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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
20 April 2017 (20.04.2017)

WIPO | PCT

(10) International Publication Number
WO 2017/066792 A1

(51) International Patent Classification:
H04L 9/32 (2006.01) *G06Q 20/40* (2012.01)

(21) International Application Number:
PCT/US2016/057400

(22) International Filing Date:
17 October 2016 (17.10.2016)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
62/242,068 15 October 2015 (15.10.2015) US
62/242,074 15 October 2015 (15.10.2015) US

(71) Applicant: **VISA INTERNATIONAL SERVICE ASSOCIATION** [US/US]; P.O. Box 8999, San Francisco, California 94128 (US).

(72) Inventors: **AL-BEDAIWI, Mohammad**; 6017 Ronchamps Drive, Round Rock, Texas 78681 (US). **ALTENHOFEN, Meredith**; 1800 Pacific Avenue, Apt. 406, San Francisco, California 94109 (US). **BLACKHURST, Jason**; 1536 Pacific Avenue, Apt. No. 6, San Francisco, California 94109 (US).

(74) Agents: **TAKAGI, Moeka** et al.; Kilpatrick Townsend & Stockton LLP, 1100 Peachtree Drive, #2800, Atlanta, GEORGIA 30309 (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, DJ, 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, KW, 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, 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))*

(54) **Title**: INSTANT TOKEN ISSUANCE SYSTEM

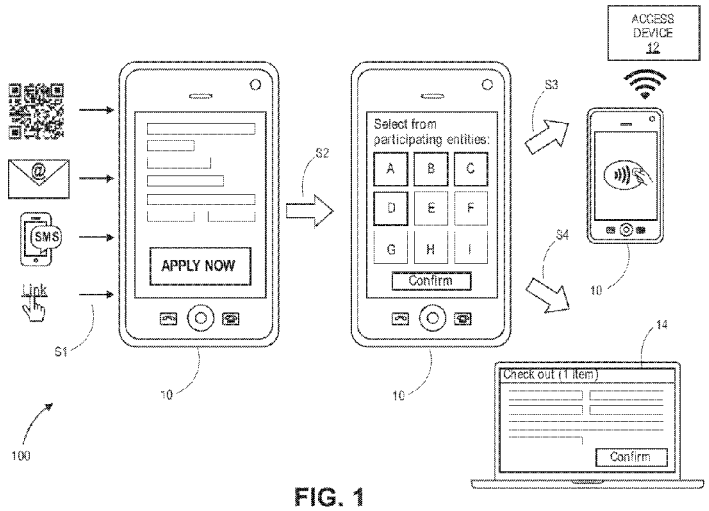

FIG. 1

(57) **Abstract**: A user can request provisioning of account information for an account to a plurality of resource providing entities. The account may be a new or existing account issued by an authorization computer. The authorization computer may prompt the user to select one or more resource providing entities to which to provision a token associated with the account. Processor server computer may then tokenize the account information associated with the account by determining a token for each resource providing entity selected by the user. In some cases, a token may be provisioned to an already existing account or profile (e.g., account on file) associated with a resource providing entity. In other cases, an account or profile associated with a resource providing entity may not yet exist and thus may be created before a token may be provisioned. Subsequently, the user may utilize provisioned tokens to conduct transactions.

WO 2017/066792 A1

INSTANT TOKEN ISSUANCE SYSTEM

CROSS-REFERENCES TO RELATED APPLICATIONS

[0001] This application is a non-provisional of and claims the benefit of priority to U.S. Provisional Application No. 62/242,068, filed October 15, 2015, and U.S. Provisional Application No. 62/242,074, filed October 15, 2015, which are hereby incorporated by reference in its entirety for all purposes.

BACKGROUND

[0002] Users often manage multiple digital accounts associated with various entities. For example, these accounts may be associated with a variety of resource providing entities, such as merchants, digital wallet providers, and service providers. In some cases, a user may add a card account to these digital accounts to conduct transactions. Typically, the user may have to provide their card account information to each of the corresponding resource providing entities separately before conducting the transactions. This is cumbersome, since the user has to perform redundant steps of inputting the same card account information. Additionally, since each resource provider may run a different platform, the input process is not smooth and timely.

[0003] Furthermore, this process of adding a card account to digital accounts is even more cumbersome when the card account is for a new card. When a user applies for a card account, such as for a credit card, there is typically a delay until the user can utilize the card for transactions. For example, the user typically may wait until the card is made on plastic and shipped to the user, which can take at least five to seven days. This delay limits the user's ability to use the card. In addition, once the card is approved, if the user wishes to add their card account to other digital accounts, they need to add account information for the card manually for each digital account. It would be desirable to provide the user with the ability to use the new card as soon as possible.

[0004] Embodiments of the invention address this and other problems, individually and collectively.

BRIEF SUMMARY

[0005] Embodiments of the invention relate to systems and methods for provisioning account information to resource providing entities and devices. In some cases, the account information may be for an account that already exists or a new account requested by a user. Embodiments of the invention enable the user to control, through an issuer application (or a third party token portal), to which resource providing entities (e.g., merchants, digital wallet providers, service providers, etc.) the account information is provisioned. In some embodiments, the account information may include a tokenized card account information associated with a card account. In some cases, the token may also be provisioned to other devices (e.g., mobile device, tablet, wearable devices, etc.) indicated by the user. The devices may have a secure element or may be cloud-based. Embodiments of the invention make possible in-app provisioning of the card onto the user's device.

[0006] According to one embodiment of the invention, a server computer can perform a method. The server computer may send a list of participating resource providing entities to an authorization computer. The authorization computer may prompt a user operating a user device to make a selection from the list of participating resource providing entities. The server can then receive a selection of one or more resource providing entities from the participating resource providing entities and can receive a request to issue tokens associated with an account of the user for the one or more resource providing entities. For each of the one or more resource providing entities, the server computer can determine a token associated with the account of the user and can send the token to a resource providing entity computer associated with the resource providing entity, wherein the user conducts a transaction with the resource providing entity using the token.

[0007] The account may be a new account or an existing account. When the account is a new account, the server computer can receive account information associated with the account from the authorization computer. When the account is an

existing account, the server computer can retrieve the account information associated with the account.

[0008] In some embodiments, the server computer can perform authentication processes. For each of the plurality of participating resource providing entities selected by the user, the server computer can prompt the user for authentication information for the participating resource providing entity and can send the authentication information to the participating resource providing entity. In some cases, the authentication information may be utilized to generate a new account for the user associated with the participating resource providing entity.

[0009] In some embodiments, the server computer can further determine an authentication method supported by the authorization computer. For each of the list of participating resource providing entities, the server computer can also determine an authentication method supported by the participating resource providing entity and can compare the authentication method supported by the participating resource providing entity and the authentication method supported by the authorization computer. Upon determining that the compared authentication methods match, the server computer can include the participating resource providing entity in the list of participating resource providing entities.

[0010] In some embodiments, the server computer can determine that at least one of the participating resource providing entities has an account on file for the user. The server computer can send, to the authorization computer, information indicating the at least one participating resource providing entity with which the user has the account on file. In some cases, the selection of the one or more resource providing entities by the user may include a participating resource providing entity that has an account on file for the user. In some cases, the user may further conduct the transaction using the account on file.

[0011] In some embodiments, the server computer can generate one or more links. In some implementations, the server computer may generate a link routed to the server computer and can send the link to the authorization computer. The user may activate the link using the user device after the authorization computer prompts the

user. In some implementation, the server computer can generate a plurality of links routed to the plurality of resource providing entities and can send the plurality of links to the authorization computer. The user may activate the plurality of links using the user device after the authorization computer prompts the user.

[0012] Embodiments of the invention are further directed to a server computer comprising a processor and a computer readable medium. The computer readable medium can be coupled to the processor and can comprise code, executable by the processor, for implementing any of the methods described herein.

[0013] These and other embodiments of the invention are described in further detail below.

BRIEF DESCRIPTION OF THE DRAWINGS

[0014] FIG. 1 shows an exemplary flow diagram of a method according to embodiments of the present invention.

[0015] FIG. 2 shows an exemplary user interface according to embodiments of the present invention.

[0016] FIG. 3 shows an exemplary user interface according to embodiments of the present invention.

[0017] FIG. 4 shows a block diagram of an exemplary system according to embodiments of the present invention.

[0018] FIG. 5 shows a block diagram of an exemplary system according to embodiments of the present invention.

[0019] FIG. 6 shows an exemplary flow diagram of a method according to embodiments of the present invention.

[0020] FIG. 7 shows a block diagram of an exemplary system according to embodiments of the present invention.

[0021] FIG. 8 shows an exemplary flow diagram of a method according to embodiments of the present invention.

[0022] FIG. 9 shows a flowchart of a method for enabling a user immediate card access upon approval and token provisioning to account on file merchants according to embodiments of the present invention.

[0023] FIG. 10 shows an exemplary flowchart of a method for enabling a user immediate card access upon approval according to embodiments of the present invention.

[0024] FIG. 11 shows an exemplary flowchart of a method for enabling a user immediate card access upon approval according to embodiments of the present invention.

[0025] FIG. 12 shows an exemplary flowchart of a method for enabling a user immediate card access upon approval according to embodiments of the present invention.

DETAILED DESCRIPTION

[0026] Embodiments of the invention relate to account information that can be provisioned to resource providing entities and devices. In some embodiments, the account information may be instantly issued to a user. For example, when the user applies for a new payment card with an authorizing entity using a user device, the user can be approved for the new payment card. Subsequently, tokens associated with the new payment card can be provisioned to the user device as well as to resource providing entities selected by the user. In other embodiments, tokens associated with the new payment card may be created at a later time following issuance of the card. Hence, embodiments of the invention are not limited to instant issuance of cards.

[0027] Additional steps may be performed to provide the new payment card account number or token associated with the new payment account number to account on file (e.g., card on file) merchants. Embodiments of the invention enable the user to control, through an issuer application (or a third party token portal), to which resource

providing entities (e.g., merchants, digital wallet providers, service providers, etc.) the newly issued card's token is provisioned. In some embodiments, the token may also be provisioned to other devices (e.g., mobile device, tablet, wearable devices, etc.) indicated by the user. The devices may have a secure element or may be cloud-based. Embodiments of the invention make possible in-app provisioning of the card onto the user's device.

[0028] In some embodiments, the user may not be restricted to utilizing the tokens for recurring payments. For example, once a token is provisioned to a merchant or device, the token can be utilized for any transaction of any type (e.g., recurring, one-time, on-demand, etc.). Payment methods for the transactions may include eCommerce (electronic commerce), mCommerce (mobile commerce), In-app (purchases from within an application), NFC (near field communication), MST (Magnetic Secure Transmission™).

[0029] Further, embodiments of the invention are not limited to instant issuance and newly issued cards. Embodiments of the invention also enable provisioning of a user's existing cards to resource providing entities and devices. For example, the user may log in to their mobile or online banking account and push a token tied to one of their existing cards to resource providing entities participating in a tokenization program or to their other devices.

[0030] Further, embodiments of the invention are not limited to provisioning tokens to already existing accounts or profiles associated with the resource providing entities. Embodiments of the invention also enable the user to request the addition of tokens associated with a new or existing card to a new account or profile associated with a resource providing entity, in addition to an existing account or profile associated with a resource providing entity. In some cases, the new or existing accounts or profiles may be those associated with the user or a secondary user (e.g., family member, employee, etc.). The new account or profile can be created upon the user's request to provision tokens to the resource providing entity.

[0031] Before discussing specific embodiments and examples, some descriptions of terms used herein are provided below.

[0032] An "authorization request message" may be an electronic message that is sent to a payment processing network and/or an issuer of a payment card to request authorization for a transaction. An authorization request message according to some embodiments may comply with (International Organization of Standardization) ISO 8583, which is a standard for systems that exchange electronic transaction information associated with a payment made by a consumer using a payment device or payment account. The authorization request message may include an issuer account identifier that may be associated with a payment device or payment account. An authorization request message may also comprise additional data elements corresponding to "identification information" including, by way of example only: a service code, a CVV (card verification value), a dCVV (dynamic card verification value), an expiration date, etc.. An authorization request message may also comprise "transaction information," such as any information associated with a current transaction, such as the transaction amount, merchant identifier, merchant location, etc., as well as any other information that may be utilized in determining whether to identify and/or authorize a transaction.

[0033] An "authorization response message" may be an electronic message reply to an authorization request message generated by an issuing financial institution or a payment processing network. The authorization response message may include, by way of example only, one or more of the following status indicators: Approval -- transaction was approved; Decline -- transaction was not approved; or Call Center -- response pending more information, merchant must call the toll-free authorization phone number. The authorization response message may also include an authorization code, which may be a code that a credit card issuing bank returns in response to an authorization request message in an electronic message (either directly or through the payment processing network) to the merchant's access device (e.g. POS equipment) that indicates approval of the transaction. The code may serve as proof of authorization. As noted above, in some embodiments, a payment processing network may generate or forward the authorization response message to the merchant.

[0034] A "token" may include a substitute identifier for some information. For example, a payment token may include an identifier for a payment account that is a

substitute for an account identifier, such as a primary account number (PAN). For instance, a token may include a series of alphanumeric characters that may be used as a substitute for an original account identifier. For example, a token "4900 0000 0000 0001" may be used in place of a PAN "4147 0900 0000 1234." In some embodiments, a token may be "format preserving" and may have a numeric format that conforms to the account identifiers used in existing payment processing networks (e.g., ISO 8583 financial transaction message format). In some embodiments, a token may be used in place of a PAN to initiate, authorize, settle or resolve a payment transaction. The token may also be used to represent the original credential in other systems where the original credential would typically be provided. In some embodiments, a token value may be generated such that the recovery of the original PAN or other account identifier from the token value may not be computationally derived.

[0035] A "resource providing entity" may be an entity that may make resources available to a user. Examples of resource providing entities include merchants, vendors, suppliers, owners, traders, wallet providers, service providers, and the like. In some embodiments, such entities may be a single individual, small groups of individuals, or larger groups of individuals (e.g., companies). Resource providing entities may be associated with one or more physical locations (e.g., supermarkets, malls, stores, etc.) and online platforms (e.g., e-commerce websites, online companies, etc.). In some embodiments, resource providing entities may make available physical items (e.g., goods, products, etc.) to the user. In other embodiments, resource providing entities may make available digital resources (e.g., electronic documents, electronic files, etc.) to the user. In other embodiments, resource providing entities may manage access to certain resources by the user. In some embodiments, the resources may be services (e.g., digital wallet services). A resource providing entity may also be known as a resource provider or the like.

[0036] A "participating resource providing entity" may be a resource providing entity that is partaking in a program. In some cases, the participating resource providing entity may be a resource providing entity that is enrolled in a tokenization program. For example, the participating resource providing entity may have an account

with a token service provider (e.g., processor server computer) and may be able to process transactions conducted utilizing tokenized account information (e.g., tokens).

[0037] An "authorization computer" can include any system involved in authorization of a transaction. The authorization computer may be operated by an authorizing entity. The authorization computer may determine whether a transaction can be authorized and may generate an authorization response message including an authorization status (also may be known as an authorization decision). In some embodiments, an authorization computer may be a payment account issuer computer. In some cases, the authorization computer may store contact information of one or more users. In other embodiments, the authorization computer may authorize non-financial transactions involving a user. For example, the authorization computer may make an authorization decision regarding whether the user can access a certain resource.

[0038] "Account information" may refer to any information associated with a user's account (e.g., a payment account and/or payment device associated with the account). Such information may be directly related to the account or may be derived from information related to the account. Examples of account information may include a PAN (Primary Account Number or "account number"), user name, expiration date, CVV (Card Verification Value), dCVV (Dynamic Card Verification Value), CVV2 (Card Verification Value 2), CVC3 card verification values, etc.. CVV2 is generally understood to be a static verification value associated with a payment device. CVV2 values are generally visible to a user (e.g., a consumer), whereas CVV and dCVV values are typically embedded in memory or authorization request messages and are not readily known to the user (although they are known to the issuer and payment processors). In some cases, account information may also be known as card account information.

[0039] "Contact information" may refer to any information that can be utilized to communicate with a user. For example, contact information may include an email address, a phone number, IP address, or other information. In some embodiments, contact information may serve as an alias identifier for a user.

[0040] "Transaction data" (which may also be known as transaction information) may refer to any data or information surrounding or related to a transaction. For example, transaction data may include transaction details and any data associated with the transaction that may be utilized by entities involved in the transaction process. For instance, the transaction data may include information useful for processing and/or verifying the transaction. Transaction data may also include any data or information surrounding or related to any participants partaking in or associated with the transaction. Example transaction data may include a transaction amount, transaction location, resources received (e.g., products, documents, etc.), information about the resources received (e.g., size, amount, type, etc.), resource providing entity data (e.g., merchant data, document owner data, etc.), user data, date and time of a transaction, payment method, and other relevant information.

