart 420 of an exemplary process performed by a second device for authenticating the device as a transaction-enabled device for a secure transaction. In step 422, the second device receives communication from the secure transaction module of the master device and launches a corresponding secure transaction module. In step 424, the second device searches for a companion device and receives a unique device identifier for the companion device. In an exemplary embodiment, the second device identifies available

wireless devices in range and allows the user to select the companion device to associate with the transaction-enabled device. In various embodiments, the list of available companion devices is presented to the user on the second device, on the master device or on another device such as a laptop computer. The short range communication protocol may comprise one of near field communication, radio communication, infrared communication, Bluetooth communication, Bluetooth Low Energy (BLE) communication, LTE Direct communication, and WiFi communication.

[00049] In step 426, the second device transmits the unique device identifiers for the second and companion devices to the master device. In step 428, the second device receives authentication information from the master device via the secure transaction module. The authentication information from the second device is stored in the secure element, and the authentication information for the companion device is transmitted to the companion device for storage. The second device also stores the companion device and restriction information for that device in the secure element. In alternate embodiments, the second device communicates with the service provider over the network, bypassing the master device in steps 426 and 428.

[00050] In various embodiments, the master device may delegate a secure transaction to a plurality of transaction-enabled devices, and each transaction-enabled device may be configured to operate with a plurality of companion devices. In one embodiment, the master device may also be used as a companion device. In other embodiments, the authentication protocol used for the companion device may depend on the features of the companion device and may include (i) the companion device transmitting a device identifier, (ii) the companion device storing a private key and encrypting the device identifier for transmission to the transaction-enabled device, (iii) the companion device receiving data from the transaction-enabled device, encrypting the received data with the device private key and returning the encrypted message, and other authentication techniques and protocols as appropriate.

[00051] FIG. 5 is a flow chart 500 of an exemplary process for enabling a secure transaction on a transaction-enabled device. In step 502, the user initiates a secure transaction from the transaction-enabled device. The transaction-enabled device attempts to connect to companion device in step 504. In one embodiment, the transaction-enabled device stores companion device identification information for use in searching for and connecting to a companion device. If a companion device is not detected in close proximity to the transaction-enabled device, then the user is notified that authentication has failed in step 508.

In one embodiment, step 508 disables further transaction processing, which may include purging confidential information from the secure element, until the transaction-enabled device is reauthenticated through the master device. In other embodiments, step 508 includes notifying the master device and/or service provider of the failed authentication attempt, determining whether the transaction-enabled device has been lost or stolen, and/or disabling further transaction processing via the service provider until the device is reauthenticated through the master device.

[00052] If a companion device is detected, the transaction-enabled device requests and receives authentication information from the companion device step 510. In step 512, authentication information is transmitted to the service provider, including an identification of the transaction-enabled device and the companion device, and a token received from the transaction-enabled device during device authentication. In various embodiments, the secure transaction module of the transaction-enabled device uses (i) companion device authentication information received from the companion device and (ii) transaction-enabled device authentication information, to prepare an authentication message for the service provider. In various embodiments, the message may include transaction information such as price, payee identification, a timestamp, an electronic token and all or a portion of the message may be encrypted using one or more encryption keys received from the service provider. In one embodiment, the message is provided to a merchant who forwards the message to the service provider for authorization of the payment. In another embodiment, the message is sent to the service provider for pre-authorization and once approved, payment information is provided to the merchant to complete the transaction. For example, the service provider could return a QR code that may be scanned at the merchant.

[00053] The service provider will decrypt the message using corresponding public keys and compare the token and device identifiers to information stored in the database of the service provider. During device authentication, the device IDs were transmitted to the service provider and the service provider transmitted a unique token associated with the user account and usable only by the transaction-enabled device. If the decrypted information matches then the transaction-enabled device is authenticated and the secure transaction module is authorized in step 516. If the information does not match, then the authentication fails and the user is notified in step 508. In various embodiments, step 508 further includes disabling secure transaction processing via the service provider and/or the transaction-enabled device, which may include purging confidential information from the secure element

of the transaction-enabled device, until the transaction-enabled device is reauthenticated through the master device.

[00054] FIG. 6 is a block diagram of a computer system suitable for implementing one or more components described in Figs. 2 and 3, according to an embodiment. In various embodiments, the trusted user device may comprise a personal computing device (e.g., smart phone, a computing tablet, a personal computer, laptop, a wearable computing device such as glasses or a watch, Bluetooth device, key FOB, badge, etc.) capable of communicating with the network 150. The service provider may utilize a network computing device (e.g., a network server) capable of communicating with the network. It should be appreciated that each of the devices utilized by users and service providers may be implemented as computer system 600 in a manner as follows.

[00055] Computer system 600 includes a bus 602 or other communication mechanism for communicating information data, signals, and information between various components of computer system 600. Components include an input/output (I/O) component 604 that processes a user action, such as selecting keys from a keypad/keyboard, selecting one or more buttons, image, or links, and/or moving one or more images, etc., and sends a corresponding signal to bus 602. I/O component 604 may also include an output component, such as a display 611 and a cursor control 613 (such as a keyboard, keypad, mouse, etc.). An optional audio input/output component 605 may also be included to allow a user to use voice for inputting information by converting audio signals. Audio I/O component 605 may allow the user to hear audio. A transceiver or network interface 606 transmits and receives signals between computer system 600 and other devices, such as another user device, service device, or a service provider server via network 150. In one embodiment, the transmission is wireless, although other transmission mediums and methods may also be suitable. One or more processors 612, which can be a micro-controller, digital signal processor (DSP), or other processing component, processes these various signals, such as for display on computer system 600 or transmission to other devices via a communication link 618. Processor(s) 612 may also control transmission of information, such as cookies or IP addresses, to other devices.

