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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
26 October 2017 (26.10.2017)

WIPO | PCT

(10) International Publication Number
WO 2017/184121 A1

(51) International Patent Classification:
G06Q 20/38 (2012.01) *G06Q 20/08* (2012.01)

(21) International Application Number:
PCT/US2016/028276

(22) International Filing Date:
19 April 2016 (19.04.2016)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant: **VISA INTERNATIONAL SERVICE ASSOCIATION** [US/US]; 900 Metro Center Blvd, Foster City, California 94404 (US).

(72) Inventors: **KUMAR, Satish**; #08-80 185, Bedok North Road, 460185 Singapore (SG). **SAMANTARAY, Debabrata**; #07-01 10 Eunos Road 8, 408600 Singapore (SG). **BALAKRISHNAN NAIR, Bibin**; #04-107 206 Clementi Avenue 6, 120206 Singapore (SG). **SAHU, Ajit**; #13-56 Block-571, Street-53 Pasir Ris, 510571 Singapore (SG). **GOPALAKRISHNAN, Kaushik**; #13-37, A Treasure Trove, 68 Punggol Walk, 828784 Singapore (SG).

(74) Agent: **BAKER, Amanda** et al.; Kilpatrick Townsend & Stockton LLP, Two Embarcadero Center, 8th Floor, San Francisco, California 94111 (US).

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

(54) Title: SYSTEMS AND METHODS FOR PERFORMING PUSH TRANSACTIONS

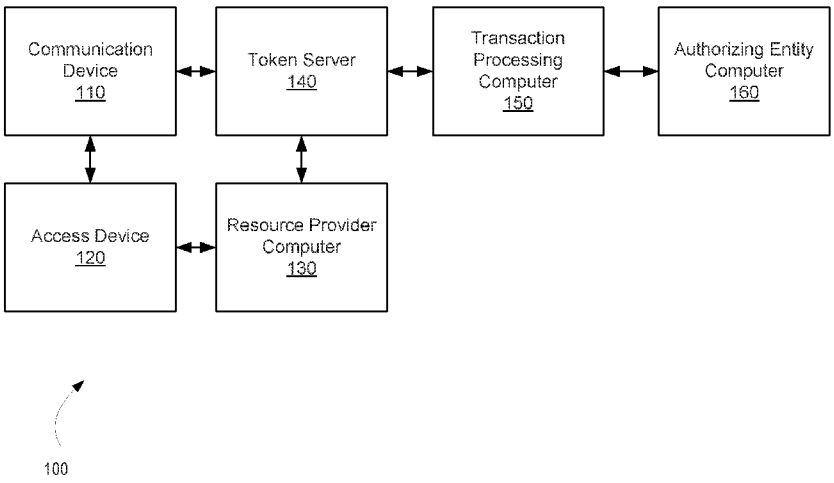

FIG. 1

(57) Abstract: Embodiments of the invention are directed to systems and methods for pushing tokenized payments to resource providers for goods or services, after the goods or services are received. A user may make a transaction request including a credential and a resource provider ID (e.g., a resource provider location) via a server computer. The server computer may generate a token corresponding to the credential and transmit it to the resource provider using the resource provider ID. Upon receiving the token, the resource provider may enter a transaction amount and send it with the token in an authorization request message. The transaction can then be processed according to standard transaction processing methods, as if the resource provider had initiated the transaction request.

WO 2017/184121 A1

[Continued on next page]

(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))*

SYSTEMS AND METHODS FOR PERFORMING PUSH TRANSACTIONS

CROSS-REFERENCES TO RELATED APPLICATIONS

[0001] None.

BACKGROUND

[0002] There are instances in which a consumer may want to pay for goods or services without knowing the final amount of the transaction. For example, a consumer may want to preauthorize a payment amount for gas or for a meal to provide assurance that they will indeed pay for the gas or meal, even though they may not know the final cost. Further, a consumer may want to pay for the goods or services while still protecting sensitive account information, such as a primary account number (PAN). Thus, a consumer may want to minimize the number of parties having access to the sensitive information, or eliminate access to the sensitive information altogether. Systems and methods for allowing consumers to push payments to merchants in a safe and secure manner are needed.

[0003] Embodiments of the invention address this and other problems, individually and collectively.