[0041] A "card on file" may be alternatively referred to as an "account on file." An account on file may refer to an account identifier (e.g., an account number) that is on file with a resource providing entity, such as a merchant, digital wallet, or other entity. In such situations, the account identifier may be used by a user to conduct purchases with the resource providing entity. The user does not need to specifically provide his or her account number to the resource providing entity when conducting a transaction, since the resource providing entity already has it. In some embodiments, account on file purchases may vary in frequency and/or amount and may represent an agreement between a cardholder and a merchant to purchase goods or services provided over a period of time or on demand.

[0042] A "server computer" can be a powerful computer or a cluster of computers. For example, the server computer can be a large mainframe, a minicomputer cluster, or a group of servers functioning as a unit. In one example, the server computer may be a database server coupled to a Web server.

[0043] FIG. 1 shows an exemplary flow diagram 100 of a method according to embodiments of the present invention. FIG. 1 includes a user device 10 that can communicate with an access device 12. FIG. 1 also includes a user device 14. User

device 10 and user device 14 may have similar characteristics to those described for user device 103 in FIG. 4.

[0044] Access device 12 may be any suitable device that provides access to a remote system. Access device 12 may be in any suitable form. Some examples of access devices include POS or point of sale devices (e.g., POS terminals), cellular phones, PDAs, personal computers (PCs), tablet PCs, hand-held specialized readers, set-top boxes, electronic cash registers (ECRs), automated teller machines (ATMs), virtual cash registers (VCRs), kiosks, security systems, access systems, and the like. Access device 12 may use any suitable contact or contactless mode of operation to send or receive data from, or associated with, user device 10.

[0045] In some embodiments, where access device 12 may comprise a POS terminal, any suitable POS terminal may be used and can include a reader, a processor, and a computer-readable medium. A reader may include any suitable contact or contactless mode of operation. For example, exemplary card readers can include radio frequency (RF) antennas, optical scanners, bar code readers, or magnetic stripe readers to interact with a payment device and/or mobile device. In some embodiments, a cellular phone, tablet, or other dedicated wireless device used as a POS terminal may be referred to as a mobile point of sale or an “mPOS” terminal.

[0046] At step S1, the user may apply for a new account. In some embodiments, the user may see an advertisement for creating the new account, where the advertisement may lead to a website from which the user can send a request to apply for the new account. The website may be hosted by an authorization computer associated with an authorizing entity (e.g., issuer) that may issue the new account.

[0047] The advertisement may be in various forms. In some cases, the advertisement may be in the form of a physical poster, which may include a scannable code (e.g., QR code) or printed link. The user may scan the scannable code, which may open a browser on user device 10. In other cases, the user may type in the printed link to open the website. In other cases, the advertisement may be received by email or text message, and may include a link that the user may activate to be routed to the website. In yet other embodiments, the advertisement may be an online advertisement

that may appear when the user is browsing the web. The advertisement may be clicked to route the user to the website.

[0048] After being routed the website, the user may be prompted to input information to apply for the new account. In some cases, the information may include a name, address, and contact information (e.g., email address, a phone number, etc.). In some cases, upon entering the information, the user may confirm the information by activating a software button (e.g., "Apply Now" button). This may trigger the information input by the user to be sent to the authorization computer, which may conduct an approval process to determine whether the new account can be created for the user. If generation of the account is approved, the authorization computer may generate the new account associated with the user. In some cases, generating the new account may comprise generating an account identifier associated with the new account.

[0049] At step S2, the user may be prompted with a plurality of participating resource providing entities from which the user can make a selection. The participating resource providing entities may be entities participating in a tokenization program. By selecting a resource providing entity, the user may indicate that they want to provision a token associated with the new account to the resource providing entity. In some cases, the participating resource providing entities may include various merchants, digital wallet providers, and service providers with which the user may or may not have an existing account or profile.

[0050] The user may be prompted with any suitable interface that enables selection of one or more participating resource providing entities. In some cases, the user interface may comprise selectable tiles labeled with identifiers (e.g., names) associated with a corresponding resource providing entity as shown in FIG. 1. In other cases, the user interface may comprise selectable checkboxes as shown by user interface 200 in FIG. 2. Other exemplary user interfaces may include other selectable user interface elements, such as radio buttons, dropdown lists, list boxes, buttons, toggle, sliders, and icons.

[0051] In some embodiments, the participating resource providing entities may be presented in the user interface in a certain manner. For example, in some cases, the

participating resource providing entities may be pre-selected when presented in the interface. In some cases, there participating resource providing entity may also be displayed at the top of the list of participating resource providing entities presented in the user interface. This may allow the user to easily confirm whether to add the new account to these pre-selected participating resource providing entities. However, the user may de-select any of the pre-selected participating resource providing entities to indicate that tokens associated with the new account should not be provisioned to that particular participating resource providing entity. The user may also select any additional participating resource providing entities to which tokens associated with the new account should be provisioned.

[0052] In some cases, upon making a selection of participating resource provider entities, the user may confirm the selection by activating a software button (e.g., "Confirm" button). This may trigger the selection to be sent to the authorization computer or to a processor server computer (e.g., token service provider). A token associated with the new account may be provisioned to each of the selected participating resource providing entities.

[0053] In an exemplary case, one of the selected participating resource providing entities may be a digital wallet provider. If the user already had an account associated with the selected digital wallet provider, a token may be provisioned to the existing account. If the user did not already have an account associated with the selected digital wallet provider, an account may be generated after which a token may be provisioned to the account associated with the digital wallet provider.

[0054] In an exemplary case, one of the selected participating resource providing entities may be a merchant. If the user already had an account associated with the selected merchant (e.g., account on file), a token may be provisioned to the existing account. If the user did not already have an account associated with the selected merchant, an account may be generated after which a token may be provisioned to the account associated with the merchant.

[0055] At step S3, the user may conduct a transaction utilizing a token provisioned to a selected participating resource providing entity. The selected

participating resource providing entity may be a digital wallet provider, as described in the exemplary case above. The user may utilize user device 10 to run an application hosted by the digital wallet provider. In some embodiments, the application may be a digital wallet application that enables contactless transactions. In some cases, the user may indicate to the application to utilize the provisioned token for the transaction. In other cases, information related to the token may be pre-filled by the application. User device 10 may then communicate account information including the token to access device 12 to conduct the transaction. As a result, the new account can be utilized to conduct a transaction with the digital wallet application instantly after issuance.

[0056] At step S4, the user may conduct another transaction utilizing a token provisioned to another selected participating resource providing entity. The selected participating resource providing entity may be a merchant, as described in the exemplary case above. In some embodiments, the user may utilize user device 14 to conduct the transaction utilizing the provisioned token. In some embodiments, user device 14 may run a website or application hosted by the merchant. In some cases, the user may indicate to the application or website to utilize the provisioned token for the transaction. In other cases, information related to the token may be pre-filled by the application or website. The user may then conduct the transaction with the merchant using the provisioned token. As a result, the new account can be utilized to conduct a transaction with the merchant instantly after issuance.

[0057] While exemplary cases in which the user operates user device 10 and user device 14 are described above, embodiments are not so limited. For example, the tokens may be provisioned for use by another secondary user (e.g., family member, employee, etc.). Based upon the selection of participating resource providing entities by the user, the secondary user may be able to conduct transactions utilizing tokens associated with the user's account with the selected participating resource providing entities.

[0058] Further, while exemplary cases in which the provisioned token are associated with a newly issued account, embodiments are not so limited. For example, the provisioned token may be for an existing account associated with the user. In this

case, the user may open an application associated with an authorization entity on user device 10, where the application may host the existing account. The user may indicate that they want to provision tokens associated with the existing account to a plurality of selected participating resource providing entities. For any of the selected participating resource providing entities with which no account or profile exists, an account or profile may be generated before a token is added to the generated account or profile. As a result, the user may control the provisioned tokens from the application associated with the authorization entity, while each of the selected resource providing entities may store the token for future use.

[0059] Embodiments of the invention may enable provisioning of tokens for various use cases, such as those shown in Table 1 below.

TABLE 1

Account from which tokens are issued	**Resource providing entity account to which tokens are provisioned**	**Use case description**
New Account	New Account/Profile	User signs up for new card and wants to add the new card to a new account/profile associated with a resource providing entity.
New Account	Existing Account/Profile	User signs up for new card and wants to add the new card to an existing account/profile associated with a resource providing entity.
New Account	Secondary User Account/Profile	User signs up for new card and wants to add the new card to a secondary user's account/profile (new or existing) associated with a resource providing entity.
Existing Account	New Account/Profile	User wants to add an existing card to a new account/profile associated with a resource providing entity.
Existing Account	Existing Account/Profile	User wants to add an existing card to an existing account/profile

		associated with a resource providing entity.
Existing Account	Secondary User Account/Profile	User wants to add an existing card to a secondary user's account/profile (new or existing) associated with a resource providing entity.

[0060] In some embodiments, the user may manage the provisioned tokens through an application (e.g., hosted by authorization entity) or a third party token portal. An exemplary user interface 300 is shown in FIG. 3. Activation of any of the user interface elements (e.g., buttons) of user interface 300 may open another user interface that enables the user to view data and configure setting associated with provisioned tokens. For example, activating the "History" button may enable the user to review historical information (e.g., historical transactions) for any of the provisioned tokens. Activating the "Suspend" button may enable the user to request to suspend use of any of the provisioned tokens. In an exemplary case, the user may indicate to suspend use (e.g., temporarily) of a provisioned token by a particular secondary user or a certain device. Activating "Delete" button may enable the user to request deletion of any of the provisioned tokens from the corresponding resource providing entity systems. Activating the "Controls" button may enable the user to configure and execute controls (e.g., spend controls, time limit controls, etc.) for the provisioned tokens. For example, the user may configure a provisioned token to be authorized for use with transactions below a certain transaction amount. Activating the "Alerts" button may enable the user to configure alert setting indicating when the user should receive an alert regarding the provisioned tokens. In an exemplary case, the user may configure alert setting so that an alert is sent when a provisioned token is utilized over a day for transactions that sum to greater than a certain transaction amount.

[0061] FIG. 4 illustrates an exemplary system 400 with at least some of the components for implementing embodiments of the invention. FIG. 4 includes a user 101, a user device 103 operating a service provider application 113, a resource provider computer 106, a transport computer 108, a processor server computer 110 in

communication with a token vault 116, an authorization computer 112, and a service provider computer 114. Any of the computing devices (e.g., user device 103, resource provider computer 106, transport computer 108, processor server computer 110, service provider computer 114, and authorization computer 112) in FIG. 1 may be in communication by any suitable communications network.

[0062] The communications network may comprise a plurality of networks for secure communication of data and information between entities. In some embodiments, the communications network may follow a suitable communication protocol to generate one or more secure communication channels between user device 103 and processor server computer 110. Any suitable communications protocol may be used for generating a communications channel. A communication channel may in some instance comprise a "secure communication channel," which may be established in any known manner, including the use of mutual authentication and a session key and establishment of an SSL session. However, any method of creating a secure channel may be used. By establishing a secure channel, sensitive information may be securely transmitted to facilitate a transaction.

[0063] A user 101 (which may also be known as a consumer) may be a cardholder operating user device 103. User 101 may select one or more resource providing entities (e.g., merchants, digital wallet services providers, service providers etc.) to which to provision tokens associated with an account. In some embodiments, the account may be an existing account associated with user 101. In other embodiments, user 101 may request generation of a new account (e.g., new card account) from authorization computer 112. In some embodiments, user 101 may utilize the provisioned tokens associated with the account with service provider application 113 or other platforms related to the selected one or more resource providing entities to conduct a transaction using user device 103.

[0064] User device 103 may be any suitable device to conduct a transaction. User device 103 may include a memory that may store service provider application 113 and may be utilized to conduct transactions using service provider application 113. User device 103 may communicate over a communications network with one or more

entities, including service provider computer 114 and processor server computer 110. User device 103 may be utilized in a card-not-present transaction, such as through a website hosted by a resource providing entity. In some embodiments, user device 103 may also be capable of communicating by contact or wirelessly with an access device at a payment terminal. In some embodiments, payment methods for the transactions may include eCommerce (electronic commerce), mCommerce (mobile commerce), In-app (purchases from within an application), NFC (near field communication), MST (Magnetic Secure Transmission™).

[0065] Some non-limiting examples of user device 103 may include mobile devices (e.g., cellular phones, keychain devices, personal digital assistants (PDAs), pagers, notebooks, laptops, notepads, smart watches, fitness bands, jewelry, etc.), automobiles with remote communication capabilities, personal computers, payment cards (e.g., smart cards, magnetic stripe cards, etc.), and the like. In some embodiments, user device 103 may be configured to communicate with one or more cellular networks.

[0066] Service provider application 113 may be accessible by user device 103. Service provider application 113 may be operated by service provider computer 114. In some embodiments, service provider application 113 may store a digital wallet and may include card account information associated with user 101. In some cases, the digital wallet may be a mobile wallet. Some exemplary service provider applications include a wallet application, a digital wallet application, a wallet provider application, a mobile wallet application, or the like.

[0067] Service provider computer 114 may issue a service provider account for a user. In some embodiments, service provider computer 114 may be associated with a service provider. In some cases, the service provider may be an application provider, which may be an entity that provides an application to a mobile device for use by a user. In some embodiments, the service provider may be a wallet provider computer and can provide a mobile wallet or payment application (e.g., wallet application) to the user device 103. Service provider computer 114 may operate a server computer that may send and receive messages to and from service provider application 113 on user device

103. The service provider account issued by service provider computer 114 may also be accessed by a website. In some embodiments, the service provider computer 114 may maintain one or more digital wallets for each user, and each digital wallet may be associated with payment data for one or more payment accounts. An example of a digital wallet may be Visa Checkout™. In some cases, the service provider may be known as a resource provider and service provider computer 114 may be known as a resource provider computer.

[0068] Resource provider computer 106 may be configured to receive and process transaction data. In some embodiments, the transaction data may be received from user device 103 or an access device in communication with user device 103. Resource provider computer 106 may engage in transactions, sell goods or services, or provide access to goods or services to the consumer. Resource provider computer 106 may accept transaction data in multiple forms and may use multiple tools to conduct different types of transactions. For example, resource provider computer 106 may sell goods and/or services via a website or application, and may accept payments over the Internet. Resource provider computer 106 may also be associated with a physical store that utilizes an access device that can receive transaction data from user device 103 for in-person transactions.

[0069] Transport computer 108 is typically a system for an entity (e.g., a bank) that has a business relationship with a particular merchant or other entity. Transport computer 108 may route an authorization request for a transaction to authorization computer 112 via processor server computer 110. In some cases, transport computer 108 may be known as an acquirer computer.

[0070] Processor server computer 110 may include data processing subsystems, networks, and operations used to support and deliver authorization services, and clearing and settlement services. An example of processor server computer 110 includes VisaNet®, operated by Visa®. Processor server computer 110 may include wired or wireless network, including the Internet. In some embodiments, processor server computer 110 may be a token service provider and may be in communciation with token vault 116, which may store tokens associated with accounts of user 101. In

some cases, processor server computer 110 may also be known as a payment processing server computer.

[0071] Token vault 116 may comprise any information related to tokens. For example, token vault 116 may store tokens associated with service provider application 113 and a mapping of the tokens to their associated accounts. Token vault 116 may comprise any sensitive information (e.g., account number) associated with the tokens. In some embodiments, processor server computer 110 may communicate with token vault 116 to de-tokenize a token. In some cases, token vault 116 may reside at processor server computer 110.

[0072] Authorization computer 112 may be a computer involved in authorization processes. In some embodiments, authorization computer 112 may be run by an entity that can issue accounts. When a transaction involves an account issued by authorization computer 112, authorization computer 112 may verify the account and respond with an authorization response message to transport computer 108 that may be forwarded to an access device, if applicable. Some systems may perform functions of both authorization computer 112 and transport computer 108.

[0073] Upon receiving a request from user 101 by user device 103 for a new account, authorization computer 112 may approve user 101 and prompt user 101 to select resource providing entities with which to utilize the new account. In some embodiments, authorization computer 112 may communicate with processor server computer 110 to request tokenization of the newly approved account. In some embodiments, authorization computer 112 may be an issuer computer associated with an authorizing entity (e.g., issuer bank) that issues a payment (credit/debit) card, account numbers or payment tokens utilized for the transactions.

[0074] At a later time (e.g., at the end of the day), a clearing and settlement process can occur between transport computer 108, processor server computer 110, and authorization computer 112.

[0075] Any of the computing devices (e.g., user device 103, resource provider computer 106, transport computer 108, processor server computer 110, service

provider computer 114, and authorization computer 112) may include a processor and a computer readable medium comprising code, executable by the processor for performing the functionality described herein.