[00056] Components of computer system 600 also include a system memory component 614 (e.g., RAM), a static storage component 616 (e.g., ROM), and/or a disk or flash drive 617. Computer system 600 performs specific operations by processor(s) 612 and other components by executing one or more sequences of instructions contained in system memory

component 614. Logic may be encoded in a computer readable medium, which may refer to any medium that participates in providing instructions to processor(s) 612 for execution. Such a medium may take many forms, including but not limited to, non-volatile media, volatile media, and transmission media. In various embodiments, non-volatile media includes optical or magnetic disks, volatile media includes dynamic memory, such as system memory component 514, and transmission media includes coaxial cables, copper wire, and fiber optics, including wires that comprise bus 602. In one embodiment, the logic is encoded in non-transitory computer readable medium. In one example, transmission media may take the form of acoustic or light waves, such as those generated during radio wave, optical, and infrared data communications.

[00057] Some common forms of computer readable media includes, for example, floppy disk, flexible disk, hard disk, magnetic tape, any other magnetic medium, CD-ROM, any other optical medium, punch cards, paper tape, any other physical medium with patterns of holes, RAM, PROM, EEPROM, FLASH-EEPROM, any other memory chip or cartridge, or any other medium from which a computer is adapted to read.

[00058] In various embodiments of the present disclosure, execution of instruction sequences to practice the present disclosure may be performed by computer system 600. In various other embodiments of the present disclosure, a plurality of computer systems 600 coupled by communication link 618 to the network (e.g., such as a LAN, WLAN, PTSN, and/or various other wired or wireless networks, including telecommunications, mobile, and cellular phone networks) may perform instruction sequences to practice the present disclosure in coordination with one another.

[00059] FIGs. 7a-b illustrate exemplary data structures for stored information at the transaction-enabled device and transaction processing server, respectively. In Fig. 7a, the transaction-enabled device stores transaction authentication data 700 and companion device data 702. The transaction authentication data 700 includes account data, device authentication data, transaction service provider data and other authentication data as required by the transaction processing server. In one embodiment, the transaction authentication data 700 is provided by the transaction processing server during authentication of the transaction-enabled device and includes a payment token associated with the user account, a private encryption key for use by the transaction-enabled device in digitally signing transaction messages, and identifying information for the service provider. In various embodiments, the transaction authentication data may include other data corresponding to one or more electronic payment

protocols used by the transaction processing server. The companion device data 702 includes information for locating and authenticating a companion device.

[00060] Referring to Fig. 7b, the transaction processing server stores delegation information and authentication information mapping the user account to one or more master devices, one or more transaction-enabled devices and one or more companion devices. The account data may include an account number and user information. The master device data may include a device identifier and information for device and user authentication. The transaction-enabled device data may include a device ID, payment token, and encryption keys. The companion device information may include a device ID for the companion device and encryption key for decoding companion device message.

[00061] Where applicable, various embodiments provided by the present disclosure may be implemented using hardware, software, or combinations of hardware and software. Also, where applicable, the various hardware components and/or software components set forth herein may be combined into composite components comprising software, hardware, and/or both without departing from the spirit of the present disclosure. Where applicable, the various hardware components and/or software components set forth herein may be separated into sub-components comprising software, hardware, or both without departing from the scope of the present disclosure. In addition, where applicable, it is contemplated that software components may be implemented as hardware components and vice-versa.

[00062] Software, in accordance with the present disclosure, such as program code and/or data, may be stored on one or more computer readable mediums. It is also contemplated that software identified herein may be implemented using one or more general purpose or specific purpose computers and/or computer systems, networked and/or otherwise. Where applicable, the ordering of various steps described herein may be changed, combined into composite steps, and/or separated into sub-steps to provide features described herein.

[00063] The foregoing disclosure is not intended to limit the present disclosure to the precise forms or particular fields of use disclosed. As such, it is contemplated that various alternate embodiments and/or modifications to the present disclosure, whether explicitly described or implied herein, are possible in light of the disclosure. Having thus described embodiments of the present disclosure, persons of ordinary skill in the art will recognize that changes may be made in form and detail without departing from the scope of the present disclosure. Thus, the present disclosure is limited only by the claims.

CLAIMS

WHAT IS CLAIMED IS:

1. In a secure transaction system having master device associated with a user account, the master device configured to engage in a secure transaction with a second device, a mobile device comprising:

a secure element storing at least one identifier of a companion device and authentication information associated with the mobile device and the user account;

a companion detection module comprising a short range wireless communication system configured to detect the presence of a companion device; and

a secure transaction module configured to engage in a secure transaction with the second device while a companion device is detected, the secure transaction being associated with the user account.

2. The mobile device of claim 1, wherein the secure transaction module is configured to terminate a secure transaction if the presence of a companion device is not detected.

3. The mobile device of claim 1, wherein the companion detection module is configured to receive authentication information associated with the companion device; and wherein the secure transaction module is configured to generate a transaction message comprising the stored authentication information and the received authentication information.

4. The mobile device of claim 1, wherein the secure transaction module is further configured to detect communication from the master device, and engage in an authentication process, including receiving the authentication information from the master device.

5. The mobile device of claim 4, wherein the secure transaction module is further configured to terminate the secure transaction if a companion device is not detected.

6. The mobile device of claim 5, wherein if the secure transaction is initiated without a detected companion device, the secure transaction module disables secure transaction processing on the mobile device until the mobile device is re-authenticated through the master device.

7. In an electronic payment system having a first device authenticated by a service provider for electronic payments associated with a user account, a method for delegating secure transactions to a second mobile device, the method comprising the steps:

- authenticating the second device for use with the account;
- storing authentication information on the second device, the authentication information including authentication information associated with a third device;
- detecting the third device in proximity to the second device; and
- processing an electronic payment transaction through the second device while the third device is detected.

8. The method of claim 7 wherein the stored authentication information further comprises authentication information associated with the second device, including a payment token associated with the second device and a private key associated with the second device.

9. The method of claim 8 wherein the stored authentication information further comprises a public key associated with the third device.

10. The method of claim 9 wherein the step of processing further comprises the steps:

- establishing communication between the second device and a third party device;
- receiving transaction data from the third party device;
- using the private key associated with the second device, encrypting the transaction data, second device authentication information and third device authenticating information to produce a transaction message; and
- transmitting the transaction message to the third party device.