SUMMARY

[0004] According to one embodiment of the invention, a method is provided. The method comprises receiving, at a server computer from a communication device, a transaction request including a credential and a resource provider ID associated with a resource provider computer. The method further comprises transmitting a token corresponding to the credential to the resource provider computer using the resource provider ID, wherein a transaction input value is entered into the resource provider computer after the token is received at the resource provider computer. The method further comprises receiving the token and the transaction input value, and processing the transaction request in accordance with the transaction input value.

[0005] According to one embodiment of the invention, another method is provided. The method comprises providing, by a resource provider computer to a communication device, transaction data including a resource provider ID associated with the resource provider computer, wherein the communication device thereafter sends a transaction request including a credential and the resource provider ID to a server computer. The method further comprises receiving, by the resource provider computer, a token corresponding to the credential from the server computer, wherein the server computer sends the token to the resource provider computer using the resource provider ID. The method further comprises sending, by the resource provider computer, a transaction input value and the token to the server computer, wherein the server computer thereafter processes the transaction request in accordance with the transaction input value.

[0006] Embodiments of the invention are further directed to a server computer comprising a processor and a memory coupled to the processor. The memory can store instructions, executable by the processor, for implementing the above described methods.

[0007] These and other embodiments of the invention are described in further detail below.

BRIEF DESCRIPTION OF THE DRAWINGS

[0008] FIG. 1 shows a block diagram of a system according to embodiments of the present invention.

[0009] FIG. 2 shows a flowchart of a method for performing push transactions according to embodiments of the present invention.

[0010] FIG. 3 shows a flowchart of a method for performing push transactions according to embodiments of the present invention.

[0011] FIG. 4 shows a block diagram of a communication device according to embodiments of the present invention.

[0012] FIG. 5 shows a block diagram of a token server according to embodiments of the present invention.

DETAILED DESCRIPTION

[0013] Embodiments of the invention are directed to systems and methods for pushing tokenized payments to resource providers for goods or services, after the goods or services are received. A user may make a transaction request including a credential and a resource provider ID (e.g., a resource provider location) via a server computer. The server computer may generate a token corresponding to the credential and transmit it to the resource provider using the resource provider ID. Upon receiving the token, the resource provider may enter a transaction amount and send it with the token in an authorization request message. The transaction can then be processed according to standard transaction processing methods, as if the resource provider had initiated the transaction request. In one embodiment, before providing the token to the resource provider, the server computer initiates preauthorization for a capped amount using the credential, which ensures that a transaction amount entered by a resource provider that is over the capped amount is declined. This reduces the risk of fraud by the resource provider.

[0014] Before discussing specific embodiments and examples, some descriptions of terms used herein are provided below.

[0015] An "authorization request message" may be a message that requests authorization for a particular event. For example, an authorization request message may request authorization to perform a payment transaction. In some embodiments, an authorization request message 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.

[0016] 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.

[0017] A "communication device" may comprise any suitable electronic device that may be operated by a user, which may also provide remote communication capabilities to a network. Examples of remote communication capabilities include using a mobile phone (wireless) network, wireless data network (e.g., 3G, 4G or similar networks), Wi-Fi, Wi-Max, or any other communication medium that may provide access to a network such as the Internet or a private network. Examples of communication devices include mobile phones (e.g., cellular phones), PDAs, tablet computers, net books, laptop computers, personal music players, handheld specialized readers, watches, fitness bands, ankle bracelets, rings, earrings, etc., as well as automobiles with remote communication capabilities. A communication device may comprise any suitable hardware and software for performing such functions, and may also include multiple devices or components (e.g., when a device has remote access to a network by tethering to another device – i.e., using the other device as a modem – both devices taken together may be considered a single communication device).

[0018] A "credential" may comprise any evidence of authority, rights, or entitlement to privileges. For example, access credentials may comprise permissions to access certain tangible or intangible assets, such as a building or a file. In another example, payment credentials may include any suitable information

associated with and/or identifying an 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 an "account identifier" such as a PAN (primary account number or "account number"), a token, a subtoken, a gift card number or code, a prepaid card number or code, a user name, an expiration date, a CVV (card verification value), a dCVV (dynamic card verification value), a CVV2 (card verification value 2), a CVC3 card verification value, etc. An example of a PAN is a 16-digit number, such as "4147 0900 0000 1234". In some embodiments, credentials may be considered sensitive information.