[0076] Embodiments of the invention enable provisioning of tokens to resource providing entities. There are several configurations of systems and computers, such as those described in FIG. 4, that can be utilized to accomplish the provisioning of tokens. One exemplary case may comprise a one-to-many implementation and another exemplary case may comprise a one-to-one implementation, which are described in more detail below.

[0077] Embodiments of the invention may enable a one-to-many implementation in which an authorization computer may integrate with a plurality of resource providing entities through a single connection with a token provider, which may be a processor server computer. While not explicitly shown in FIG. 4, processor server computer 110 may be in communication with a plurality of resource providing entities participating in a tokenization program. Processor server computer 110 may provision tokens to the plurality of resource providing entities upon request by authorization computer 112. Descriptions with respect to FIG. 5 and FIG. 6 below describe an exemplary one-to-many implementation in further detail.

[0078] FIG. 5 shows a block diagram 500 of an exemplary system enabling a one-to-many implementation according to embodiments of the present invention. FIG. 5 includes a plurality of authorization computers 512 in communication with a processor server computer 510. In some embodiments, processor server computer 510 may be a token provider or token service provider. Each of authorization computers 512 may have similar characteristics to those described with respect to authorization computer 112 in FIG. 4. Processor server computer 510 may have similar characteristics to those described with respect to processor server computer 110 of FIG. 4.

[0079] Processor server computer 510 may be capable of communicating with a plurality of resource providing entities. In some cases, processor server computer 510 may provision tokens to any of the plurality of resource providing entities upon request by any of authorization computers 512. The resource providing entities may include

those associated with service provider computers 501, issuer digital wallet provider computers 502, third party digital wallet provider computers 503, merchant computers 504, and networked devices 505. Service provider computer 501 may be associated with any service providers that may store and utilize tokens for transactions. In some embodiments, service provider computers 501 may be provide services (e.g., Visa Checkout™) associated with processor server computer 510. Issuer digital wallet provider computers 502 may enable digital wallets for accounts issued by an authorization computer. Third party digital wallet provider computers 503 may be associated with third parties that provide digital wallets that may store a plurality of accounts. Digital wallets provided by issuer digital wallet provider computers 502 and third party digital wallet provider computers 503 may utilize tokens for transactions conducted with the digital wallets. Merchant computers 504 may be associated with a merchant, which may enable transactions to be conducted utilizing tokens. In some cases, merchant computers 504 may store accounts on file with information related to the tokens. Networked devices 505 may be any suitable devices that can communicate with other computing devices and may store data. In some embodiments, networked devices 505 may be known as IoT devices (Internet of Things devices), which may include wearable devices that can be utilized to conduct transactions with tokens.

[0080] In a one-to-many implementation, an exemplary process as shown in flow diagram 600 of FIG. 6 may be performed. FIG. 6 may include user device 601 in communication with an authorization computer 612, a processor server computer 610, and a resource provider computer 615. User device 601 may have similar characteristics to those described with respect to user device 103 in FIG. 4. Authorization computer 612 may have similar characteristics to those described with respect to authorization computer 112 of FIG. 4, as well as authorization computers 512 of FIG. 5. Processor server computer 610 may have similar characteristics to those described with respect to processor server computer 110 of FIG. 4 and processor server computer 510 of FIG. 5. Resource provider computer 615 may have similar characteristics to those described with respect to resource provider computer 106 of FIG. 4 and any of resource provider computers 501-505 of FIG. 5.

[0081] At step S61, user device 601 operated by a user may communicate with authorization computer 612. In some embodiments, user device 601 may run an application hosted by authorization computer 612. In other embodiments, user device 601 may run a browser for a website hosted by authorization computer 612. From within the application or browser, the user may send a request to provision tokens associated with their account (e.g., new or existing) to a plurality of selected resource providing entities. The resource providing entities may also be known as token requestors.

[0082] At step S62, authorization computer 612 may communicate with processor server computer 610 to request provisioning of the tokens. Processor server computer 610 may be a service provider that provides tokenization services. Processor server computer 610 may generate tokens for each of the plurality of resource providing entities.

[0083] At step S63, processor server computer 610 may communicate with resource provider computer 615. Resource provider computer 615 may be associated with a resource providing entity from the plurality of selected resource providing entities. In some cases, processor server computer 610 may send a token generated for the resource providing entity associated with resource provider computer 615 to resource provider computer 615. Prior to provisioning the token, an authentication process may be conducted between the user and resource provider computer 615. Various authentication methods may be utilized in the one-to-many implementation.

[0084] One type of authentication method may be straight through provisioning. In this case, existing integrations (e.g., Security Assertion Markup Language) between authorization computer 612 and processor server computer 610 may be leveraged. Processor server computer 610 may provide services that enable account creation and loading authentication information for resource providing entities. In an exemplary case, a service provided by processor server computer 610 may be Visa Checkout™. The user may access their Visa Checkout™ account through the application or website hosted by authorization computer 612 for authentication when requesting provisioning of the tokens.

[0085] Another exemplary authentication method for the one-to many implementation may utilize a pop-up display or the like. For example, when a user utilizes an application or website hosted by authorization computer 612 to request provisioning of tokens, a lightbox display may appear. The lightbox display may be pre-populated with some information related to the user. In some cases, the lightbox display may prompt the user to enter or create a password for an account or profile associated with resource provider computer 615 to which a token is to be provisioned.

[0086] At steps S64 and S65, resource provider computer 615 may send information confirming that the token was provisioned. In some embodiments, the information may be sent to authorization computer 612 via processor server computer 610. While FIG. 6 shows a single resource provider computer 615, it is understood that the authentication process and token provisioning process may be performed for each of the plurality of resource providing entities selected by the user.

[0087] The one-to-many implementation as described above also enables authorization computers to select preferences related to authentication through a single platform, which is convenient. This configuration of preference may occur at any time. For example, authorization computer 612 may login to their account hosted by a processor server computer 610. Authorization computer 612 may select channels (e.g., application, browser, etc.) for which to enable push provisioning of tokens. Authorization computer 612 may further select authentication methods that are supported (e.g., Visa Checkout™, lightbox display, etc.). Authorization computer 612 may view a list of all resource providing entities (e.g., token requestors) that are compatible for push provisioning of tokens based on the selected channels and authentication methods. In some embodiments, authorization computer 612 may also view other information, such as reasons as to why some resource providing entities cannot be supported for push provisioning (e.g., incompatible channel or authentication method). The one-to-many implementation may enable authorization computers to "opt-in" for tokenization programs easily without having to interface with multiple resource providing entities.

[0088] In some embodiments, processor server computer 610 may determine and compare authentication methods and authentication channels supported by authorization computer 612 and those supported by a resource providing entity to determine whether the resource providing entity is to be provided to the user for selection. If the compared authentication methods and authentication channels match for an authorization computer and a resource providing entity match, processor server computer 610 may notify authorization computer 612 of the resource providing entity. Subsequently, authorization computer 612 may then prompt the user with a list of participating resource providing entities including the resource providing entity. In some embodiments, this comparison process may be conducted for each of the participating resource providing entities in the list of participating resource providing entities.

[0089] Embodiments of the invention may also enable another type of implementation, which may be known as a one-to-one implementation. A one-to-one implementation may enable an authorization computer to integrate directly with resource providing entities on an individual basis. For example, an authorization computer may enable token provisioning to each resource providing entity separately based on a standard (e.g., associated with a processor server computer) or proprietary APIs (e.g., push provisioning API). FIG. 7 and Fig. 8 below describe an exemplary one-to-one implementation in further detail.

[0090] FIG. 7 shows a block diagram 700 of an exemplary system enabling a one-to-one implementation according to embodiments of the present invention. FIG. 7 includes an authorization computer 710, an authorization computer 711, and an authorization computer 712. Each of authorization computers 710, 711, and 712 may have similar characteristics to those described with respect to authorization computer 112 in FIG. 4. FIG. 7 also includes a resource provider computer 720, a resource provider computer 721, and a resource provider computer 722. Each of resource provider computers 720, 721, and 722 may have similar characteristics to those described with respect to resource provider computer 106 of FIG. 4. Only three authorization computer and three resource provider computers are shown in FIG. 7 for simplicity. However, embodiments are not so limited and any suitable number of

authorization computers and resource provider computers may exists in a one-to-one implementation.

[0091] In a one-to-one implementation as shown in FIG. 7, each authorization computer may integrate directly with each resource provider computer (e.g., token requestor). Thus, an intermediary entity, such as a processor server computer, that handles all tokenization may be not present. This may provide the ability for integration with each resource provider computer to be performed based on either a standard (e.g., associated with a processor server computer) or proprietary push provisioning APIs specific to the resource provider computer.

[0092] In a one-to-one implementation, an exemplary process as shown in flow diagram 800 of FIG. 8 may be performed. FIG. 8 may include user device 801 in communication with an authorization computer 812, a resource provider computer 815, and a processor server computer 810. User device 801 may have similar characteristics to those described with respect to user device 103 in FIG. 4. Authorization computer 812 may have similar characteristics to those described with respect to authorization computer 112 of FIG. 4, as well as any of authorization computers 710-712 of FIG. 7. Processor server computer 810 may have similar characteristics to those described with respect to processor server computer 110 of FIG. 4. Resource provider computer 815 may have similar characteristics to those described with respect to resource provider computer 106 of FIG. 4 and any of resource provider computers 720-722 of FIG. 7.

[0093] At step S81, user device 801 operated by a user may communicate with authorization computer 812. In some embodiments, user device 801 may run an application hosted by authorization computer 812. In other embodiments, user device 801 may run a browser for a website hosted by authorization computer 812. From within the application or browser, the user may send a request to provision tokens associated with their account (e.g., new or existing) to a plurality of selected resource providing entities. The resource providing entities may also be known as token requestors.

[0094] At step S82, authorization computer 812 may communicate with resource provider computer 815 to request provisioning of a token to resource provider computer 815. Resource provider computer 815 may be associated with a resource providing entity from the plurality of resource providing entities selected by the user. In some embodiments, an authentication process may be performed between the user and resource provider computer 815.

[0095] One type of authentication method may comprise redirecting the user to a channel associated with the resource providing entity. For example, the user may be redirected from the application or browser hosted by authorization computer 812 to an application or website hosted by resource provider computer 815. In some embodiments, a page may be displayed prompting the user for information to complete account creation or the authentication process. For example, the user may create or enter a password to be utilized with their account or profile hosted by resource provider computer 815.

[0096] Another type of authentication method may comprise sending a message to enable a secondary user to login or create an account with the resource providing entity. For example, in some cases, the user may want to provision a token to a secondary user's account (e.g., family member's account, employee's account, etc.). In some embodiments, the user may enter an channel identifier (e.g., email address, phone number, etc.) associated with the secondary user, and authorization computer 812 may send a message to the secondary user through a channel (e.g., email, text message, etc.) associated with the channel identifier. The message may include a link that may direct the secondary user to an application or website hosted by resource provider computer 815, which may prompt the secondary user to input information to login or create an account. For example, the secondary user may create or enter a password to be utilized with their account or profile hosted by resource provider computer 815.

[0097] At step S83, resource provider computer 815 may request a token from processor server computer 810. In some cases, resource provider computer 815 may confirm to processor server computer 810 that the user or secondary user was

authenticated based on information provided by the user before the token can be generated.

[0098] At step S84, processor server computer 810 may generate and provision a token to resource provider computer 815. Processor server computer 810 may generate a token meant for use with resource provider computer 815 and send it to resource provider computer 815.

[0099] At step S85, resource provider computer 815 may send information confirming that the token was provisioned. In some embodiments, the user may be redirected back to the application or website hosted by authorization computer 812. While FIG. 8 shows a single resource provider computer 815, it is understood that the authentication process and token provisioning process may be performed for each of the plurality of resource providing entities selected by the user. In the one-to-one implementation, each authentication process performed may be specific to each resource provider computer.

[0100] FIG. 9 through FIG. 12 show flow diagrams for exemplary methods that may be performed according to embodiments of the invention. However, it is understood that additional methods and processes may be included within these methods and may be recognized by one of ordinary skill in the art, in light of the description below. Further, in some embodiments of the present invention, the described methods may be combined, mixed, and matched, as one of ordinary skill would recognize.

[0101] For example, certain steps described in FIG. 9 and FIG. 12 can be modified to enable a different use case according to embodiments of the invention. For example, while FIG. 9 and FIG. 12 are directed to provisioning account information associated with newly issued card accounts, similar processes may be applied for existing card accounts. In this case, the steps for applying for a new card may be omitted. Instead, the flow may start with the user device of the user running an application or browser hosted by authorization computer 912, which may already store information for an existing account.

[0102] A method according to the embodiments of the invention can be described with respect to FIG. 9 FIG. 9 shows a flowchart 900 of a method for enabling a user immediate card access upon approval and token provisioning to resource providing entities according to embodiments of the invention. FIG. 9 includes a user device 903 operated by a user, a resource provider computer 906 associated with a resource providing entity, processor server computer 910, authorization computer 912 associated with an authorizing entity, and service provider computer 914. In some embodiments, authorization computer 912 may also be known as an issuer computer, service provider computer 914 as a digital wallet provider, and resource provider computer 906 as a merchant computer. In some cases, the user may have an account on file with resource provider computer 906. Processor server computer 910 may also be a token service provider.

[0103] At step 1, resource provider computer 906 may send a request to processor server computer 910 to sign up for tokenization. This sign up process may be conducted at any time prior to a transaction. The resource providing entity associated with resource provider computer 906 may request processor server computer 910 to participate in tokenized transactions, in which a user may utilize a token when making a payment with the resource providing entity. Upon receiving the request, processor server computer 910 may store information indicating the resource providing entity as a participating resource providing entity.

[0104] At step 2, the user may apply for a new card account using their user device 903. In some embodiments, the user may receive a promotion (e.g., by email, text message, etc.) to create a new card. The promotion may include a link which the user may activate to initiate a request for the new card. The user may activate the link (e.g., by clicking the link), which may launch an application (e.g., banking application) on user device 903. In some embodiments, the application may be hosted by authorization computer 912. The application may display a user interface requesting the user to enter information to be utilized to create the new card account with the authorizing entity associated with authorization computer 912. The user may enter the user information into user device 903.

[0105] At step 3, user device 903 may send a request for the new card account including the information entered by the user to authorization computer 912. In some embodiments, the information may include user information, such as name, address, and other contact information associated with the user.

[0106] At step 4, authorization computer 912 may approve the user based on the entered information. If authorization computer 912 approves the user, authorization computer 912 may issue the new card to the user. Authorization computer 912 may generate card account information for the new card requested by the user. In some embodiments, the card account information may include an account identifier (e.g., account number), an expiration date, a card verification value (CVV), and other transaction information that may be utilized for a transaction.

[0107] At step 5, authorization computer 912 may send the card account information for the new card and the user information to processor server computer 910. The information may be sent in any suitable manner, such as by an electronic message sent over a communications network. Processor server computer 910 may be a token service provider.

[0108] At step 6, processor server computer 910 may notify authorization computer 912 about a list of the participating resource providing entities that signed up for tokenization. In this exemplary case, resource provider computer 906 and service provider computer 914 may be associated with participating resource providing entities. In some embodiments, resource provider computer 906 may also be known as a merchant computer and service provider computer 914 may also be known as a digital wallet provider computer. Additionally, in some embodiments, processor server computer 910 may notify authorization computer 912 about a list of entities with preexisting tokens and thus already have an account on file associated with the user. This may enable instant association with preexisting tokens associated with the user.

[0109] At step 7, authorization computer 912 may prompt the user to make a selection from the participating resource providing entities with which utilize the new card. For example, authorization computer 912 may prompt the user using a user interface (e.g., including a list, tile options, etc.) displayed on user device 903 including

the participating resource providing entities that are signed up for tokenization. In some embodiments, authorization computer 912 may also provide pre-selected resource providing entities that correspond to those resource providing entities with which the user already has an account (e.g., token) on file. However, the user may deselect any of the pre-selected resource providing entities if the user does not desire to utilize their new card with any of the pre-selected resource providing entities. Thus, the resource providing entities options provided to the user may be those with which the user may or may not already have an account on file. While FIG. 9 shows authorization computer 912 communicating directly with user device 903, embodiments are not so limited. For example, authorization computer 912 may send communications indirectly to user device 903 through another computer (e.g., processor server computer 910).