11. The method of claim 9 wherein the step of authenticating further comprises the following steps performed on the first device:

- accessing the user account;
- connecting to the second device;
- receiving a second device identifier associated with the second device;
- receiving a third device identifier associated with the third device; and
- requesting authentication information for the second device, as a transaction-enabled device, and the third device, as a companion device.

12. The method of claim 7 wherein the step of detecting further comprises the steps:

- determining detection information for the third device through the stored authentication information; and
- running a short range communication protocol associated with the third device comprising one of near field communication, radio communication, infrared communication, Bluetooth communication, Bluetooth Low Energy (BLE) communication, LTE Direct communication, and WiFi communication.

13. In an electronic payment system having a first device authenticated by a service provider for electronic payments associated with a user account, a system for delegating secure transactions to a secondary device, the system comprising:

a secure transaction module configured to process an electronic payment transaction from an authorized device;

a database storing user account information, including an account identifier and an associated device authentication information; and

an authentication module configured to receive a transaction message associated with a secondary device, the transaction message including authentication information associated with a third device, and authenticate the received transaction if the secondary device and a third device are authenticated.

14. The system of claim 13, wherein the stored user account information further includes at least one restriction associated with the user account information.

15. The system of claim 14, wherein the associated device authentication information comprises a first device identifier for authenticating electronic payments originating from the first device.

16. The system of claim 15, wherein the associated device authentication information comprises a second device identifier and a third device identifier for authenticating electronic payments originating from the second device.

17. The system of claim 13, wherein the authentication module further comprises an administration module configured to generate a payment token and encryption keys for authorized devices.

18. The system of claim 13 wherein the authentication module is further configured to deny authentication of the received transaction if either the secondary or third device are not authenticated.

19. The system of claim 13 wherein the authentication of the second device includes decrypting the transaction message using a stored public key associated with the second device.

20. The system of claim 13 wherein the user account information includes a mapping of potential companion devices that may be used to authenticate the secondary device, and wherein the authentication of the secondary and third devices includes verifying an associated mapping of the devices in the database.