[0019] A "digital wallet" can include an electronic application or device that allows an individual to conduct electronic transactions. A digital wallet may store user profile information, payment credentials, bank account information, one or more digital wallet identifiers, and/or the like, and can be used in a variety of transactions, such as but not limited to eCommerce, social networks, money transfer/personal payments, mobile commerce, proximity payments, gaming, and/or the like for retail purchases, digital goods purchases, utility payments, purchasing games or gaming credits from gaming websites or systems, transferring funds between users, and/or the like. A digital wallet may be designed to streamline the purchase and payment process. A digital wallet may allow the user to load one or more payment cards onto the digital wallet so as to make a payment without having to enter an account number or present a physical card. A digital wallet may also store transaction records (e.g., electronic receipts).

[0020] A "resource provider" may be an entity that can provide a resource such as goods, services, information, and/or access. Examples of a resource provider include merchants, access devices, secure data access points, etc. A "merchant" may typically be an entity that engages in transactions and can sell goods or services, or provide access to goods or services.

[0021] A "resource provider ID" may be any identifier associated with a resource provider. The identifier may be any combination of letters, numbers, symbols, and/or images, such as a code. A resource provider ID may include or indicate a location associated with a resource provider.

[0022] A "server computer" may include a powerful computer or 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. The server computer may comprise one or more computational apparatuses and may use any of a variety of computing structures, arrangements, and compilations for servicing the requests from one or more client computers.

[0023] 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. Further, in some embodiments, the token format may be configured to allow the entity receiving the token to identify it as a token and recognize the entity that issued the token.

[0024] A "transaction input value" can include any parameter of a transaction, including any unit of data or information. For example, a transaction input value may include an amount of money, a type of transaction, a particular resource provider, a type of resource provider, etc.

[0025] FIG. 1 shows a block diagram of a system 100 according to embodiments of the present invention. The system 100 includes a communication device 110, an access device 120, a resource provider computer 130, a token server 140, a transaction processing computer 150, and an authorizing entity computer 160.

Each of these systems and computers may be in operative communication with each other. The communication device 110 may be operated by a user (not shown).

[0026] Communication device 110 may be any device suitable to carry out a financial transaction or any other additional related actions. Communication device 110 may include a memory that may store a digital wallet application or payment application. The application may be provisioned with a credential to enable communication device 110 to conduct transactions. Communication device 110 may also include a secure element that can be implemented in either hardware and/or software, which may store sensitive account or personal information. Communication device 110 may communicate over a communication network with one or more entities, including access device 120 and token server 140.

[0027] In embodiments in which communication device 110 includes a digital wallet application, communication device 110 may further be in communication with a service provider computer that may be operated or associated with an application provider (not shown). The application provider may be an entity that provides the digital wallet application to communication device 110 for use by a user. The service provider computer may maintain one or more digital wallets for each user, and each digital wallet may be associated with credentials for one or more payment accounts. Examples of digital wallets may include Visa Checkout™ or Google™ Wallet, etc. The service provider computer may send and receive over-the-air (OTA) messages to a digital wallet application stored on the communication device 110. The service provider computer may include a processor and a computer readable medium coupled to the processor, the computer readable medium comprising code, executable by the processor for performing the disclosed digital wallet functionalities.

[0028] Access device 120 may be any suitable device that provides access to an external device, such as, in one example, resource provider computer 130. An access device may generally be located in any suitable location, such as at the location of a resource provider. An access device 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, web interfaces, and the like. Access device 120 may use any suitable contact or contactless mode of operation to send or receive data from, or associated with, communication device 110. In some embodiments, where access device 120 may comprise a POS terminal, any suitable POS terminal may be used and may 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, access device 120 may be part of resource provider computer 130.

[0029] The resource provider computer 130 may be configured to receive transaction data from access device 120. Resource provider computer 130 may enable a resource provider such as a merchant to engage in transactions, sell goods or services, or provide access to goods or services to the consumer. The resource provider computer 130 may accept multiple forms of payment and may use multiple tools to conduct different types of transactions. For example, the resource provider computer 130 may communicate with, include, or be an access device 120 at a physical store operated by the merchant for in-person transactions. The resource provider computer 130 may also enable the merchant to sell goods and/or services via a website, and may accept payments over the Internet.

[0030] Token server 140 may comprise a server computer to facilitate performance of the token management functions described herein. The server computer may include a processor and a computer readable medium coupled to the processor, the computer readable medium comprising code, executable by the processor.