[0110] At step 8, the user may select one or more resource providing entities from the received list. The selection may be indicated by any suitable interaction with the user interface displayed on the user device of the user. For example, the user may confirm their selection by clicking on software or hardware buttons (e.g., checkboxes, tiles, etc.), inputting a voice command, or other suitable methods. In an exemplary case, the user may select a resource providing entity associated with resource provider computer 906 and a resource providing entity associated with service provider computer 914. While the exemplary case in which the user selects two resource providing entities is described in flowchart 900, in other embodiments, the user may select any suitable number of resource providing entities. User device 903 may send the selection of the one or more resource providing entities to processor server computer 910 with a request to issue tokens associated with the account of the user to the selected one or more resource providing entities

[0111] In some embodiments, processor server computer 910 may verify communications sent from user device 903 in step 8. Processor server computer 910 may conduct a verification process based on information related to the user operating user device 903 or user device 903. For example, user device 903 may send an identifier (e.g., transaction identifier) along with the selection of one or more resource providing entities in step 8. In some cases, the identifier may be generated by user

device 903 or authorization computer 912 hosting the application on user device 903. In some embodiments, the identifier may be generated based on any combination of a device identifier, timestamp, user information, IP address, or other information. Processor server computer 910 may check whether the identifier received from user device 903 in step 8 matches an identifier received previously from user device 903 (e.g., at step 3) or authorization computer 912 (e.g., at step 5).

[0112] At step 9, processor server computer 910 may tokenize the new card. Processor server computer 910 may generate one or more tokens associated with the account of the new card that may be utilized for transactions by the user. Processor server computer 910 may be in communication with a token vault, which may store the one or more tokens, a mapping between the one or more tokens and the account of the new card issued to the user, and any other information related to the token. During a transaction, processor server computer 910 may receive the one or more tokens and may de-tokenize the tokens based on information in the token vault, so that the transaction can be applied to the appropriate account associated with the token.

[0113] Processor server computer 910 may determine a token for each selected resource providing entity. Determining a token may comprise generating a token or identifying a token, if the token has been pre-generated. For example, processor server computer 910 may determine a first token to be provisioned to service provider computer 914 and a second token to be provisioned to resource provider computer 906. Both the first token and the second token may be associated with the newly issued card by authorization computer 912. In the exemplary flowchart 900, the user may already be enrolled with service provider computer 914 and may have an account on file with resource provider computer 206.

[0114] At step 10, processor server computer 910 may send the user information and the first token to service provider computer 914. Service provider computer 214 may be associated with a wallet provider selected by the user and that is supported by the authorizing entity associated with authorization computer 912. The user information and the first token may be sent in any suitable manner, such as by an electronic message sent over a communications network.

[0115] At step 11, service provider computer 914 may authenticate the user. In some embodiments, service provider computer 914 may conduct an authentication process with backend processing without requesting input from the user, such as checking whether the received user information matches information associated with the user already stored in its systems. Further details regarding exemplary authentication processes are described with respect to FIG. 6 above.

[0116] At step 12, service provider computer 914 may store the received user information and the first token. Service provider computer 914 may store the first token such that it is associated with the newly issued card and the user information. Hence, the first token may be provisioned directly from the mobile banking application operated by the user to service provider computer 914.

[0117] At step 13, processor server computer 910 may send the user information and the second token to resource provider computer 906. Resource provider computer 906 may be associated with the resource providing entity (e.g., merchant) selected by the user. The user information and the second token may be sent in any suitable manner, such as by an electronic message sent over a communications network.

[0118] At step 14, resource provider computer 906 may authenticate the user. In some embodiments, resource provider computer 906 may conduct an authentication process with backend processing without requesting input from the user, such as checking whether the received user information matches information associated with the user already stored in its systems. Further details regarding exemplary authentication processes are described with respect to FIG. 6 above.

[0119] At step 15, resource provider computer 906 may store the received user information and the second token. Resource provider computer 906 may store the second token such that it is associated with the newly issued card and the user information. Hence, the second token may be provisioned directly from the mobile banking application operated by the user to resource provider computer 906. In some embodiments, the second token may also be stored in association with other accounts on file (e.g., including preexisting tokens) that the user has with resource provider computer 906.

[0120] In some embodiments, steps 10 through 12 and steps 13 through 15 described above may be initiated at the same time or in a different order than as shown in flowchart 900. For example, processor server computer 910 may send information in step 13, followed by steps 14 and 15, to resource provider computer 906 before sending information in step 10, flowed by steps 11 and 12, to service provider computer 914, or may send information to resource provider computer 906 and service provider computer 914 at the same time.

[0121] At step 16, the user may utilize their user device 903 to conduct transactions with their newly provisioned tokens. For example, the user may access their digital wallet (e.g., by a wallet application) associated with service provider computer 914 and utilize the first token with the digital wallet to make a purchase. Additionally, the user may access an online website associated with resource provider computer 906 and utilize the second token to make another purchase. In subsequent purchases, the user may utilize the first token and second token. Hence, the tokens can be provisioned when the card is issued, which can enable the user to immediately access and utilize the tokens for transactions, including with account on file merchants. This is efficient, takes minimal effort by the user, and provides more flexibility for the user. Further, the use of tokenization enables security of the transactions since sensitive data is masked.

[0122] A concrete example of a case in which the steps of flowchart 900 may be performed is provided below. A user may be operating a user device and may receive a promotion for a new card by email. The user may click on the promotion, which can launch their mobile banking application on their user device. The user may enter user information to apply for the new card and send to an issuer hosting the application by pressing an “Apply” button. The issuer may approve the user and the new card may be issued to the user.

[0123] Subsequently, the user may be prompted to add their newly issued card (e.g., tokens) to participating resource providing entities. The user may be presented with a user interface including a list of resource providing entity names (e.g., vendors, retailers, digital wallet providers, etc.). The user may select one or more resource

providing entities by clicking on the one or more resource providing entities indicated on the list. The user may select a digital wallet provider and a merchant, with which the user may already have accounts. A first token may be generated and pushed to the user's digital wallet provider account associated with the selected digital wallet provider and a second token may be generated and pushed to the user's merchant account associated with the selected merchant.

[0124] The provisioned tokens may then be available for immediate use by the user. For example, the user may go to a store to purchase a beverage. The user may utilize their digital wallet provider account with their user device to pay for the beverage with the account of their newly issued card. Additionally, the user may shop online with their merchant account using the same user device or another device. When the user checks out to make a purchase, the newly issued card may already be provisioned such that the user may select it from a list including other accounts on file that the user has with the merchant. In other cases, the account information (e.g., token) may be pre-filled on the checkout page. Subsequently, the user may then utilize the newly issued card to pay for the purchase.

[0125] As described above, the user may utilize their new card for transactions conducted at physical POS (point-of-sale) terminal, as well as transactions conducted remotely. For example, the user may pay for a transaction using their new card by a contactless transaction with an access device at a merchant. Additionally, the user may pay for an e-commerce transaction using their new card account. Hence, the user device may be any suitable device that may be capable of conducting both types of transactions. Some exemplary payment methods may include eCommerce (electronic commerce), mCommerce (mobile commerce), In-app (purchases from within an application), NFC (near field communication), and MST (Magnetic Secure Transmission™).

[0126] As indicated above with respect to the description related to FIG. 9, embodiments of the invention enable multiple tokens to be provisioned to multiple resource providing entities. However, it is understood that FIG. 9 depicts one exemplary case in which two tokens were provisioned to two resource providing entities

and is not limiting. For example, embodiments of the invention enable one or more tokens to be provisioned one or more resource providing entities. In some embodiments, more than one token may be provisioned to a single resource providing entity.

[0127] While the description related to FIG. 9 above describes one exemplary use of the invention, embodiments are not so limited. For example, embodiments of the invention can also be utilized to provision a token related to a user's existing cards, rather than just newly issued cards. Further, tokens (e.g., associated with a user's existing cards and newly issued card) can be provisioned to resource providing entities that may be participating in a tokenization program, which may not be account on file merchants. Thus, tokens may be utilized for a variety of transaction types (e.g., recurring, one-time, on-demand, etc.). In some embodiments, tokens may also be pushed to other devices indicated by the user (e.g., mobile devices, tablets, wearable devices, etc.).

[0128] Embodiments of the invention may provide a number of advantages. For example, embodiments of the invention increase efficiency as a user no longer needs to wait to receive a plastic card in order to utilize a new card account and can have a new card immediately available, with minimal user input, on their mobile device once approved by an issuer. This forgoes the need for the user to manually set up accounts with multiple resource providing entities, which can be repetitive and cumbersome. In some cases, embodiments of the invention may enable users to be inclined to utilize their new card with new resource providing entities including digital wallet services and merchants, in addition to resource providing entities with which the user may already have an account on file, since tokens for the newly issued card can be easily provisioned with minimal user effort. Additionally, embodiments of the invention enable users to proactively create, view, and manage their tokens, which gives them control, security, flexibility, and the ability to better track their credentials. Regarding the processor server computer, embodiments of the invention also provide advantages. For example, leveraging the ability of token services provided by a processor server

computer forgoes the need to build and manage any token vault by a third party, which may not be as efficient and secure.

[0129] Descriptions corresponding to FIGs. 10-12 below describe exemplary methods according to embodiments of the invention and are not limiting. For example, while the descriptions describe provisioning tokens to a service provider computer, which may be a digital wallet provider, embodiments are not so limiting. Similar processes can be performed with any resource provider computer associated with a resource providing entity (e.g., merchant, digital wallet provider, service provider, etc.). For example, the service provider computer in any of the FIGs. 10-12 can be replaced with a resource providing computer.

[0130] A method according to the embodiments of the invention can be described with respect to FIG. 10. FIG. 10 shows a flowchart 1000 of a method for enabling a user immediate card access upon approval according to embodiments of the present invention and includes a user 201, a processor server computer 210, an authorization computer 212 associated with an authorizing entity, and a service provider computer 214. In some embodiments, processor server computer 210 may also be a token service provider. Any communications sent to and received from user 201 may be through a user device, such as user device 103 of FIG. 4, operated by user 201. In some embodiments, processor server computer 210 may also be known as a payment processor server computer or payment processing network, authorization computer 21 2 may also be known as an issuer computer, and service provider computer 214 may also be known as a resource provider computer. In the exemplary case described below, service provider computer 214 may be a wallet provider computer

[0131] At step 1, user 201 applies for a new card using their user device. For example, user 201 may be shopping online on a merchant website using their user device and may see an advertisement showing that conducting a checkout process with a card issued by the issuer associated with authorization computer 212 will give user 201 a discount. User 201 may click on the advertisement, redirecting user 201 to a website associated with the authorizing entity and hosted by authorization computer 212. The website may display a user interface requesting user 201 to enter information

to be utilized to create the new card with the issuer. User 201 may enter the information, which may be forwarded to authorization computer 212. In some embodiments, the information may include a user data (e.g., name, address, contact information, etc.).

[0132] At step 2, authorization computer 212 may approve user 201 based on the entered information. If authorization computer 212 approves user 201, authorization computer 212 may issue the new card to user 201. Authorization computer 212 may generate card information for the new card requested by user 201. In some embodiments, the card information may include an account identifier (e.g., account number), other account information (e.g., expiration date, CVV, etc.), and transaction information that may be utilized for a transaction. Card information may also be known as account information or card account information.

[0133] At step 3, authorization computer 212 may send the card information for the new card to processor server computer 210. In addition to the card information, authorization computer 212 may send cardholder information, cardholder contact information, and any additional future processing instructions. An example of a future processing instruction may be an instruction to not validate the consumer address when the consumer creates their account. The card information and additional information may be sent in any suitable manner, such as by an electronic message sent over a communications network. Processor server computer 210 may be a token service provider.

[0134] At step 4, processor server computer 210 may activate an account associated with the new card and may tokenize the new card. For example, processor server computer 210 may generate a token associated with the account of the new card that may be utilized for a transaction by user 201. Processor server computer 210 may be in communication with a token vault, which may store the token, a mapping between the token and the account of the new card issued to user 201, and any other information related to the token. During a transaction, processor server computer 210 may receive the token and may de-tokenize the token based on information in the token vault so, that the transaction can be applied to the appropriate account associated with the token.

[0135] At step 5, processor server computer 210 may send token information, which may be any information related to the token generated by processor server computer 210, to authorization computer 212. The token information may be sent in any suitable manner, such as by an electronic message sent over a communications network. In some embodiments, processor server computer 210 may also send authorization computer 212 an access link along with the token information. For example, the access link may be a link that can redirect user 201 using their user device to a website or application hosted by processor server computer 210.

[0136] At step 6, in some embodiments, authorization computer 112 may send a confirmation that the token information was received from processor server computer 210. In some embodiments, authorization computer 212 may send user information received in step 1 to processor server computer 210. In other embodiments, the user information may be sent with card information in step 3 or other appropriate step.

[0137] At step 7, authorization computer 212 may prompt user 201 to select wallet providers to utilize with the new card. For example, authorization computer 212 may prompt user 201 by a user interface (e.g., including a list, tile options, etc.) displayed on the user device of user 201. Authorization computer 212 may provide user 201 options to select wallet providers that are supported for use with the new card issued by the issuer associated with authorization computer 212. In some embodiments, user 201 may already be enrolled with one or more of the provided wallet providers. In other embodiments, user 201 may not be enrolled with one or more of the provided wallet providers.

[0138] At step 8, user 201 may select a wallet provider from the options provided by authorization computer 212. The selection may be indicated by any suitable interaction with the user interface displayed on the user device of user 201. For example, user 201 may confirm their selection of the wallet provider by clicking on a software or hardware button, inputting a voice command, or other suitable methods. While an exemplary case in which user 201 selects a single wallet provider is described in flowchart 1000 for simplicity, in some embodiments, user 201 may select multiple wallet providers from the provided options for which to utilize with the new card.

[0139] After user 201 selects the wallet provider, authorization computer 212 may redirect user 201 to processor server computer 210, so that the new card may be enrolled in the selected wallet provider. The redirection may be implemented in any suitable manner. For example, in one implementation, upon user 201 confirming their selection of the wallet provider, authorization computer 212 may redirect user 201 based on the access link provided by processor server computer 210 to authorization computer 212 in step 5. In another implementation, authorization computer 212 may embed the access link in a button clicked on by user 201 to confirm the selection of the wallet provider. The access link may be activated when the button is clicked by user 201, redirecting user 201 to a website hosted by processor server computer 210.

[0140] Processor server computer 210 may display, to user 201 by their user device, information that will be utilized to enroll the new card with the selected wallet provider. For example, the information may be user information and token information associated with the new card. Processor server computer 210 may request user 201 to validate the information before enrolling the new card with the wallet provider. For example, user 201 may check whether the displayed information is accurate and then may confirm to that the information is valid. User 201 may indicate the confirmation by clicking on a software or hardware button, inputting a voice command, or other suitable methods. In some embodiments, user 201 may validate the information prior to selecting the wallet provider.

[0141] At step 9, after user 201 validates the information, processor server computer 210 may send user information and token information to service provider computer 214. Service provider computer 214 may be associated with the wallet provider selected by user 201 and that is supported by the issuer associated with authorization computer 212. The user information and token information may be sent in any suitable manner, such as by an electronic message sent over a communications network.

[0142] At step 10, service provider computer 214 may store the received information in its local systems. Based on the received information, service provider computer 214 may determine whether user 201 has an existing account with service

provider computer 214. For example, service provider computer 214 may check whether any existing account including the received user information (e.g., name, address, etc.) is stored in its systems.

[0143] At step 11, in some embodiments, service provider computer 214 may notify processor server computer 210 that the received information was stored. In some embodiments, service provider computer 214 may also notify whether user 201 has an existing account with service provider computer 214.

[0144] At step 12, service provider computer 214 may prompt user 201 to provide wallet provider account information. If service provider computer 214 determines that user 201 does not have an existing account, service provider computer 214 may prompt user 201 to create a new account. For example, service provider computer 214 may prompt user 201 to create a new username, password, and enter any other registration information (e.g., contact information) to generate the new account.

[0145] At step 13, in response to the prompt from service provider computer 214, user 201 may enter the wallet provider account information. If user 201 is creating a new account with service provider computer 214, user 201 may enter a new username, password, and enter any other registration information to generate the new account.

[0146] At step 14, service provider computer 214 may create a wallet provider account for user 201. The account may be associated with the registration information entered by user 201. Further, service provider computer 214 may link the new account to the token received by processor server computer 210 and associated with the new card issued by authorization computer 212. This can enable user 201 to utilize the newly issued card with their wallet provider account.

[0147] In other embodiments, user 201 may already have an existing account with service provider computer 214. In this case, at step 12, service provider computer 214 may simply prompt user 201 for a registered username and password. Further at step 13, if user 201 already has an existing account with service provider computer 214, user 201 may enter their registered username and password into a user interface on their user device to log in to their existing account. At step 14, service provider

computer 214 may link the existing account to the token received by processor server computer 210 and associated with the new card issued by authorization computer 212.