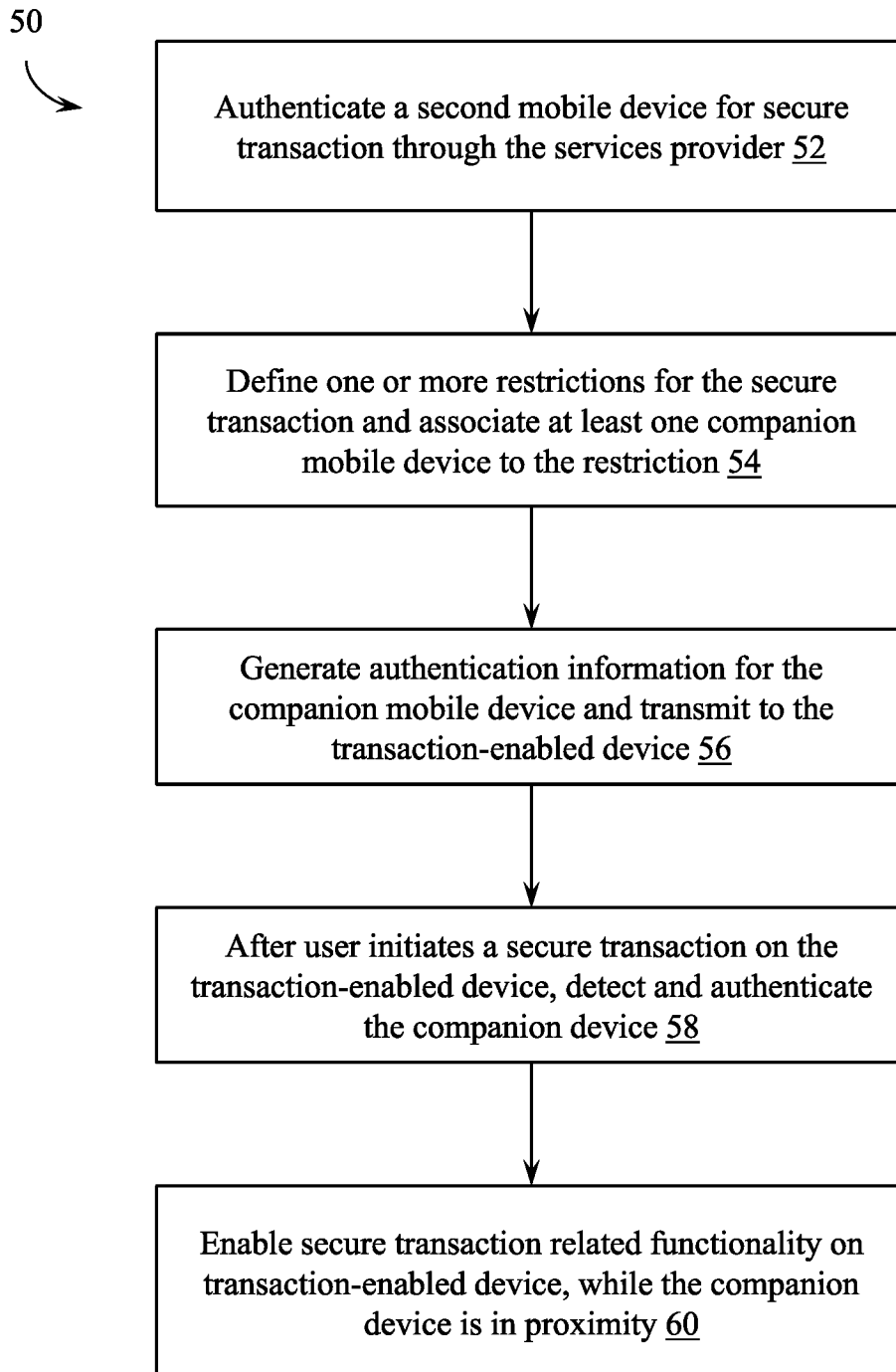


FIG. 1

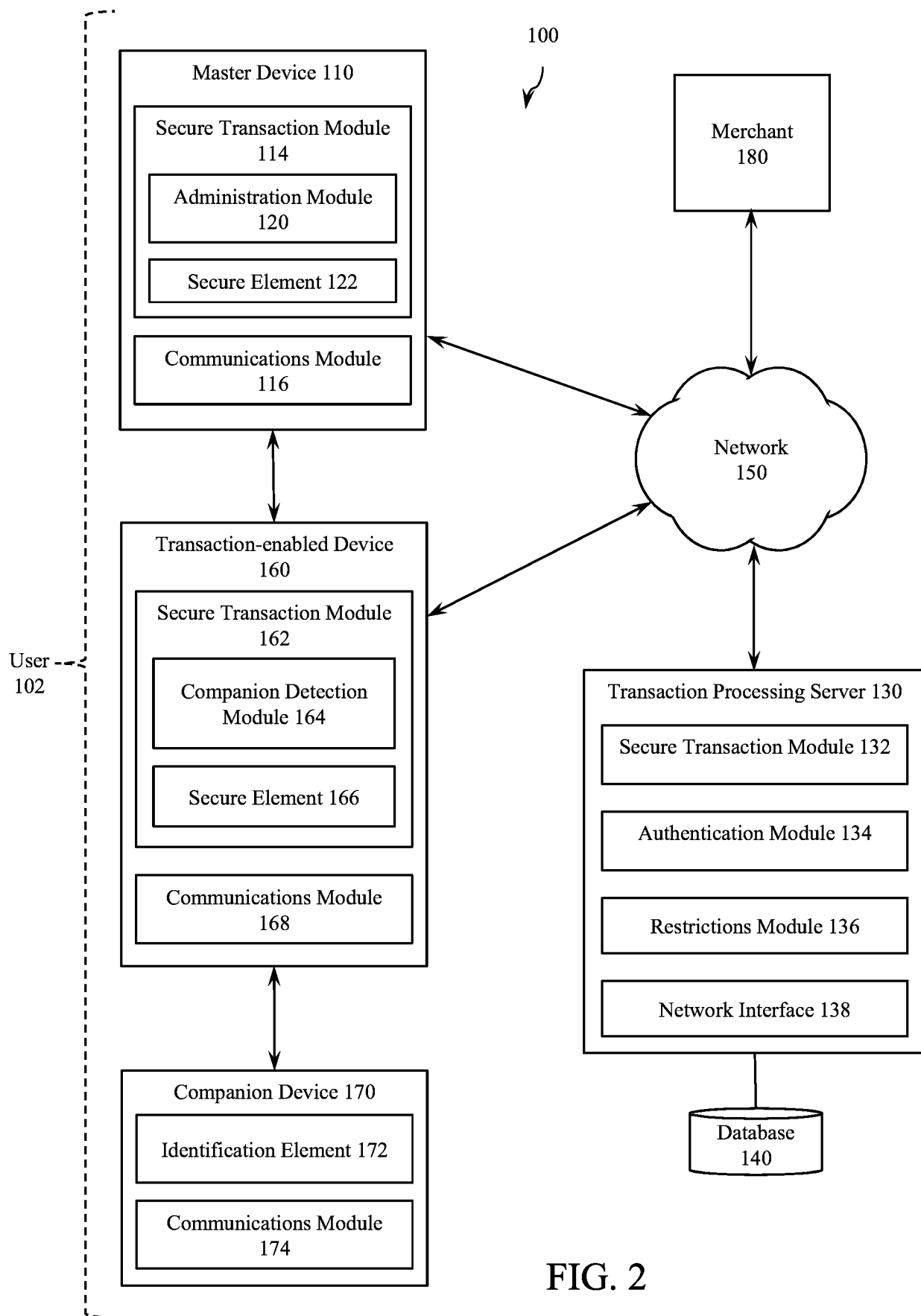


FIG. 2