[0031] In some embodiments, token server 140 may include a token generation module that can generate and/or provide a “payment token” that is associated with sensitive data (e.g., credentials). For example, the token generation module may generate a payment token that can be used as a substitute for a real account identifier (e.g., a Primary Account Number (PAN) of an account), and maintain a stored association (e.g., mapping) between the payment token and the PAN, such that a token exchange module is able to “translate” the payment token

back to the original PAN. In some embodiments, the payment token is mathematically derived from the original PAN. In other embodiments, the payment token is randomly generated with respect to the original PAN, and is simply linked to it in a data table. Regardless of how the payment token is generated from the PAN and vice versa, the use of a payment token instead of a real account identifier during a transaction can provide enhanced security. In some embodiments, the payment token and/or information regarding the payment token may be stored in a token vault. These functionalities are described further herein with respect to FIG. 5.

[0032] In some embodiments, a transport computer (not shown) is provided between the resource provider computer 130 and the transaction processing computer 150. The transport computer may be associated with an acquirer. An "acquirer" may typically be a business entity (e.g., a commercial bank) that has a business relationship with a particular resource provider (e.g., merchant) or other entity. Some entities can perform both issuer and acquirer functions. Some embodiments may encompass such single entity issuer-acquirers.

[0033] The transaction processing computer 150 may be associated with one or more payment service providers. The transaction processing computer 150 may also comprise a server computer. The server computer may include a processor and a computer readable medium coupled to the processor, the computer readable medium comprising code, executable by the processor.

[0034] The authorizing entity computer 160 may communicate with the transaction processing computer 150 to conduct transactions. The authorizing entity computer 160 may comprise a server computer. The server computer may include a processor and a computer readable medium coupled to the processor, the computer readable medium comprising code, executable by the processor.

[0035] The authorizing entity computer 160 is typically run by a business entity (e.g., a bank) that may have issued the payment (credit/debit) card, credentials or payment tokens used for the transactions. Some systems can perform both authorizing entity computer 160 and transport computer (not shown) functions. When a transaction involves a payment account associated with the authorizing entity computer 160, the authorizing entity computer 160 may verify the account and respond with an authorization response message to the transport computer (not

shown) that may be forwarded to the corresponding access device and the consumer device if applicable.

[0036] At a later time (e.g., at the end of the day), a clearing and settlement process can occur between the transport computer (not shown), the transaction processing computer 150, and the authorizing entity computer 160.

[0037] For simplicity of illustration, a certain number of components are shown in FIG. 1. It is understood, however, that embodiments of the invention may include more than one of each component. In addition, some embodiments of the invention may include fewer than or greater than all of the components shown in FIG. 1. In addition, the components in FIG. 1 may communicate via any suitable communication medium (including the Internet), using any suitable communications protocol.

[0038] FIG. 2 shows a flowchart of a method for performing push transactions according to embodiments of the present invention. FIG. 2 includes communication device 110, access device 120, resource provider computer 130, token server 140, transaction processing computer 150, and authorizing entity computer 160, of FIG. 1.

[0039] At step S210, a user of communication device 110 initiates a transaction with access device 120. The transaction may be, for example, for goods or services provided by a resource provider associated with access device 120. The communication device 110 does not initiate the transaction with access device 120 in response to a communication from the access device 120 or the resource provider associated with the access device 120. For example, the communication device 110 may request information from access device 120 that would allow communication device 110 to request that a payment request be pushed to the resource provider for the goods or services, without previously receiving a request for payment from the access device 120. In one embodiment, communication device 110 initiates the transaction with access device 120 using a digital wallet application, as described further herein. Communication device 110 may initiate the transaction with access device 120 by requesting information through a wired communications link or a wireless communications link (e.g., using NFC, WiFi or a cellular network).

[0040] At step S215, access device 120 generates or accesses a resource provider ID for the resource provider associated with access device 120. The

resource provider ID may be in any suitable form, such as in any combination of letters, numbers, symbols, and/or images, and may be included in a code, such as a QR code, a bar code, or any other scannable or interpretable code. The resource provider ID may include a name of the resource provider, a location of the resource provider, and/or contact information for the resource provider, in one embodiment. The contact information may include an IP address, e-mail address, or other electronic identifier of the resource provider computer 130 in one embodiment. For example, at step S215, access device 120 may be a web interface that generates and displays a QR code encoding a resource provider name and IP address to be used by communication device 110 to request that a payment request be pushed to the resource provider.