[0148] At step 15, user 201 may conduct the checkout process on the merchant website using their newly issued card. User 201 may receive the advertised discount on their transaction. Hence, user 201 may request a new card and immediately may be able to utilize the newly issued card with a digital wallet for the transaction.

[0149] While the embodiments above describe the user device of user 201 being utilized for remote transactions (e.g., e-commerce transaction, online transaction, etc.), embodiments are not so limited. For example, embodiments of the invention may be extended to transactions that are conducted at a physical POS terminal, in which a similar flow to that of FIG. 10 may be utilized. After user 201 requests a new card, which is then approved and linked to a digital wallet, user 201 may utilize the new card at the POS terminal. For example, user 201 may pay for a transaction using their new card by a contactless transaction with an access device at a merchant. Hence, the user device of user 201 may be any suitable device that may be capable of conducting either type of transaction.

[0150] As described above, in some embodiments, user 201 may select multiple wallet providers from the provided options for which to utilize with the new card. In this case, for each service provider selected by user 201, processor server computer 210 may send user information and token information to a wallet provider computer associated with each selected wallet provider. Additionally, each wallet provider computer that receives information from processor server computer 210 may perform steps 10-12, receive information from user 201 at step 13, and further perform step 14. Thus, the token associated with the newly issued card may be provisioned to multiple digital wallets of user 201, which may be immediately available for use by user 201.

[0151] A concrete example of a case in which the steps of flowchart 1000 may be performed is provided below. A user may be shopping at an online website of a merchant, where the website displays an advertisement that offers a discount of 25% off of the user's transaction if the user utilized a card issued by issuer. The user may click the advertisement and apply for a new card with the issuer, which may approve the user

and send card account information to a processor server computer. The processor server computer, which may also be a token service provider, may tokenize the card (e.g., generate a new token) and send token information to the issuer computer associated with the issuer along with a link routed to the token service of the token service provider. Subsequently, the issuer computer may send the user the link.

[0152] The token service may then validate the user and ask the user with which wallet they would like to enroll. The user may select a wallet provider, such as Visa Checkout™, triggering the token service to send token information to a server associated with Visa Checkout™. The merchant may accept Visa Checkout™ transactions. The Visa Checkout™ server may then prompt the user to create a new Visa Checkout™ account or log in to an existing Visa Checkout™ account. Subsequently, the new token may be provisioned to the user's Visa Checkout™ account. The user may then conduct the transaction with the merchant using the newly issued card account with Visa Checkout™ and receive the advertised 25% discount.

[0153] Another use case according to embodiments of the invention is described below. A user may be at a mall and may see an advertisement to utilize a card issuer by a certain issuer for rewards (e.g., gaining loyalty points). The user may open a wallet provider application on their mobile device. The wallet provider application may allow the user to enroll with issuers. Accordingly, the wallet provider application may collect user information from the user and send it to the issuer computer associated with the issuer indicated in the advertisement. The issuer may approve the user and send new account information to a processor server computer, which may also be a token service provider. The processor server computer may tokenize the card, and send a token back to the issuer computer. The issuer computer may send the token to the wallet provider and the wallet provider may provision the token on the user's mobile device. The user can then utilize the mobile device for a checkout process with the advertised rewards applied. Hence, the card may be made available on the mobile device immediately after approval by the issuer.

[0154] In some embodiments, tokenization of card account information may not be performed. For example, in the case of flowchart 1000 of FIG. 10, steps 3 through 6

may be omitted. In subsequent steps (e.g., step 9), an account number may be sent instead of a token. Even with the omission of tokenization, the user may still be able to utilize the newly issued card immediately after approval by the issuer. However, tokenization may provide security benefits, since a token may not be easily linked to an actual account, except by a token provider service.

[0155] A method according to the embodiments of the invention can be described with respect to FIG. 11. FIG. 11 shows a flowchart 1100 of a method for enabling a user immediate card access upon approval according to embodiments of the present invention and includes a user 301, a browser 302, an authorization computer 312 associated with an authorizing entity, a processor server computer 310, and a service provider computer 314. In some embodiments, processor server computer 310 may also be a token service provider enabling a tokenization program. Any communications sent to and received from user 301 may be through a user device, such as user device 103 of FIG. 4. The user device may run browser 302. In some embodiments, processor server computer 310 may also be known as a payment processor server computer or payment processing network, authorization computer 312 may also be known as an issuer computer, and service provider computer 314 may also be known as a resource provider computer. In the exemplary case described below, service provider computer 314 may be a wallet provider computer.

[0156] At step 1, user 301 may activate a card. User 301 may enter user data into their user device, which sends the entered user data to authorization computer 312. Authorization computer 312 may approve user 301 based on the entered information. If authorization computer 312 approves user 301, authorization computer 312 may issue the new card to user 301. Authorization computer 312 may generate card information for the new card requested by user 301. In some embodiments, the card information may include an account identifier (e.g., account number), other account information (e.g., expiration date, CVV, etc.), and transaction information that may be utilized for a transaction. Card information may also be known as account information or card account information.

[0157] At step 2, authorization computer 212 may enroll the user data in the tokenization program and by sending the user data and the card information for the new card to processor server computer 210. The user data may include cardholder information and cardholder contact information. In addition to the user data and card information, authorization computer 212 may send any additional future processing instructions. An example of a future processing instruction may be an instruction to not validate the consumer address when the consumer creates their account. The user data, card information, and additional instructions may be sent in any suitable manner, such as by an electronic message sent over a communications network.

[0158] At step 3, processor server computer 310 may store the received user data and card information and activate an account of user 301. The received user data and card information may be stored in association with user 301, such as in a data record for the account of user 301.

[0159] At step 4, processor server computer 310 may enroll the new card in the tokenization program. Processor server computer 310 may generate a token and token identifier for the new card. A token identifier may be a reference to a card account or token. In some embodiments, the token identifier may be specific to a wallet provider or may be a generic identifier that points to an account number. In some embodiments, processor server computer 310 may also generate card art for the new card.

[0160] At step 5, processor server computer 310 may generate links to wallet providers (WP links). In some embodiments, the links may be custom wallet provider links. The wallet providers for which processor server computer 310 generates links may be those which are supported by authorization computer 312.

[0161] At step 6, processor server computer 310 may send a response to authorization computer 312. The response may include the token identifier, any generated links to wallet providers, card art and other information helpful to authorization computer 312. In some embodiments, sending multiple wallet provider links may be optional.

[0162] At step 7, authorization computer 312 may deliver the token identifier and wallet provider links to user 301. In some embodiments, the wallet provider links may be provided in a user interface prompting user 301 to choose a wallet provider corresponding to one of the provided wallet provider links.

[0163] At step 8, user 301 may access the selected link received from authorization computer 312. User 301 may be able to select a link by clicking the link or a software button with the embedded link. While a case in which a single link is selected is described in this flow, in other cases, user 301 may select more than one link. In some embodiments, the selected link may be associated with service provider computer 314.

[0164] At step 9, in response to user 301 accessing the link, user 301 may be directed to browser 302. Browser 302 may open a website or application hosted by service provider computer 314.

[0165] At step 10, user 301 may visit the website or application hosted by service provider computer 314. At the backend, browser 302 may request any information utilized to run the website or application from service provider computer 314. For example, the information may include user interface components, instructions, or other information.

[0166] At step 11, service provider computer 314 may return the requested information to browser 302. This may enable browser 302 to display an appropriate page, such as a log in page, to user 301.

[0167] At step 12, user 301 may be prompted to log in to their account with service provider computer 314 by browser 302. User 301 may enter verification attributes into the user interface displayed by browser 302. The verification attributes may include a username, password, and the token identifier, which may then be transmitted to service provider computer 314 at step 13.

[0168] At step 14, service provider computer 314 may call processor server computer 310 to pull user data associated with user 301 and the newly issued card. For example, processor server computer 310 may open Application Programming Interfaces

(APIs) to enable service provider computer 314 to pull data, which may include cardholder information, payment account information, and cardholder contact information. In some embodiments, service provider computer 314 may utilize the APIs to request processor server computer 310 to retrieve certain data. For example, service provider computer 314 may provide the token identifier to processor server computer 310 and request from processor server computer 310 the token associated with the account of user 301. Thus, instead of processor server computer 310 pushing data to service provider computer 314, such as described in FIG. 10, flowchart 1100 shows service provider computer 314 calling APIs of processor server computer 310 to obtain information.

[0169] At step 15, processor server computer 310 may retrieve the token associated with the account of user 301 stored in its systems. Processor server computer 310 may send the retrieved token, cardholder information, payment account information, and cardholder contact information to service provider computer 314 at step 16.

[0170] At step 17, service provider computer 314 may enable the user to log in to their wallet provider account. Service provider computer 314 may store the information retrieved in steps 14 through 16, including cardholder information, payment account information, cardholder contact information, and token information, in association with the account of user 301.

[0171] At step 18, service provider computer 314 may display a notification to browser 302 that user 301 may utilize their new card with their wallet provider account associated with service provider computer 314. This may indicate that the token associated with the newly issued card is provisioned such that user 301 may utilize their new card for subsequent transactions.

[0172] A method according to the embodiments of the invention can be described with respect to FIG. 12. FIG. 12 shows a flowchart 1200 of a method for enabling a user immediate card access upon approval according to embodiments of the present invention and includes a user 401, a browser 402, an authorization computer 412 associated with an authorizing entity, a processor server computer 410, and a service

provider computer 414. In some embodiments, processor server computer 410 may also be a token service provider enabling a tokenization program. Any communications sent to and received from user 401 may be through a user device, such as user device 103 of FIG. 4. The user device may run browser 402. In some embodiments, processor server computer 410 may also be known as a payment processor server computer or payment processing network, authorization computer 412 may also be known as an issuer computer, and service provider computer 414 may also be known as a resource provider computer. In the exemplary case described below, service provider computer 414 may be a wallet provider computer.

[0173] Steps 1 through 11 in flowchart 1200 may be similar to corresponding steps 1 through 11 described in flowchart 1100 of FIG. 11. Thus, steps 1 through 11 are not being included in the description of flowchart 1200 herein so that information is not repeated. However, it is understood that the description corresponding to steps 1 through 11 in flowchart 1100 may be incorporated into the description of flowchart 1200 of FIG. 12.

[0174] At step 12, browser 402 may have open a website or application hosted by service provider computer 414. Browser 402 may render user 401 to sign up for an account with service provider computer 414 or sign in with an already existing account.

[0175] Accordingly, at step 13, if user 401 does not yet have an account with service provider computer 414, user 401 may create a username and password and provide any additional verification data requested by service provider computer 414. If user 401 already has an account with service provider computer 414, then user 401 may enter their registered username and password and any additional verification data requested by service provider computer 414 to enter their existing account. The additional verification data may include a token identifier associated with their new card account.

[0176] At step 14, service provider computer 414 may call processor server computer 310 to pull user data associated with user 401 and the newly issued card. For example, processor server computer 410 may open Application Programming Interfaces (APIs) to enable service provider computer 414 to pull data, which may include

cardholder information, payment account information, and cardholder contact information. In some embodiments, service provider computer 414 may utilize the APIs to request processor server computer 410 to retrieve certain data. For example, service provider computer 414 may provide the token identifier to processor server computer 410 and request from processor server computer 410 the token associated with the account of user 401. Thus, instead of processor server computer 410 pushing data to service provider computer 414, such as described in FIG. 10, flowchart 1200 shows service provider computer 414 calling APIs of processor server computer 410 to obtain information.

[0177] At step 15, processor server computer 410 may send cardholder information, payment account information, and cardholder contact information to service provider computer 414. Subsequently, at step 16, service provider computer 414 may save the received user data in a data record for the wallet provider account of user 401.

[0178] At step 17, service provider computer 414 may send a payload including the user data to a user interface displayed on browser 402 for confirmation by user 401. For example, service provider computer 414 may send web page form filled with user data associated with user 401. The form may display the user data in the user interface in editable fields, so that use 401 may change any values if desired.

[0179] At step 18, user 401 may view the data sent by service provider computer 414 and update or confirm the data. User 401 may update any data by editing the fields in the user interface. When finished editing, or if no edits are needed, user 401 may confirm the data is accurate by clicking on a button on browser 402. Subsequently, at 19, browser 402 may send an indication that user 401 confirmed the data of the wallet provider account to service provider computer 414. By allowing user 401 to confirm the data, service provider computer 414 ensures accuracy of data while forgoing the need for user 401 to input all the user data, which can be time consuming and cumbersome.

[0180] At step 20, service provider computer 414 may link the payload data to the wallet provider account of user 401. For example, service provider computer 414 may store the payload data in association with any other information related to the wallet provider account of user 401.

[0181] At step 21, service provider computer 414 may display a notification to browser 402 that user 401 may utilize their new card with their wallet provider account associated with service provider computer 414. This may indicate that the token associated with the newly issued card is provisioned such that user 401 may utilize their new card for subsequent transactions.

[0182] Embodiments of the invention may provide a number of advantages. For example, embodiments of the invention increase efficiency as a user no longer needs to wait to receive a plastic card in order to utilize a new card account and can have a new card immediately available, with minimal user input, on their mobile device once approved by an issuer. This forgoes the need for the user to manually add the new card to multiple digital wallets before use. This is in contrast to conventional systems, in which manual addition of the new card to a digital wallet disrupts user experience during a transaction, such as a checkout process.

[0183] Further, embodiments of the invention enable issuing a new card that can be utilized with a mobile wallet that was not yet installed on the mobile device when the card was issued. In other words, a digital wallet provider can be chosen after the new card is issued. This allows the user to easily utilize the issued card without the need for a previously installed mobile wallet that must be compatible with the issuer. This is convenient because the user may not know which digital wallets are compatible with the issuer before the new card is issued. Since the user is provided wallet provider options by the issuer computer, this provides the user the flexibility to choose amongst a plurality of wallet providers that may have different benefits. In addition, integrating tokenization processes with embodiments of the invention enables increased efficiency without compromising security of a transaction.

[0184] A computer system may be utilized to implement any of the entities or components described above. Subsystems of the computer system may be interconnected via a system bus. Additional subsystems may include a printer, a keyboard, a fixed disk (or other memory comprising computer readable media), a monitor, which is coupled to a display adapter, and others. Peripherals and input/output (I/O) devices, which couple to an I/O controller (which can be a processor or other

suitable controller), can be connected to the computer system by any number of means known in the art, such as by a serial port. For example, the serial port or external interface can be used to connect the computer apparatus to a wide area network such as the Internet, a mouse input device, or a scanner. The interconnection via system bus allows the central processor to communicate with each subsystem and to control the execution of instructions from system memory or the fixed disk, as well as the exchange of information between subsystems. The system memory and/or the fixed disk may embody a computer readable medium. In some embodiments, the monitor may be a touch sensitive display screen.

[0185] A computer system can include a plurality of the same components or subsystems, e.g., connected together by external interface or by an internal interface. In some embodiments, computer systems, subsystem, or apparatuses can communicate over a network. In such instances, one computer can be considered a client and another computer a server, where each can be part of a same computer system. A client and a server can each include multiple systems, subsystems, or components.

[0186] It should be understood that any of the embodiments of the present invention can be implemented in the form of control logic using hardware (e.g. an application specific integrated circuit or field programmable gate array) and/or using computer software with a generally programmable processor in a modular or integrated manner. As used herein, a processor includes a single-core processor, multi-core processor on a same integrated chip, or multiple processing units on a single circuit board or networked. Based on the disclosure and teachings provided herein, a person of ordinary skill in the art will know and appreciate other ways and/or methods to implement embodiments of the present invention using hardware and a combination of hardware and software.

[0187] Any of the software components or functions described in this application may be implemented as software code to be executed by a processor using any suitable computer language such as, for example, Java, C, C++, C#, Objective-C, Swift, or scripting language such as Perl or Python using, for example, conventional or object-

oriented techniques. The software code may be stored as a series of instructions or commands on a computer readable medium for storage and/or transmission, suitable media include random access memory (RAM), a read only memory (ROM), a magnetic medium such as a hard-drive or a floppy disk, or an optical medium such as a compact disk (CD) or DVD (digital versatile disk), flash memory, and the like. The computer readable medium may be any combination of such storage or transmission devices.

[0188] Such programs may also be encoded and transmitted using carrier signals adapted for transmission via wired, optical, and/or wireless networks conforming to a variety of protocols, including the Internet. As such, a computer readable medium according to an embodiment of the present invention may be created using a data signal encoded with such programs. Computer readable media encoded with the program code may be packaged with a compatible device or provided separately from other devices (e.g., via Internet download). Any such computer readable medium may reside on or within a single computer product (e.g. a hard drive, a CD, or an entire computer system), and may be present on or within different computer products within a system or network. A computer system may include a monitor, printer, or other suitable display for providing any of the results mentioned herein to a user.