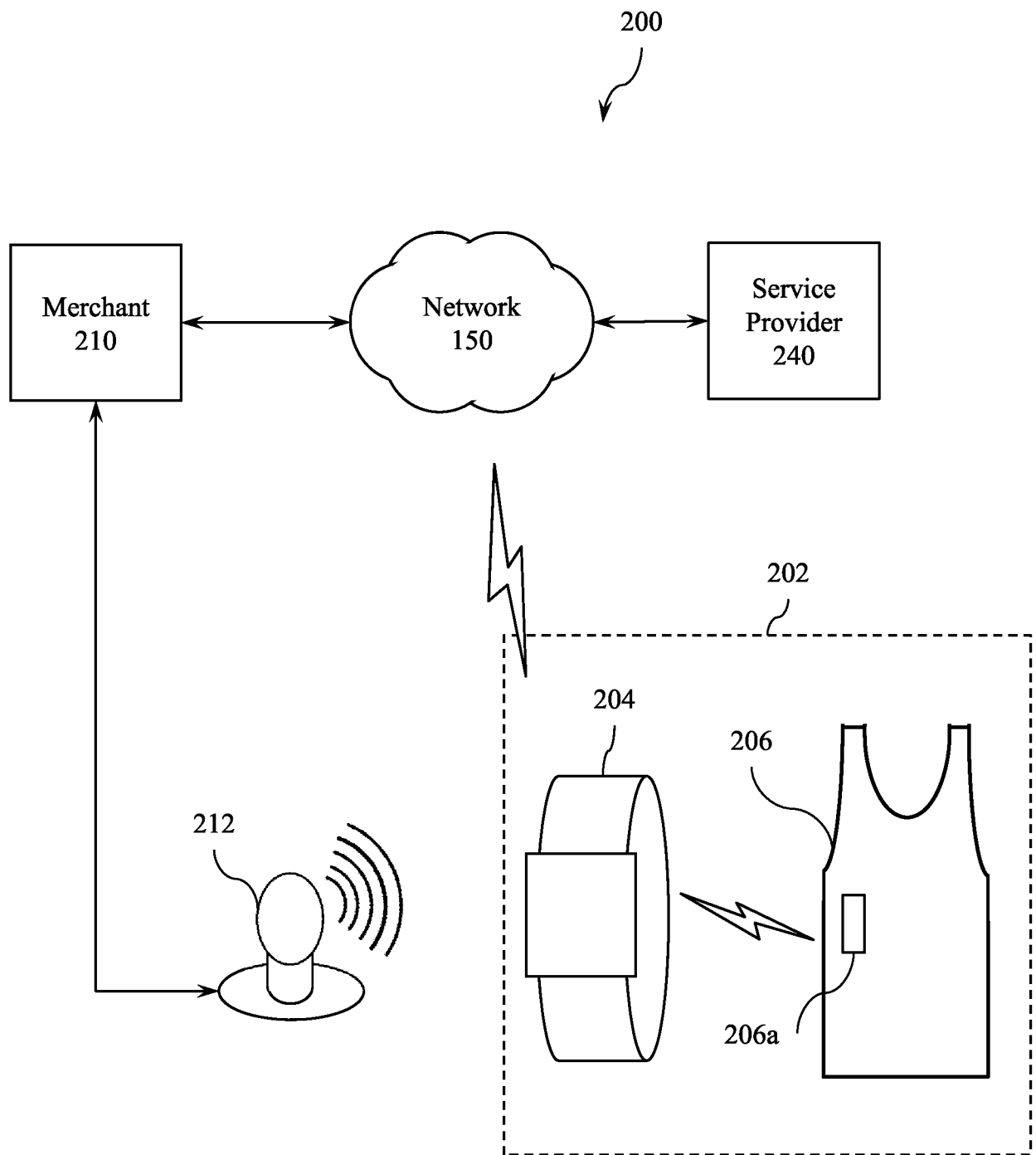
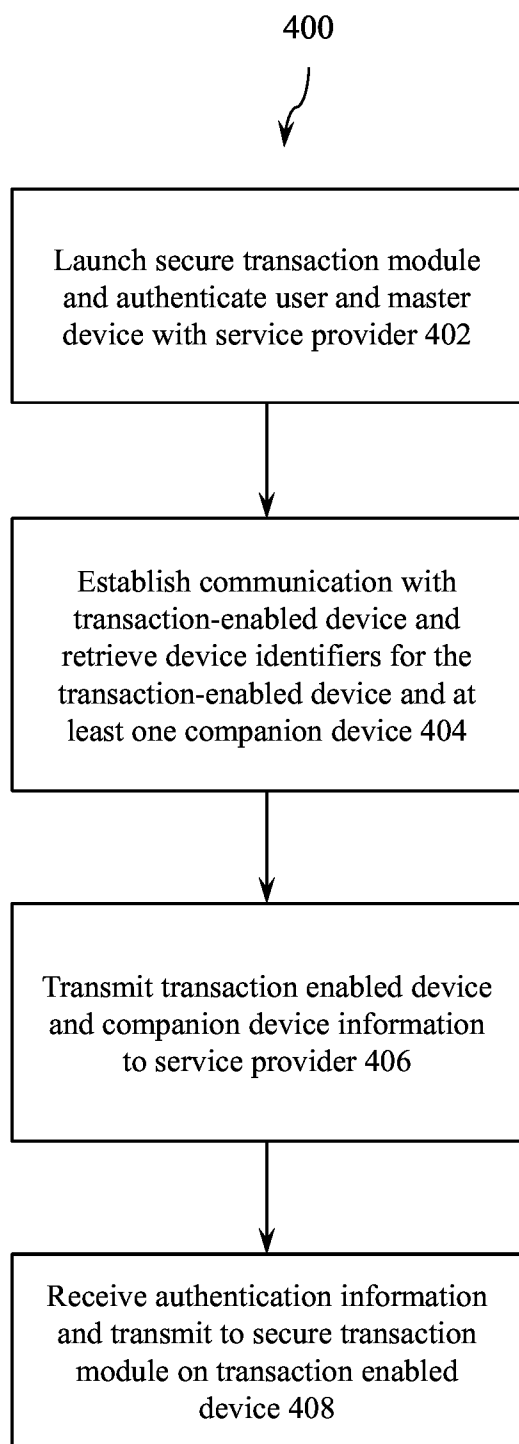
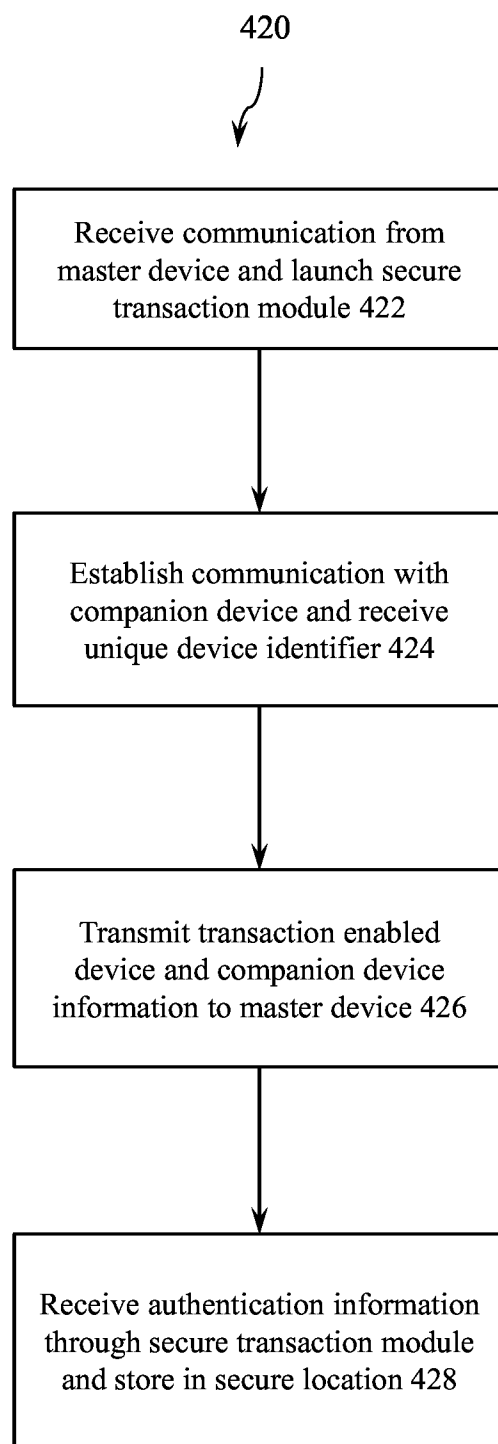