[0041] At step S220, access device 120 sends the resource provider ID (or the code including the resource provider ID) to communication device 110. At step S225, communication device 110 extracts the resource provider ID, when provided in an encoded format. For example, communication device 110 may decode or otherwise interpret the code to extract the underlying resource provider ID. At step S230, communication device 110 sends a transaction request to token server 140 including the resource provider ID and a credential with which the user of communication device 110 would like to complete the transaction. For example, the transaction request may be a request to push a payment to resource provider computer 130 for goods or services using a particular PAN.

[0042] At step S235, token server 140 determines whether a token exists for the credential, and either accesses the token associated with the credential if the token already exists, or generates a new token associated with the credential if the token does not already exist. At step S240, token server 140 pushes the token to resource provider computer 130 using the resource provider ID provided to it by communication device 110. For example, token server 140 may send a message to resource provider computer 130 including the token that notifies resource provider computer 130 that a payment using the token is ready to be accepted by the resource provider computer 130.

[0043] At step S245, resource provider computer 130 enters a transaction input value and generates an authorization request message with the token and the

transaction input value. The transaction input value may be, for example, a payment amount for the goods or services provided to the user associated with communication device 110. In other words, for example, the resource provider computer 130 may enter the payment amount after the transaction has been initiated by the user, and in one embodiment, after the goods or services have already been provided to the user. At step S250, resource provider computer 130 transmits the authorization request message including the token and the transaction input value to token server 140. The authorization request message may then be processed as a pull payment transaction.

[0044] At step S255, token server 140 locates the credential associated with the token, and replaces the token with the credential in the authorization request message. At step S260, token server 140 sends the authorization request message including the transaction input value and the credential to transaction processing computer 150, for further processing. Transaction processing computer 150 determines the authorizing entity associated with the credential, then at step S265 forwards the authorization request message including the transaction input value and the credential to the authorizing entity computer 160 for verification and authorization.

[0045] Once the transaction is authorized, the authorizing entity computer 160 may generate an authorization response message including the credential, and may transmit the authorization response message to transaction processing computer 150 at step S270. At step S275, the transaction processing computer 150 may forward the authorization response message to the token server 140. Upon receipt, the token server 140 may replace the credential in the authorization response message with its associated token at step S280.

[0046] At step S285, token server 140 may send the authorization response message including the token to resource provider computer 130 to indicate that the transaction was completed according to the transaction input value (e.g., for the entered amount). At step S290, a notification is sent by token server 140 to communication device 110 indicating that the transaction was completed. The notification may include the transaction input value entered by resource provider

computer 130, since this value may not have been previously provided to communication device 110.

[0047] At a later point in time (e.g., at the end of the day), a clearing and settlement process can be conducted between the transaction processing computer 150, the authorizing entity computer 160, and the transport computer (not shown) associated with resource provider computer 130. The resource provider computer 130 may first provide a file with the token and the associated transaction data (e.g., the transaction input value) to the transport computer. The transport computer may then transmit any clearing and settlement messages to the transaction processing computer 150 using the token. The token may then be converted to the credential as described above to facilitate the exchange of messages and the transfer of funds between the transport computer and the authorizing entity computer 160.

[0048] In other words, systems and methods according to an embodiment of the invention may be used to allow a user of a communication device to initiate a push payment transaction with a resource provider. The resource provider, instead of the user, may specify the payment amount for the transaction after the transaction has been initiated by the user, and in one embodiment, after the goods or services have already been provided to the user. The transaction may then be processed as a pull payment transaction.

[0049] A number of advantages are provided by processing transactions in this manner. For example, because the user initiates the transaction request, the user's PAN or other credential is protected from the merchant, as it is never provided to the merchant. In addition, the user can initiate payment to a remote merchant after receiving delivery of goods, whereas the merchant may otherwise not know the exact timing of delivery to request payment and/or may have no other means of accepting payment upon delivery (e.g., because deliverymen are not usually capable of processing payments). Because the transaction is ultimately processed as a pull payment transaction, little or no infrastructure changes are required by the transaction processing computer and the authorizing entity computer, which may not be configured to handle push payment transactions.

[0050] There are also benefits to allowing the resource provider to specify the payment amount after the user initiates the payment transaction. For example, the

user never needs to know the exact amount of the payment to request. This is advantageous in situations in which an exact payment amount is complicated (e.g., $1,274.18 instead of $1,000), or in which an exact payment amount is not known at the time of the initiation (e.g., the user initiates payment for hourly maid cleaning services that are not yet completed at the time of initial request; the user initiates payment for dinner at a restaurant, but has not yet specified a tip).