[0189] The above description is illustrative and is not restrictive. Many variations of the invention will become apparent to those skilled in the art upon review of the disclosure. The scope of the invention should, therefore, be determined not with reference to the above description, but instead should be determined with reference to the pending claims along with their full scope or equivalents.

[0190] One or more features from any embodiment may be combined with one or more features of any other embodiment without departing from the scope of the invention.

[0191] A recitation of "a", "an" or "the" is intended to mean "one or more" unless specifically indicated to the contrary.

[0192] All patents, patent applications, publications, and descriptions mentioned above are herein incorporated by reference in their entirety for all purposes. None is admitted to be prior art.

WHAT IS CLAIMED

1. A method, comprising performing, by a server computer:

sending, to an authorization computer, a list of participating resource providing entities, wherein the authorization computer prompts a user operating a user device to make a selection from the list of participating resource providing entities;

receiving a selection of one or more resource providing entities from the participating resource providing entities;

receiving a request to issue tokens associated with an account of the user for the one or more resource providing entities; and

for each of the one or more resource providing entities:

determining a token associated with the account of the user; and

sending the token to a resource providing entity computer associated with the resource providing entity, wherein the user conducts a transaction with the resource providing entity using the token.

2. The method of claim 1, further comprising:

determining an authentication method supported by the authorization computer;

for each of the list of participating resource providing entities:

determining an authentication method supported by the participating resource providing entity;

comparing the authentication method supported by the participating resource providing entity and the authentication method supported by the authorization computer;

upon determining that the compared authentication methods match, including the participating resource providing entity in the list of participating resource providing entities.

3. The method of claim 2, further comprising:

determining that at least one of the participating resource providing entities has an account on file for the user; and

sending, to the authorization computer, information indicating the at least one participating resource providing entity with which the user has the account on file.

4. The method of claim 3, wherein the selection of the one or more resource providing entities by the user includes a participating resource providing entity that has an account on file for the user, and wherein the user conducts the transaction using the account on file.

5. The method of claim 1, further comprising:

generating a link routed to the server computer; and

sending the link to the authorization computer, wherein the user activates the link using the user device after the authorization computer prompts the user.

6. The method of claim 5, further comprising:

for each of the plurality of participating resource providing entities selected by the user:

prompting the user for authentication information for the participating resource providing entity; and

sending the authentication information to the participating resource providing entity.

7. The method of claim 6, wherein the authentication information is utilized to generate a new account for the user associated with the participating resource providing entity.

8. The method of claim 1, further comprising:

generating a plurality of links routed to the plurality of resource providing entities; and

sending the plurality of links to the authorization computer, wherein the user activates the plurality of links using the user device after the authorization computer prompts the user.

9. The method of claim 1, wherein the account is a new account, further comprising:

receiving, from the authorization computer, account information associated with the account.

10. The method of claim 1, wherein the account is an existing account, further comprising:

retrieving account information associated with the account.

11. A server computer comprising:

a processor; and

a computer readable medium coupled to the processor, the computer readable medium comprising code executable to perform a method comprising:

sending, to an authorization computer, a list of participating resource providing entities, wherein the authorization computer prompts a user operating a user device to make a selection from the list of participating resource providing entities;

receiving a selection of one or more resource providing entities from the participating resource providing entities;

receiving a request to issue tokens associated with an account of the user for the one or more resource providing entities; and

for each of the one or more resource providing entities:

determining a token associated with the account of the user; and

sending the token to a resource providing entity computer associated with the resource providing entity, wherein the user conducts a transaction with the resource providing entity using the token.

12. The server computer of claim 11, the method further comprising:

determining an authentication method supported by the authorization computer;

for each of the list of participating resource providing entities:

determining an authentication method supported by the participating resource providing entity;

comparing the authentication method supported by the participating resource providing entity and the authentication method supported by the authorization computer;

upon determining that the compared authentication methods match, including the participating resource providing entity in the list of participating resource providing entities.

13. The server computer of claim 12, the method further comprising:

determining that at least one of the participating resource providing entities has an account on file for the user; and

sending, to the authorization computer, information indicating the at least one participating resource providing entity with which the user has the account on file.

14. The server computer of claim 13, wherein the selection of the one or more resource providing entities by the user includes a participating resource providing entity that has an account on file for the user, and wherein the user conducts the transaction using the account on file.

15. The server computer of claim 11, the method further comprising:

generating a link routed to the server computer; and

sending the link to the authorization computer, wherein the user activates the link using the user device after the authorization computer prompts the user.

16. The server computer of claim 15, the method further comprising:

for each of the plurality of participating resource providing entities selected by the user:

prompting the user for authentication information for the participating resource providing entity; and

sending the authentication information to the participating resource providing entity.

17. The server computer of claim 16, wherein the authentication information is utilized to generate a new account for the user associated with the participating resource providing entity.

18. The server computer of claim 11, the method further comprising:

generating a plurality of links routed to the plurality of resource providing entities; and

sending the plurality of links to the authorization computer, wherein the user activates the plurality of links using the user device after the authorization computer prompts the user.

19. The server computer of claim 11, wherein the account is a new account, the method further comprising:

receiving, from the authorization computer, account information associated with the account.

20. The server computer of claim 11, wherein the account is an existing account, the method further comprising:

retrieving account information associated with the account.

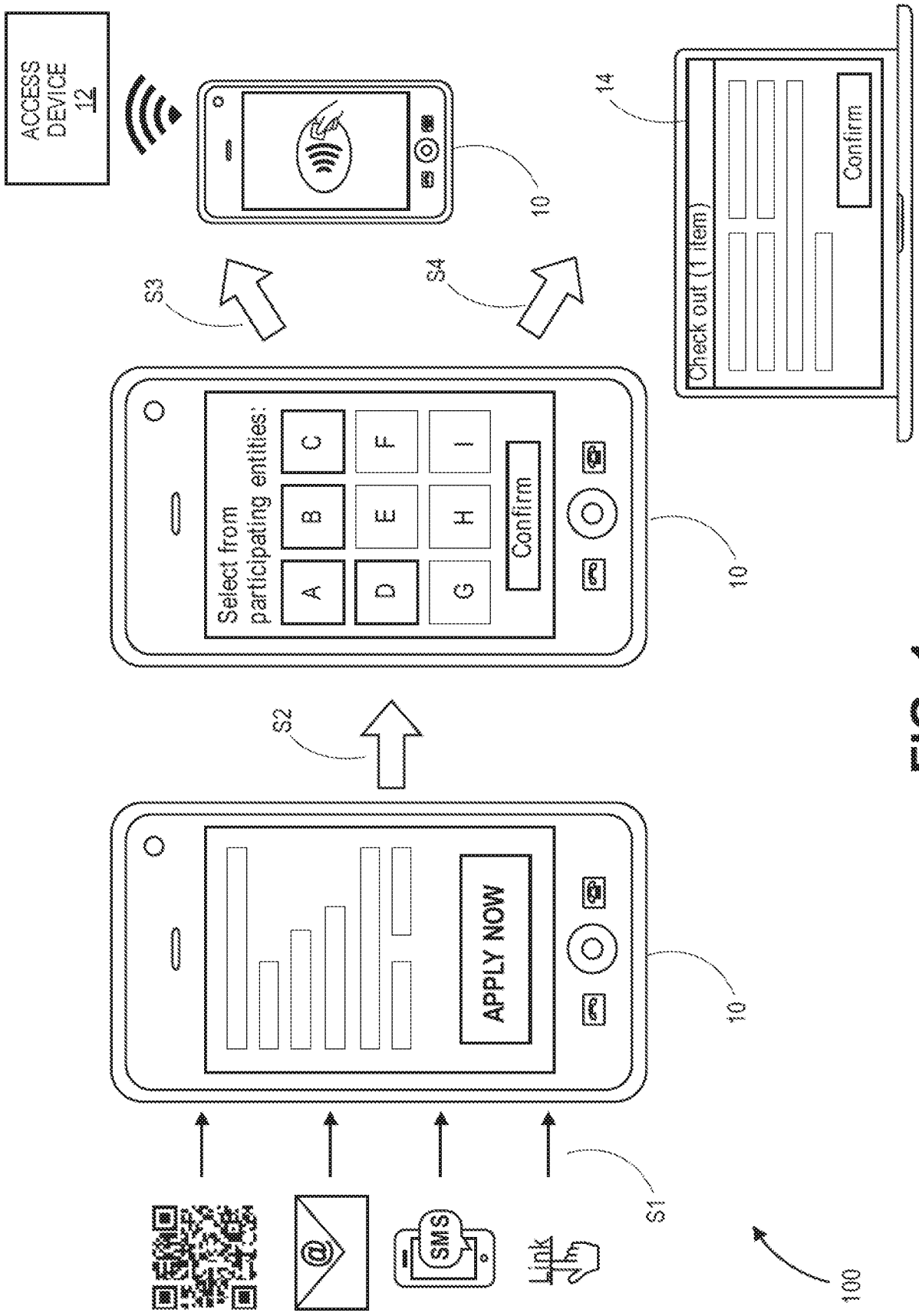
ACCESS DEVICE 12
10
14
Check out (1 item)
Confirm
S3
S4
Select from participating entities:
A
B
C
D
E
F
G
H
I
Confirm
10
S2
APPLY NOW
10
SMS
Link
S1
100

FIG. 1

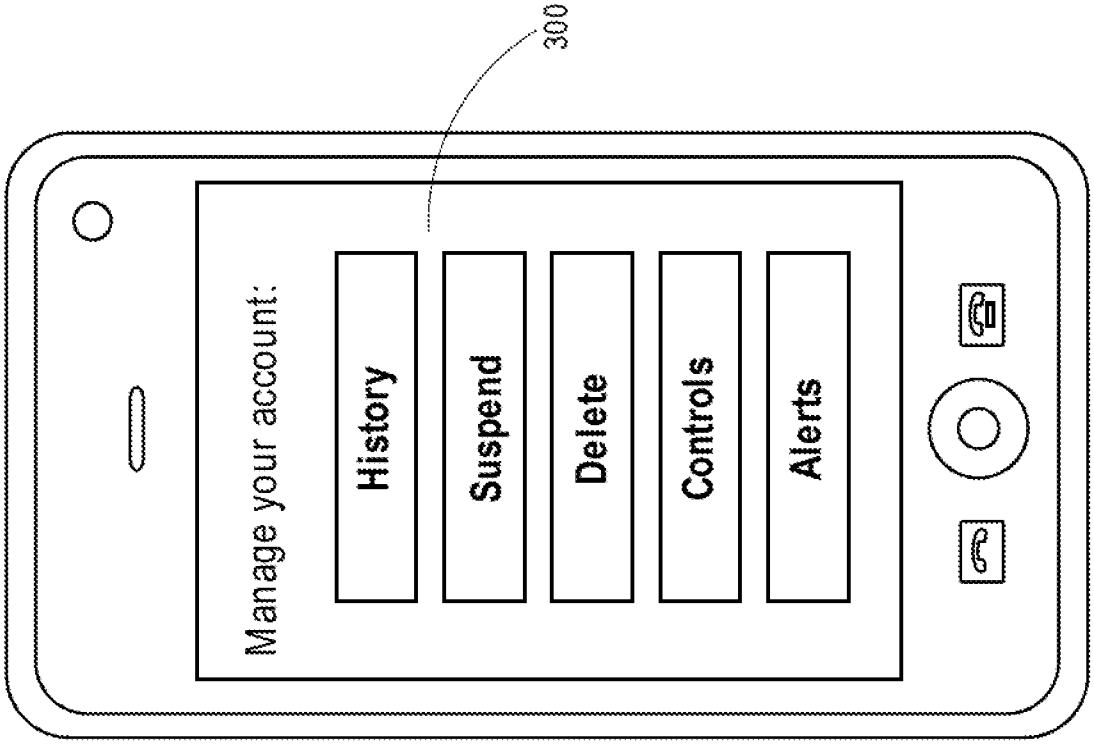
300
Manage your account:
History
Suspend
Delete
Controls
Alerts

FIG. 3

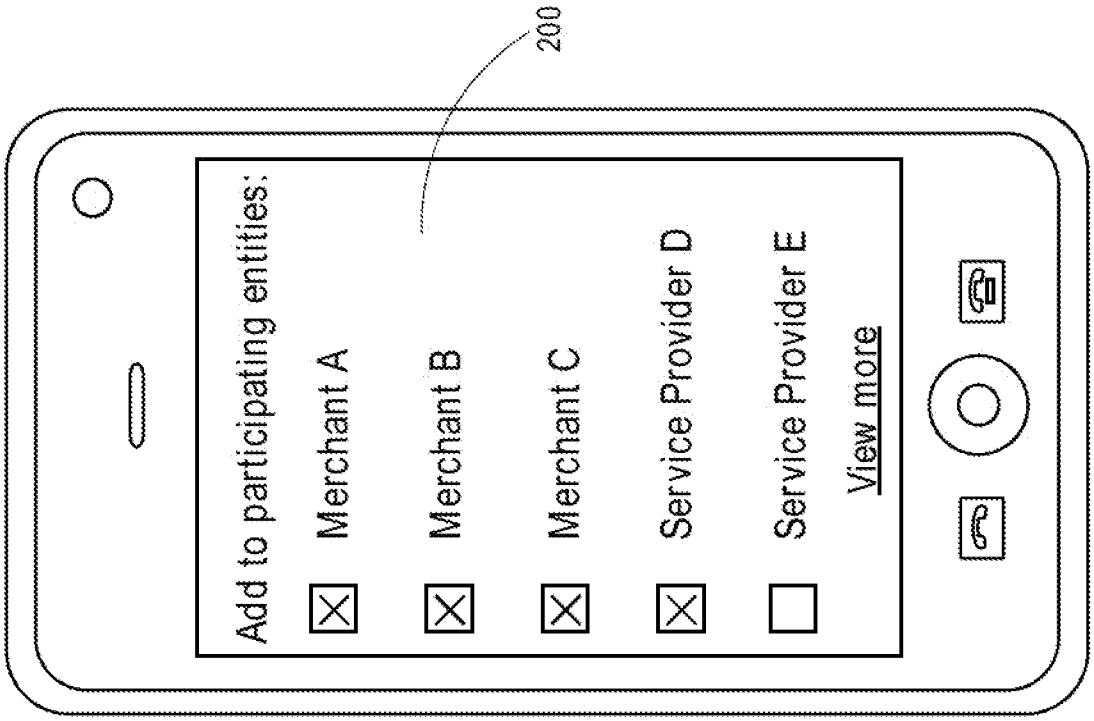
200
Add to participating entities:
Merchant A
Merchant B
Merchant C
Service Provider D
Service Provider E
View more

FIG. 2

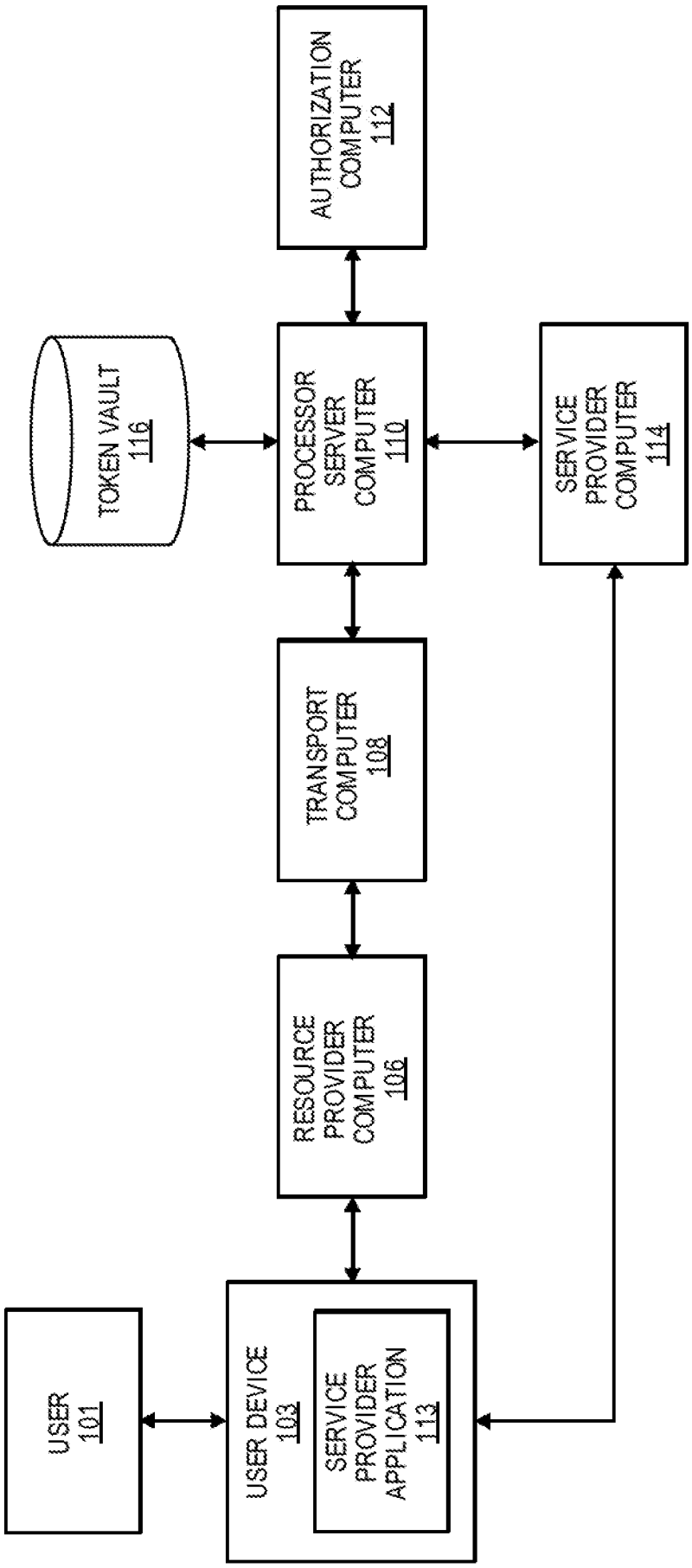
AUTHORIZATION COMPUTER 112
TOKEN VAULT 116
PROCESSOR SERVER COMPUTER 110
SERVICE PROVIDER COMPUTER 114
TRANSPORT COMPUTER 108
RESOURCE PROVIDER COMPUTER 106
USER 101
USER DEVICE 103
SERVICE PROVIDER APPLICATION 113
400