FIG. 3



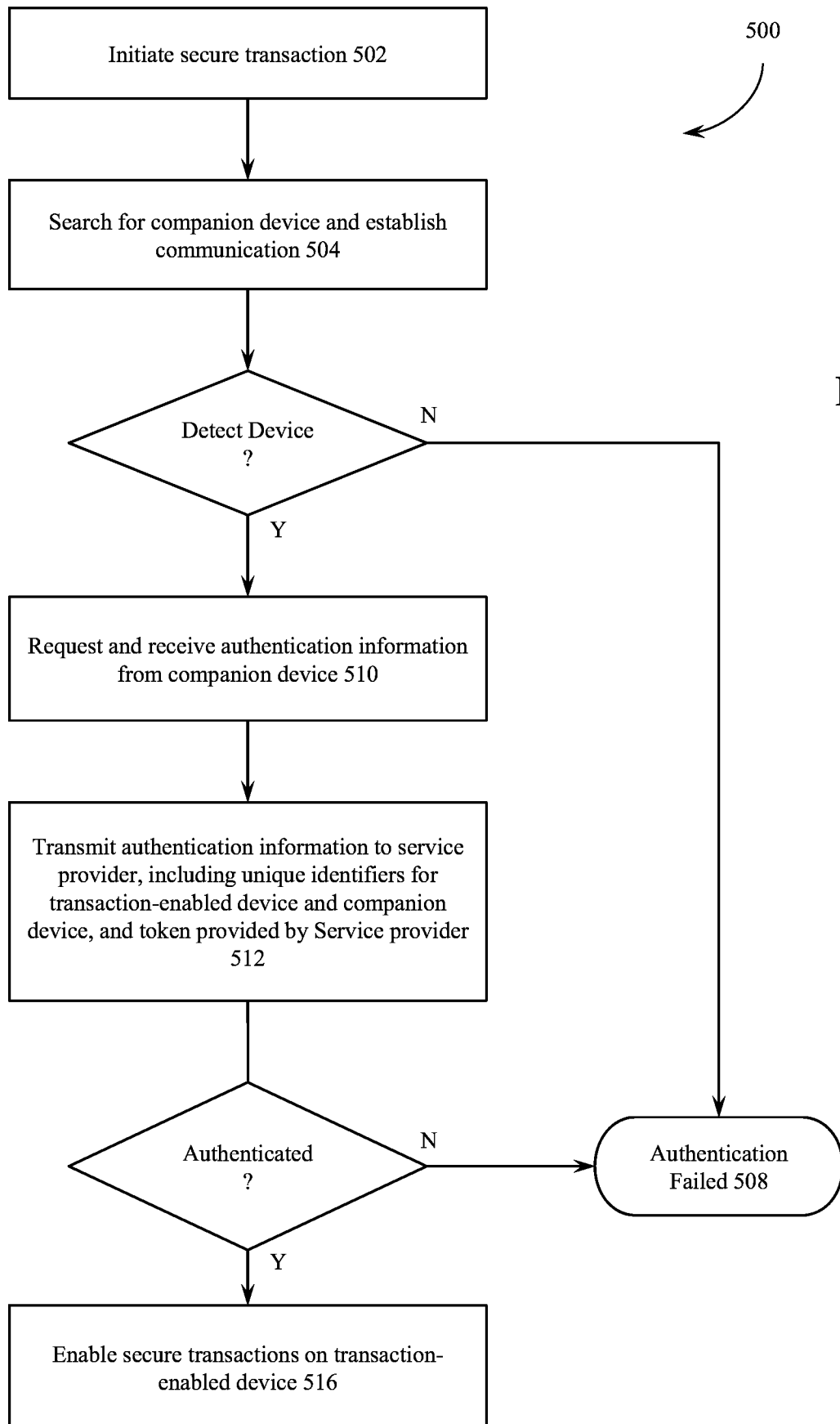
Master Device

FIG. 4a



Transaction-Enabled Device

FIG. 4b



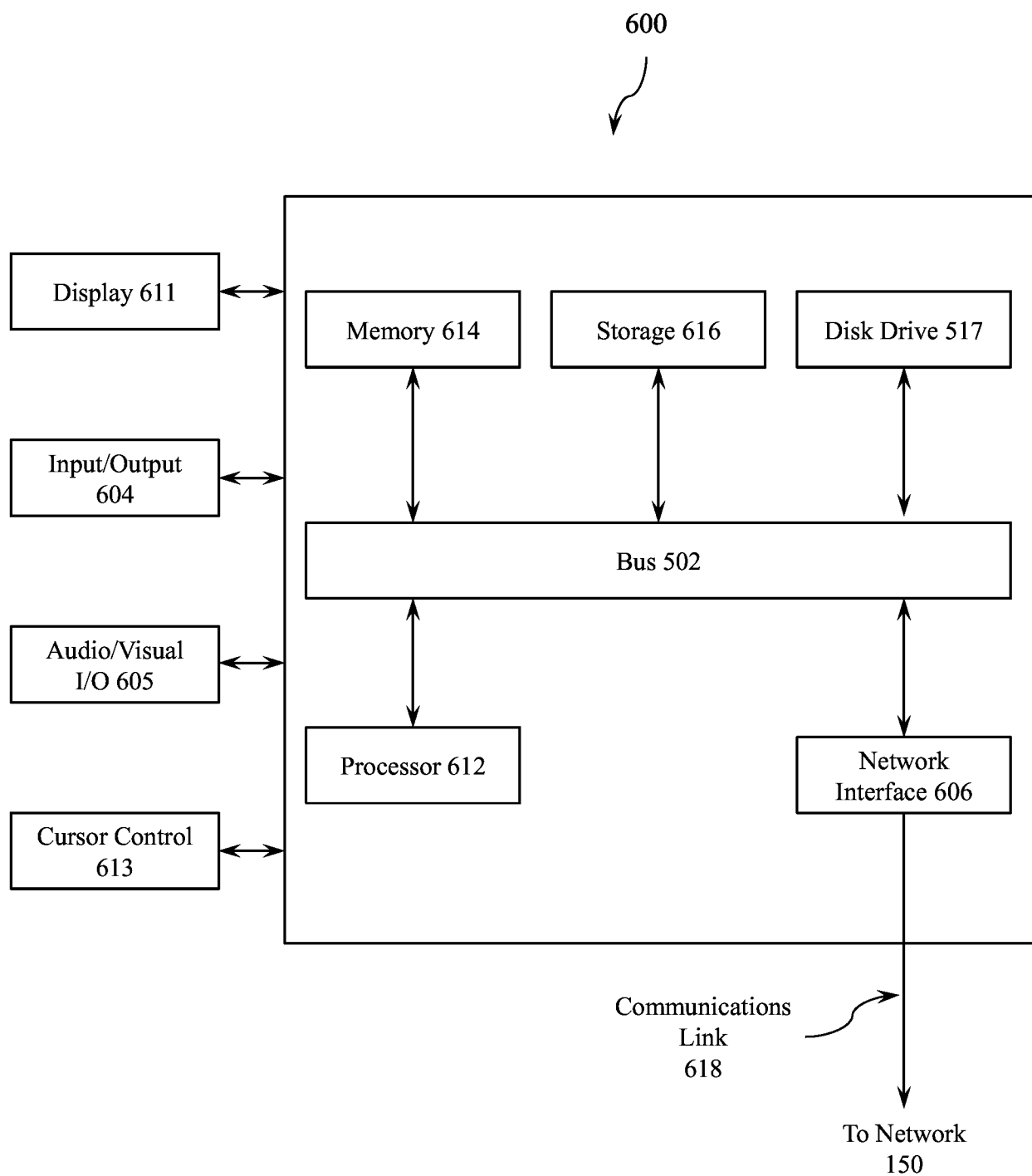


FIG. 6