[0051] In addition, systems and methods according to an embodiment of the claimed invention reduce processing time for a transaction. For example, if the user or resource provider were to enter a payment amount when initiating the transaction, there would be a delay while the token was generated prior to processing the payment. Instead, because the token is already generated when the resource provider enters the payment amount, the payment can begin processing immediately once the payment amount is entered.

[0052] FIG. 3 shows a flowchart of another method for performing push transactions according to embodiments of the present invention. FIG. 3 includes communication device 110, access device 120, resource provider computer 130, token server 140, transaction processing computer 150, and authorizing entity computer 160, of FIG. 1.

[0053] At step S310, a user of communication device 110 initiates a transaction with access device 120. Step S310 may be similar to step S210 as described above. At step S315, access device 120 generates or accesses a resource provider ID. The resource provider ID may be as described above with respect to FIG. 2.

[0054] At step S320, access device 120 sends the resource provider ID (or the code including the resource provider ID) to communication device 110. At step S325, communication device 110 extracts the resource provider ID, when provided in an encoded format. At step S330, communication device 110 sends a transaction request to token server 140 including the resource provider ID and a credential with which the user of communication device 110 would like to complete the transaction. For example, the transaction request may be a request to pay resource provider computer 130 for goods or services using a particular credential (e.g., a PAN). Steps S320-S330 may be similar to steps S220-S230 as described above.

[0055] At step S335, token server 140 requests preauthorization of a threshold transaction input value (e.g., a capped amount) from transaction processing computer 150 using the credential. The capped amount may be determined according to any of a number of methods. In one embodiment, the capped amount may be specified by communication device 110 in the transaction request sent at step S330. In another embodiment, the capped amount may be set by token server 140. In the latter embodiment, the capped amount may be determined based on a type of resource provider associated with resource provider computer 130, and/or based on a location associated with the resource provider ID. For example, the capped amount may be set at $50 if the resource provider associated with resource provider computer 130 is a coffee shop, while the capped amount may be set at $3,000 if the resource provider is an electronics store. In another example, the capped amount may be set at $500 if the resource provider ID indicates that the resource provider is located in the United States, but may be set at $100 if the resource provider ID indicates that the resource provider is located outside of the United States, to reflect the higher risk of fraud for transactions associated with resource providers located outside of the United States.

[0056] At step S337, the transaction processing computer 150 determines the authorizing entity associated with the credential, then forwards the preauthorization request including the threshold transaction input value and the credential to the authorizing entity computer 160 for verification and preauthorization. At step S340, the authorizing entity computer 160 preauthorizes the transaction request, and sends the preauthorization response to the transaction processing computer 150. At step S343, the transaction processing computer 150 sends the preauthorization response including the threshold transaction input value and the credential to the token server 140.

[0057] At step S345, token server 140 determines whether a token exists for the credential, and either accesses the token associated with the credential if the token already exists, or generates a new token associated with the credential if the token does not already exist. At step S347, token server 140 sends the token to resource provider computer 130 using the resource provider ID provided to it by communication device 110. For example, token server 140 may send a message to

resource provider computer 130 including the token that notifies resource provider computer 130 that a payment using the token is ready to be accepted.

[0058] At step S350, resource provider computer 130 enters a transaction input value and generates an authorization request message with the token and the transaction input value. The transaction input value may be, for example, a payment amount for the goods or services provided to communication device 110. At step S353, resource provider computer 130 transmits the authorization request message including the token and the transaction input value to token server 140.

[0059] At step S355, token server 140 determines whether the transaction input value is within the threshold transaction input value (e.g., whether the amount entered by resource provider computer 130 is within the capped amount). If the transaction input value is within the threshold, token server 140 locates the credential associated with the token, and replaces the token with the credential in the authorization request message. At step S357, token server 140 sends the authorization request message including the transaction input value and the credential to transaction processing computer 150, for further processing. Transaction processing computer 150 determines the authorizing entity associated with the credential, then at step S360 forwards the authorization request message including the transaction input value and the credential to the authorizing entity computer 160 for verification and authorization.

[0060] Once the transaction is authorized, the authorizing entity computer 160 may generate an authorization response message including the credential, and may transmit the authorization response message to transaction processing computer 150 at step S363. At step S365, the transaction processing computer 150 may forward the authorization response message to the token server 140. Upon receipt, the token server 140 may replace the credential in the authorization response message with its associated token at step S367.