FIG. 4

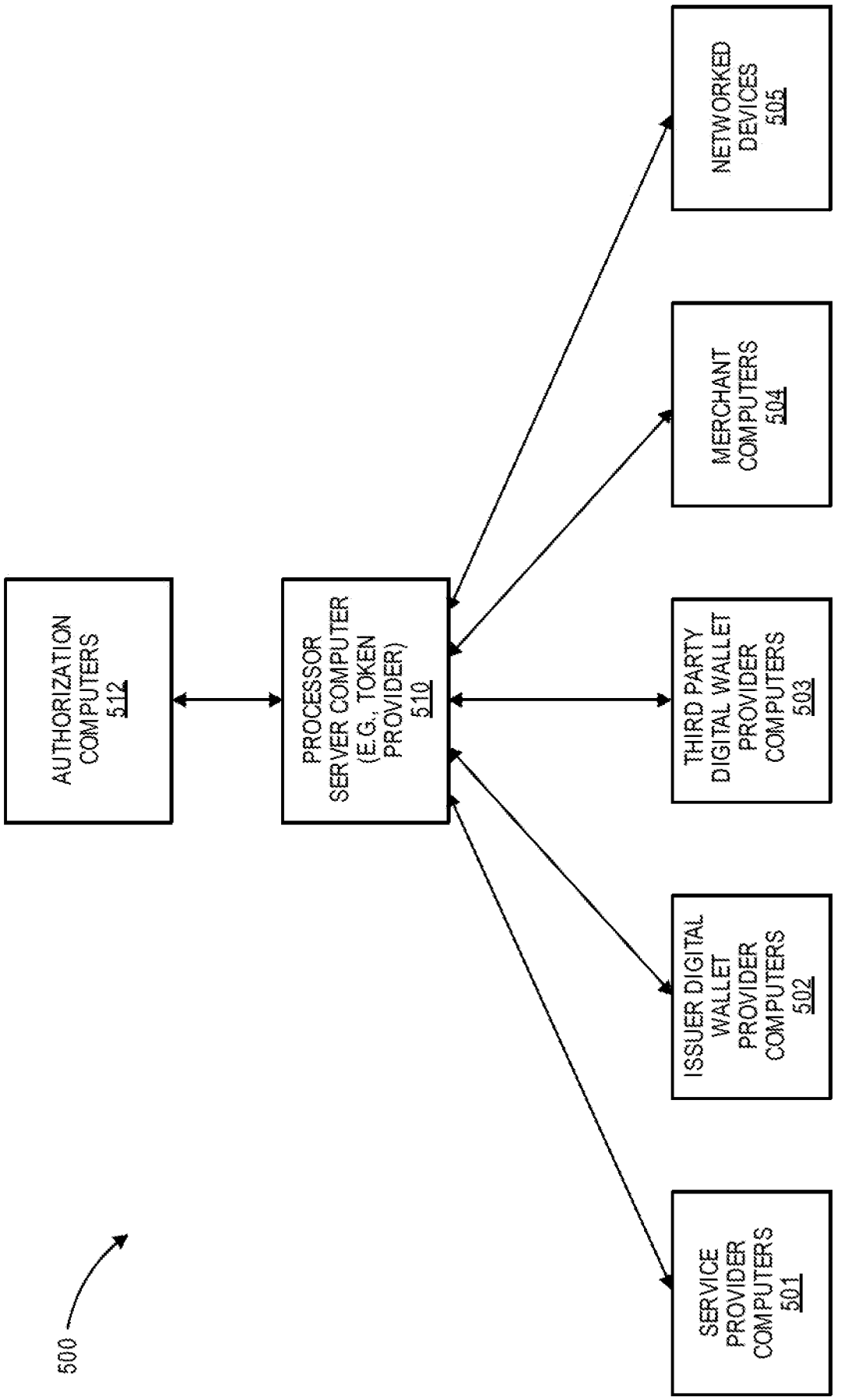
500
SERVICE PROVIDER COMPUTERS 501
ISSUER DIGITAL WALLET PROVIDER COMPUTERS 502
THIRD PARTY DIGITAL WALLET PROVIDER COMPUTERS 503
MERCHANT COMPUTERS 504
NETWORKED DEVICES 505
PROCESSOR SERVER COMPUTER (E.G., TOKEN PROVIDER) 510
AUTHORIZATION COMPUTERS 512

FIG. 5

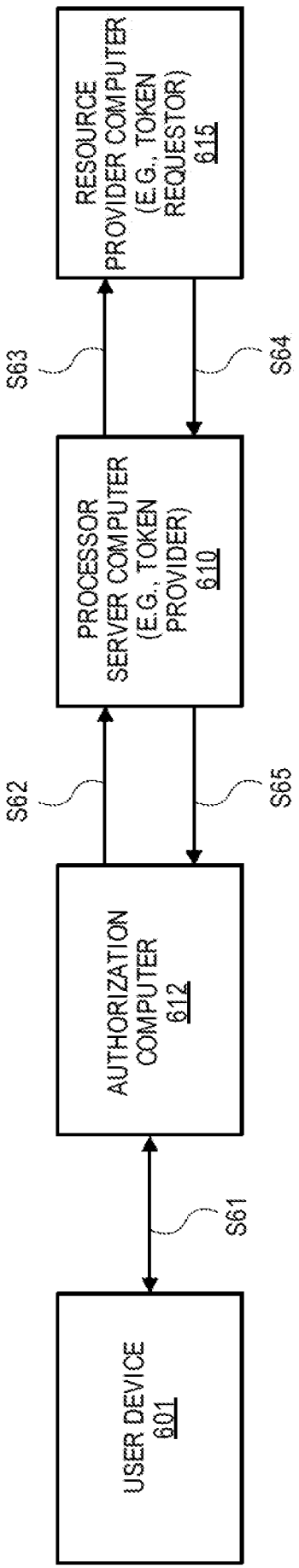
RESOURCE PROVIDER COMPUTER (E.G., TOKEN REQUESTOR) 615
S63
S64
PROCESSOR SERVER COMPUTER (E.G., TOKEN PROVIDER) 610
S62
S65
AUTHORIZATION COMPUTER 612
S61
USER DEVICE 601
600

FIG. 6

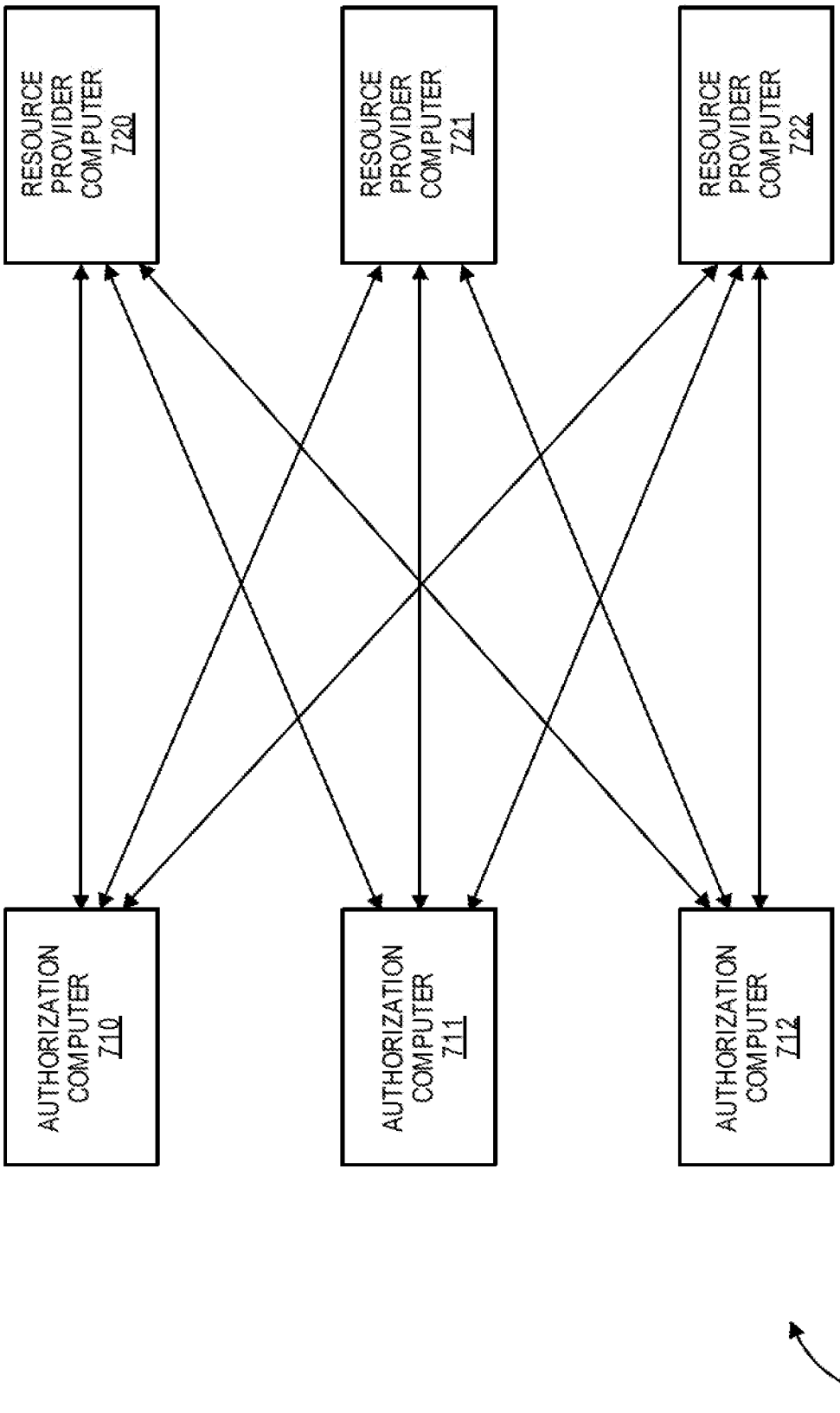
RESOURCE PROVIDER COMPUTER Z20
RESOURCE PROVIDER COMPUTER Z21
RESOURCE PROVIDER COMPUTER Z22
AUTHORIZATION COMPUTER Z10
AUTHORIZATION COMPUTER Z11
AUTHORIZATION COMPUTER Z12
700

FIG. 7

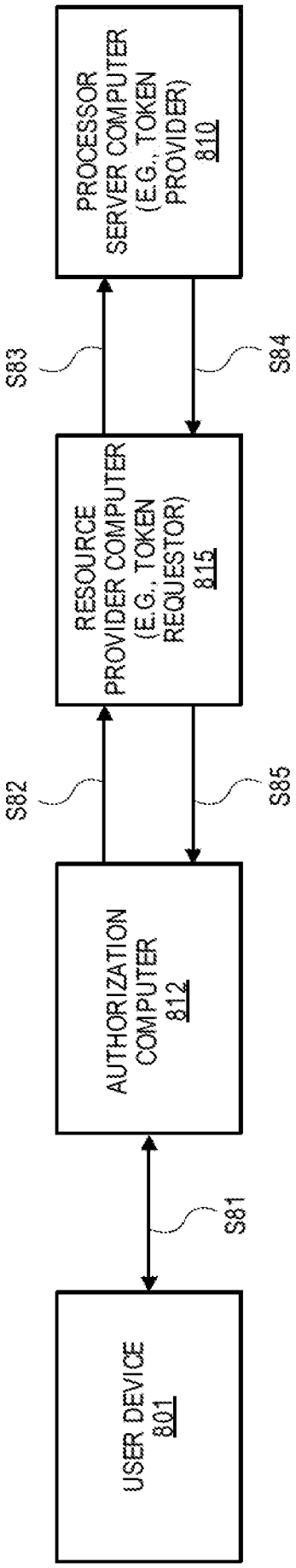
PROCESSOR SERVER COMPUTER (E.G., TOKEN PROVIDER) 810
RESOURCE PROVIDER COMPUTER (E.G., TOKEN REQUESTOR) 815
AUTHORIZATION COMPUTER 812
USER DEVICE 801
S81
S82
S83
S84
S85
800

FIG. 8

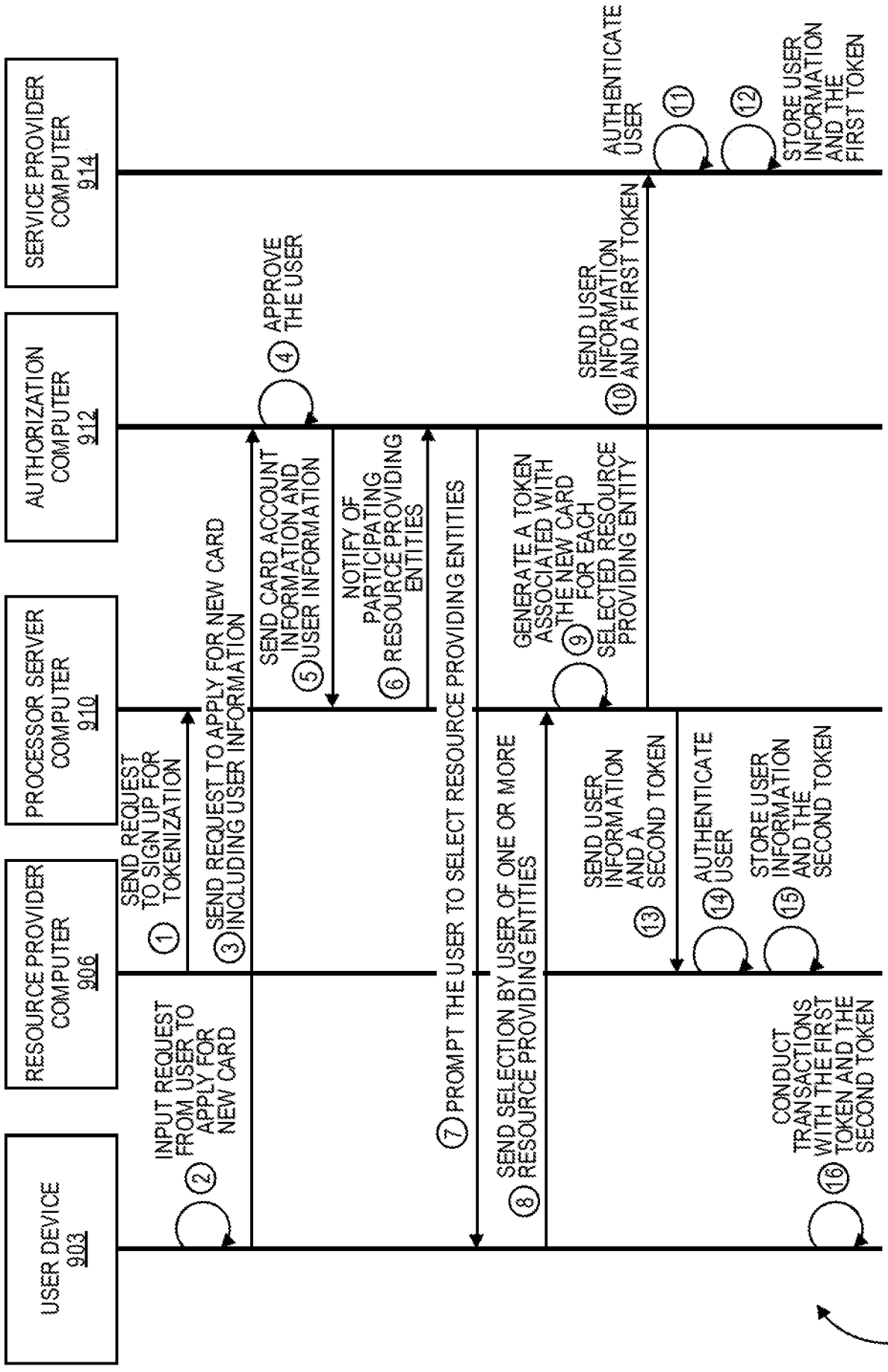
USER DEVICE 903
RESOURCE PROVIDER COMPUTER 906
PROCESSOR SERVER COMPUTER 910
AUTHORIZATION COMPUTER 912
SERVICE PROVIDER COMPUTER 914
SEND REQUEST TO SIGN UP FOR TOKENIZATION ①
INPUT REQUEST FROM USER TO APPLY FOR NEW CARD ②
SEND REQUEST TO APPLY FOR NEW CARD INCLUDING USER INFORMATION ③
APPROVE THE USER ④
SEND CARD ACCOUNT INFORMATION AND USER INFORMATION ⑤
NOTIFY OF PARTICIPATING RESOURCE PROVIDING ENTITIES ⑥
PROMPT THE USER TO SELECT RESOURCE PROVIDING ENTITIES ⑦
SEND SELECTION BY USER OF ONE OR MORE RESOURCE PROVIDING ENTITIES ⑧
GENERATE A TOKEN ASSOCIATED WITH THE NEW CARD FOR EACH SELECTED RESOURCE PROVIDING ENTITY ⑨
SEND USER INFORMATION AND A FIRST TOKEN ⑩
AUTHENTICATE USER ⑪
STORE USER INFORMATION AND THE FIRST TOKEN ⑫
SEND USER INFORMATION AND A SECOND TOKEN ⑬
AUTHENTICATE USER ⑭
STORE USER INFORMATION AND THE SECOND TOKEN ⑮
CONDUCT TRANSACTIONS WITH THE FIRST TOKEN AND THE SECOND TOKEN ⑯
900