FIG. 7a

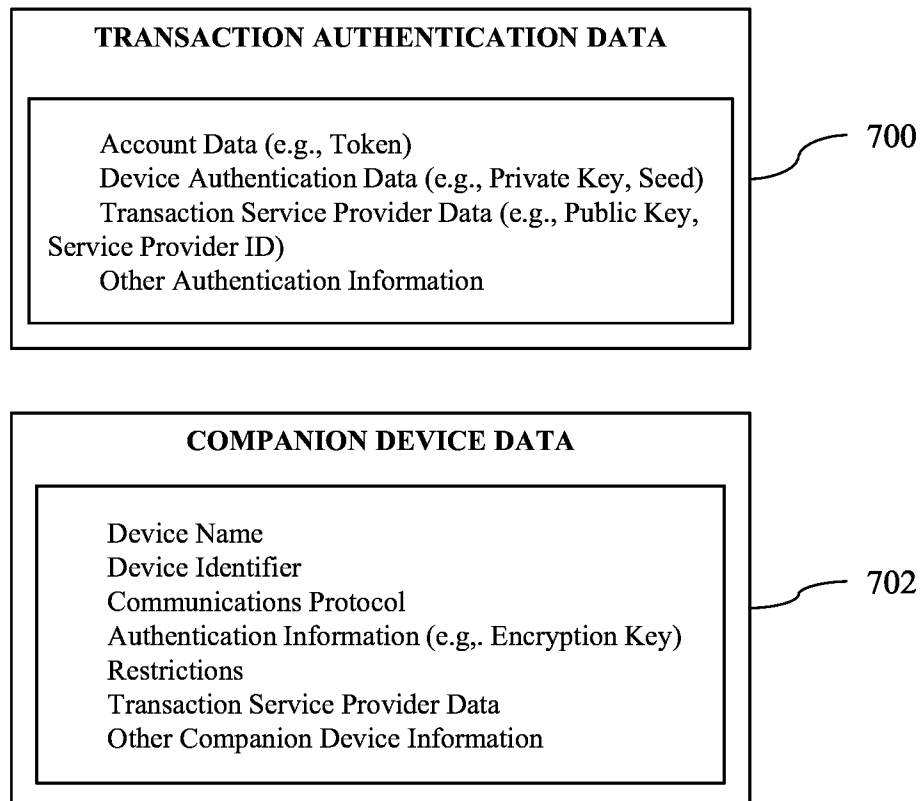
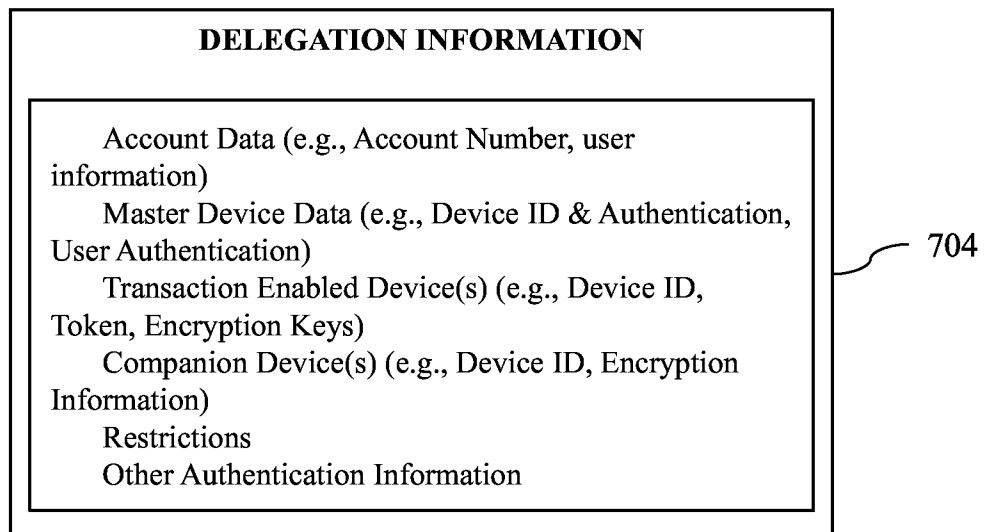


FIG. 7b



INTERNATIONAL SEARCH REPORT

International application No.