[0061] At step S370, token server 140 may send the authorization response message including the token to resource provider computer 130 to indicate that the transaction was completed according to the transaction input value (e.g., for the entered amount). At step S375, a notification is sent by token server 140 to communication device 110 indicating that the transaction was completed. The

notification may include the transaction input value entered by resource provider computer 130, since this value may not have been previously provided to communication device 110.

[0062] At a later point in time (e.g., at the end of the day), a clearing and settlement process can be conducted between the transaction processing computer 150, the authorizing entity computer 160, and the transport computer (not shown) associated with resource provider computer 130. The resource provider computer 130 may first provide a file with the token and the associated transaction data (e.g., the transaction input value) to the transport computer. The transport computer may then transmit any clearing and settlement messages to the transaction processing computer 150 using the token. The token may then be converted to the credential as described above to facilitate the exchange of messages and the transfer of funds between the transport computer and the authorizing entity computer 160.

[0063] In addition to those advantages described above, the embodiment of the invention described with respect to FIG. 3 provides a number of additional advantages. For example, by requesting preauthorization for a capped amount, embodiments of the invention guarantee and provide assurance that payment will be available for the resource provider up to that capped amount. In addition, the use of a capped amount reduces the risk of fraud by the resource provider, and/or limits the spending capacity of the resource provider to an expected amount. For example, by limiting resource providers located outside of the United States to $100, the likelihood of fraud is reduced because more fraudulent transactions are associated with foreign resource providers. In another example, by limiting certain types of resource providers to maximum expected amounts (e.g., a coffee shop to $50), those resource providers are not able to fraudulently or accidentally request higher, potentially unjustified payment amounts.

[0064] FIG. 4 shows a block diagram of a communication device 400 according to embodiments of the present invention. Communication device 400 may be used to implement communication device 110 of FIG. 1, for example. Communication device 400 may include device hardware 404 coupled to a memory 402. Device hardware 404 may include a processor 405, a communications subsystem 409, and a user interface 406. In some embodiments, device hardware

404 may include a display 407 (which can be part of user interface 406). Device hardware 404 may also include a contactless interface 408, for example, in some embodiments in which communication device 400 is a portable communication device. Processor 405 can be implemented as one or more integrated circuits (e.g., one or more single core or multicore microprocessors and/or microcontrollers), and is used to control the operation of communication device 400. Processor 405 can execute a variety of programs in response to program code or computer-readable code stored in memory 402, and can maintain multiple concurrently executing programs or processes. Communications subsystem 409 may include one or more RF transceivers and/or connectors that can be used by portable communication device 400 to communicate with other devices and/or to connect with external networks. User interface 406 can include any combination of input and output elements to allow a user to interact with and invoke the functionalities of communication device 400. In some embodiments, user interface 406 may include a component such as display 407 that can be used for both input and output functions.

[0065] Contactless interface 408 may include one or more specialized RF transceivers (e.g., near field communication (NFC) transceivers) to interact with a contactless reader of an access device to conduct a transaction (e.g., payment transaction, access transaction, information exchange, etc.). In secure element based implementations, only a secure element (not shown) may have access to contactless interface 408. In some embodiments, contactless interface 408 can be accessed by the mobile OS 420 using specialized card emulation APIs 422 without requiring the use of a secure element. In some embodiments, display 407 can also be part of contactless interface 408, and is used, for example, to perform transactions using QR codes, bar codes, etc.

[0066] Memory 402 can be implemented using any combination of any number of non-volatile memories (e.g., flash memory) and volatile memories (e.g., DRAM, SRAM), or any other non-transitory storage medium, or a combination thereof media. Memory 402 may store an operating system (OS) 420 and an application environment 410 where one or more applications reside including application 412 to be executed by processor 405. In some embodiments, OS 420 may implement a set of card emulation APIs 422 that can be invoked by application 412 to access contactless interface 408 to interact with an access device.

[0067] Application 412 can include an application that uses, accesses, and/or stores sensitive information, such as credentials or tokens. For example, application 412 can include a digital wallet or payment application that uses credentials (e.g., a token and/or payment credentials) to conduct transactions via communication device 400. In some embodiments, access to application 412 by a user can be protected by user authentication data such as a password, passcode, PIN, etc. For example, when a user attempts to launch or execute application 412, the user may be requested to enter valid user authentication data before the user can access application 412. Application 412 may include a download manager 418, a cryptography module 414, a credential (e.g., token and/or payment credentials) data store 415, and/or a code translation module 416. In some embodiments, one or more of these components can be provided by another application or component that is not part of application 412.