FIG. 9

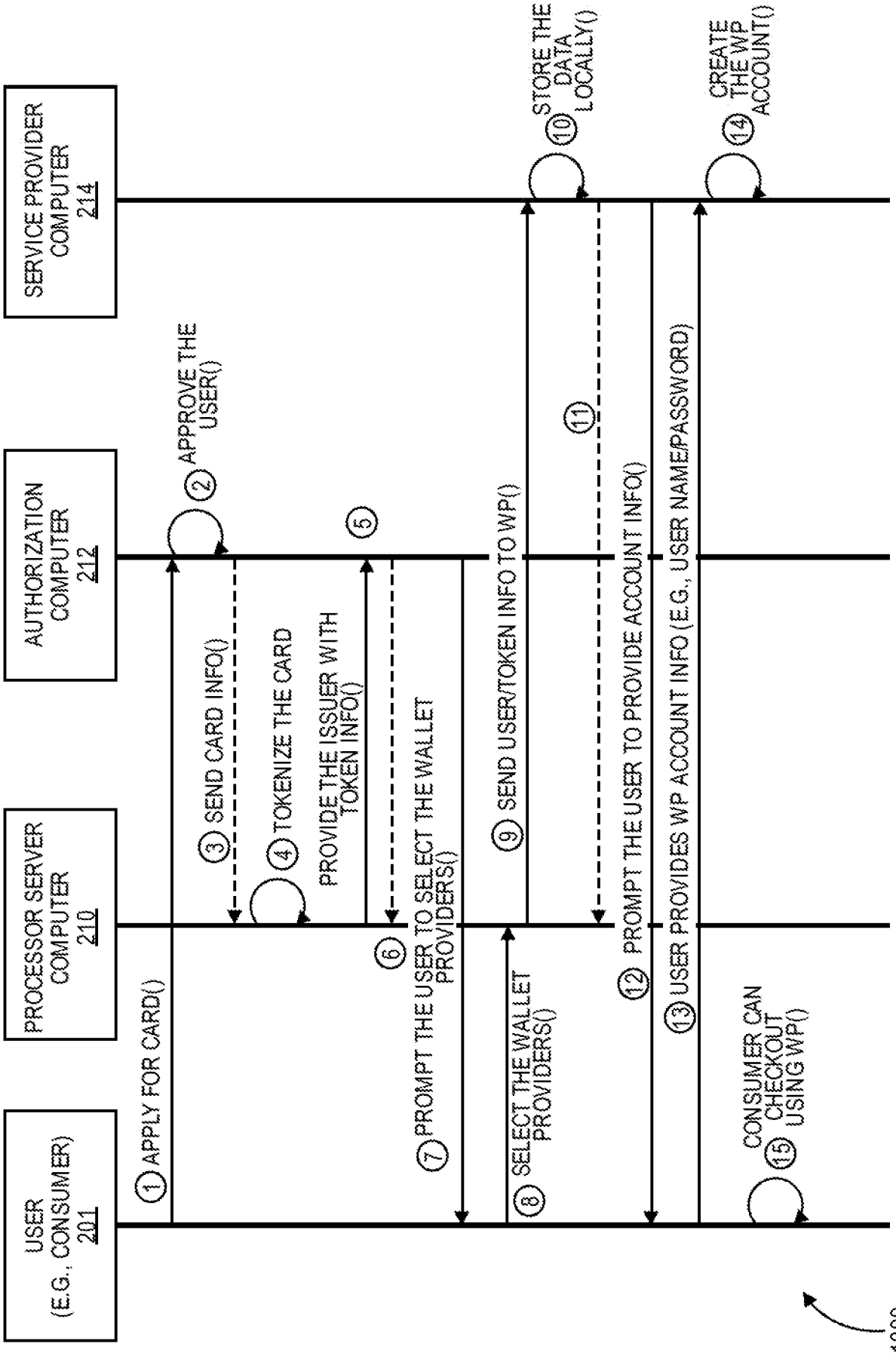
USER (E.G., CONSUMER) 201
PROCESSOR SERVER COMPUTER 210
AUTHORIZATION COMPUTER 212
SERVICE PROVIDER COMPUTER 214
1 APPLY FOR CARD()
2 APPROVE THE USER()
3 SEND CARD INFO()
4 TOKENIZE THE CARD
5 PROVIDE THE ISSUER WITH TOKEN INFO()
6
7 PROMPT THE USER TO SELECT THE WALLET PROVIDERS()
8 SELECT THE WALLET PROVIDERS()
9 SEND USER/TOKEN INFO TO WP()
10 STORE THE DATA LOCALLY()
11
12 PROMPT THE USER TO PROVIDE ACCOUNT INFO()
13 USER PROVIDES WP ACCOUNT INFO (E.G., USER NAME/PASSWORD)
14 CREATE THE WP ACCOUNT()
15 CONSUMER CAN CHECKOUT USING WP()
1000

FIG. 10

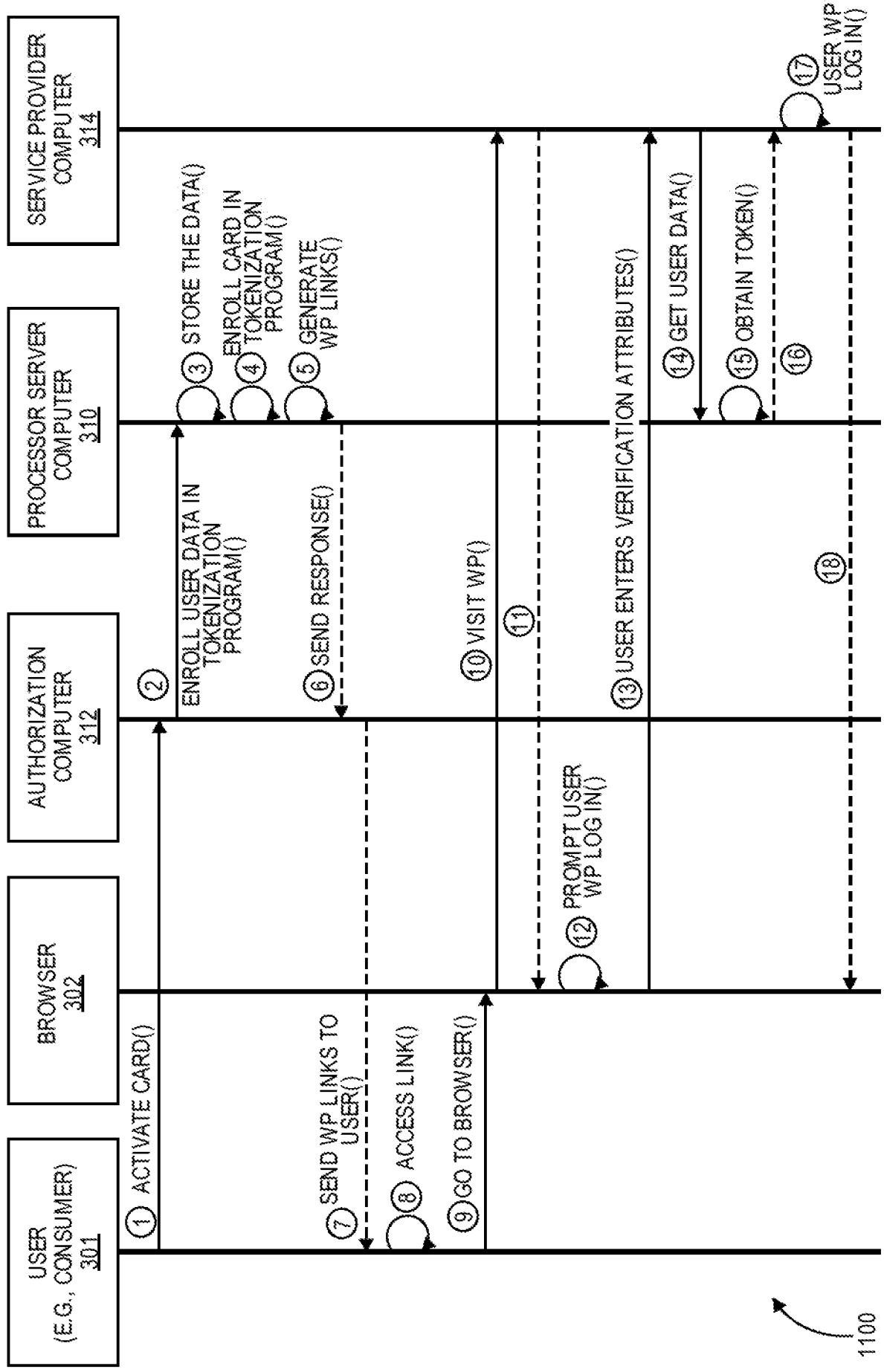
USER (E.G., CONSUMER) 301
BROWSER 302
AUTHORIZATION COMPUTER 312
PROCESSOR SERVER COMPUTER 310
SERVICE PROVIDER COMPUTER 314
1 ACTIVATE CARD()
2 ENROLL USER DATA IN TOKENIZATION PROGRAM()
3 STORE THE DATA()
4 ENROLL CARD IN TOKENIZATION PROGRAM()
5 GENERATE WP LINKS()
6 SEND RESPONSE()
7 SEND WP LINKS TO USER()
8 ACCESS LINK()
9 GO TO BROWSER()
10 VISIT WP()
11
12 PROMPT USER WP LOG IN()
13 USER ENTERS VERIFICATION ATTRIBUTES()
14 GET USER DATA()
15 OBTAIN TOKEN()
16
17 USER WP LOG IN()
18
1100

FIG. 11

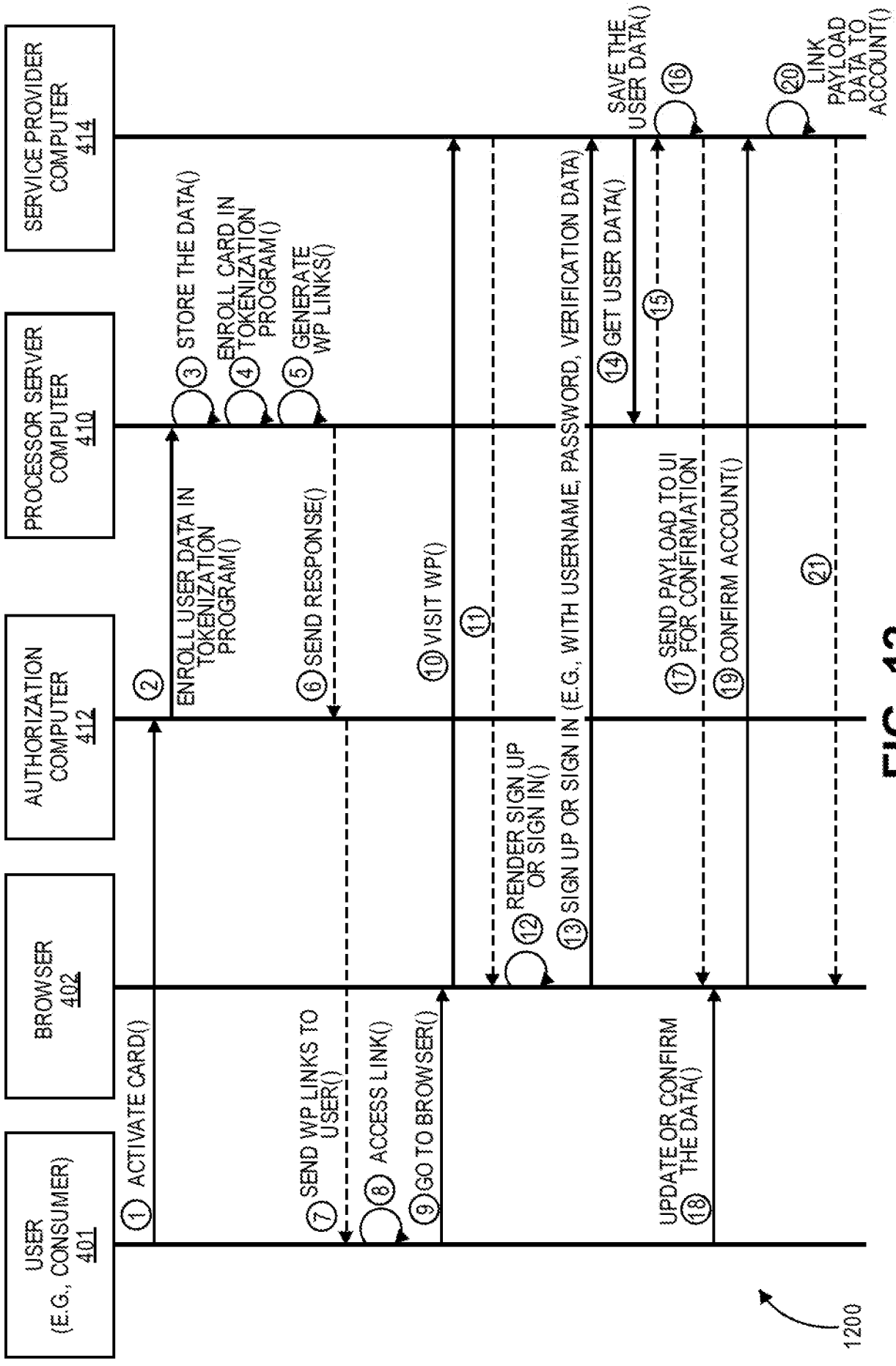
USER (E.G., CONSUMER) 401
BROWSER 402
AUTHORIZATION COMPUTER 412
PROCESSOR SERVER COMPUTER 410
SERVICE PROVIDER COMPUTER 414
1 ACTIVATE CARD()
2 ENROLL USER DATA IN TOKENIZATION PROGRAM()
3 STORE THE DATA()
4 ENROLL CARD IN TOKENIZATION PROGRAM()
5 GENERATE WP LINKS()
6 SEND RESPONSE()
7 SEND WP LINKS TO USER()
8 ACCESS LINK()
9 GO TO BROWSER()
10 VISIT WP()
11
12 RENDER SIGN UP OR SIGN IN()
13 SIGN UP OR SIGN IN (E.G., WITH USERNAME, PASSWORD, VERIFICATION DATA)
14 GET USER DATA()
15
16 SAVE THE USER DATA()
17 SEND PAYLOAD TO UI FOR CONFIRMATION
18 UPDATE OR CONFIRM THE DATA()
19 CONFIRM ACCOUNT()
20 LINK PAYLOAD DATA TO ACCOUNT()
21
1200

FIG. 12