PCT/US15/63315

A. CLASSIFICATION OF SUBJECT MATTER IPC(8) - G06Q20/36, G06Q30/06, H04L9/32 (2016.01) CPC - G06Q20/367, G06Q20/40, H04L9/32 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) IPC(8) Classifications: G06Q20/36, G06Q20/38, G06Q20/40, G06Q30/02, G06Q30/06, H04L9/32 (2016.01) CPC Classifications: G06Q20/367, G06Q20/382, G06Q20/401, G06Q20/40, G06Q20/409, G06Q30/06, H04L9/32 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 practicable, search terms used) PatSeer (US, EP, WO, JP, DE, GB, CN, FR, KR, ES, AU, IN, CA, AT, DK, CH, FI, TH, BE, BR, NL, PH, LU, SE, RU, NO, INPADOC Data); EBSCO; IP.com; Google Keywords: device, authenticate, identify, master, primary, first, second, process, secure, transaction		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2014/0258132 A1 (EZETAP MOBILE SOLUTIONS PRIVATE LIMITED) 11 September 2014; abstract; figures 1, 3; paragraphs [0027], [0077], [0149], [0153], [0154], [0176]; claim 1	1-6
Y	US 2014/0278892 A1 (TRACFONE WIRELESS, INC.) 18 September 2014; figures 1, 2; paragraphs [0028], [0038], [0054]	1-6
Y	US 2013/0132307 A1 (PHELPS, J et al.) 23 May 2013; paragraph [0047]	2, 5, 6
Y	US 2014/0279477 A1 (SHEETS, J et al.) 18 September 2014; paragraph [0061]	3
Y	US 8,805,726 B2 (BLAZE MOBILE, INC) 12 August 2014; figures 1, 2; column 2, lines 60-67; column 3, lines 1-19; column 4, lines 4-7	6
Y	US 2010/0057623 A1 (KAPUR, S et al.) 04 March 2010; abstract; figure 1; paragraphs [0023], [0024], [0026], [0027]	7-12
Y	US 2014/0095580 A1 (VERIZON PATENT AND LICENSING, INC.) 03 April 2014; figure 8; paragraphs [0018], [0019], [0067], [0069], [0072]	7-12
Y	US 2014/0250016 A1 (KRANZLEY, A) 04 September 2014; paragraphs [0024], [0026], [0027]	8-11
Y	US 6,957,198 B2 (KUMHYR, D) 18 October 2005; abstract	9-11
☐ 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 application or patent 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 22 March 2016 (22.03.2016)		Date of mailing of the international search report 11 APR 2016
Name and mailing address of the ISA/ Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-8300		Authorized officer Shane Thomas PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US15/63315

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

-See Extra Sheet-

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
2. ☐ As all searchable claims could be searched without effort justifying additional fees, this Authority did not invite payment of additional fees.
3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:
4. ☒ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:
Group I: Claims 1-12

Remark on Protest

- ☐ The additional search fees were accompanied by the applicant's protest and, where applicable, the payment of a protest fee.
- ☐ The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.
- ☐ No protest accompanied the payment of additional search fees.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US15/63315

-Continued from Box No. III Observations where unity of invention is lacking-

This application contains the following inventions or groups of inventions which are not so linked as to form a single general inventive concept under PCT Rule 13.1. In order for all inventions to be examined, the appropriate additional examination fee must be paid.

Group I: Claims 1-12 are directed toward a mobile device and method for delegating secure transactions using second device proximity.

Group II: Claims 13-20 are directed toward a system for delegating secure transactions using second device authentication.

The inventions listed as Groups I and II do not relate to a single general inventive concept under PCT Rule 13.1 because, under PCT Rule 13.2, they lack the same or corresponding special technical features for the following reasons:

The special technical features of Group I include detecting the third device in proximity to the second device; and processing an electronic payment transaction through the second device while the third device is detected, which are not present in Group II.

The special technical features of Group II include the transaction message including authentication information associated with a third device, and authenticate the received transaction if the secondary device and a third device are authenticated, which are not present in Group I.

The common technical features shared by Groups I and II are in an electronic payment system having a first device authenticated by a service provider for electronic payments associated with a user account, a system for delegating secure transactions to a secondary device, the system comprising: a secure module configured to process an electronic payment transaction from an authorized device; storing an account identifier and an associated device authentication information; and a module configured to receive a transaction message associated with a secondary device.

However, these common features are previously disclosed by US 2014/0095580 A1 to Verizon Patent and Licensing Inc. (hereinafter 'Verizon'). Verizon discloses in an electronic payment system having a first device authenticated by a service provider for electronic payments associated with a user account (a querying server 220 authenticated with a proximity server (service provider) for payment verification, paragraphs [0037] and [0069]), a system for delegating secure transactions to a secondary device (transactions are premised on proximity of second device, paragraph [0069]), the system comprising: a secure module configured to process an electronic payment transaction from an authorized device (device may securely process payment transactions, paragraph [0022] and [0069]); storing an account identifier and an associated device authentication information (system stores account information and associated device information, paragraph [0071]); and a module configured to receive a transaction message associated with a secondary device (system receives location information for the second user device, paragraphs [0067] and [0069]).

Since the common technical features are previously disclosed by the Verizon reference, these common features are not special and so Groups I and II lack unity.