[0068] Download manager 418 can be programmed to provide functionalities to communicate with an application provider associated with application 412 to download information via the application provider. Download manager 418 working in conjunction with the processor 405 may request or otherwise manage the acquisition and/or storage of credentials. For example, download manager 418 working in conjunction with the processor 405 may request and obtain credentials via the application provider associated with application 412, and store the credentials in credential data store 415. In some embodiments, the credentials provided by the application provider can be received in an encrypted form. For example, the credentials can be encrypted with a session key generated by a server computer. Download manager 418 working in conjunction with the processor 405 may also receive, from the application provider, the session key in an encrypted form, and store the encrypted session key in credential data store 415.

[0069] Cryptography module 414 working in conjunction with the processor 405 may provide cryptographic functionalities for application 412. For example, cryptography module 414 may implement and perform encryption/decryption operations for application 412 using encryption algorithms such as DES, AES, TDES, or the like, and/or hash functions such as SHA, or the like. For example, when application 412 accesses credential data store 415 to retrieve and use the credentials stored therein (e.g., to conduct a transaction), application 412 may

invoke cryptography module 414 to decrypt the session key that is used to encrypt the stored credentials, and then decrypt the credentials using the decrypted session key. The decrypted credentials can then be used by application 412.

[0070] Code translation module 416, in conjunction with processor 405, may receive and translate codes containing underlying data. For example, code translation module 416 may, in conjunction with processor 405, interpret a code (e.g., a QR code, a bar code, etc.) to extract a resource provider ID. The resource provider ID may include a name of the resource provider, a location of the resource provider, and/or contact information for the resource provider, in one embodiment. The contact information may include an IP address, e-mail address, or other electronic identifier of the resource provider computer 130, for example. In one embodiment, the code is scannable by a camera (not shown) contained in device hardware 404 of communication device 400.

[0071] FIG. 5 illustrates a block diagram of a token server 500 according to embodiments of the present invention. Token server 500 may be used to implement token server 140 of FIG. 1, for example. In some embodiments, one or more token servers 500 can be used, for example, to implement a network token system. Token server 500 may include a processor 501 coupled to a network interface 502 and a computer readable medium 506. In some embodiments, token server computer 500 may also include a hardware security module (HSM) 520. Token server 500 may also include a token database 503 that may be internal or external to token server 500.

[0072] Processor 501 may include one or more microprocessors to execute program components for performing the management functions 530 of token server 500. Network interface 502 may be configured to connect to one or more communication networks to allow token server 500 to communicate with other entities such as a communication device operated by a user, an application provider computer or a token request computer, resource provider computer, transport computer, transaction processing network computer, authorizing entity computer, etc. Computer readable medium 506 may include any combination of one or more volatile and/or non-volatile memories, for example, RAM, DRAM, SRAM, ROM, flash, or any other suitable memory components. Computer readable medium 506

may store code executable by the processor 501 for implementing some or all of the management functions 530 of token server 500 described herein. For example, computer readable medium 506 may include a requestor registration module 508, a user registration module 510, a token generation module 512, a verification and authentication module 514, a token exchange and routing module 516, a token life-cycle management module 518, and a threshold transaction input value determination module 519.

[0073] Requestor registration module 508 may, in conjunction with processor 501, register a token requestor entity (e.g., application provider) with the token database 503, and to generate a token requestor identifier (ID) for the registered entity. Each registered entity can use their respective token requestor ID as part of a token service request to facilitate identification and validation of the entity. In some embodiments, a token requestor entity may provide token requestor information to the requestor registration module 508 such as an entity name, contact information, an entity type (e.g., resource provider, digital wallet provider, payment service provider, authorizing entity, payment enabler, acquirer, etc.). In some embodiments in which the token is transaction related, the token requestor information may also include token presentment modes (e.g., scan, contactless, e-commerce, etc.), token type (e.g., static/dynamic, payment/non-payment), integration and connectivity parameters, and services subscribed (e.g., token request, authentication and verification, life-cycle management, etc.) and any other relevant information for the onboarding process.

[0074] User registration module 510 may, in conjunction with processor 501, perform registration of users and accounts of the users. In some embodiments, token server 500 may allow authorized entities to register credentials (e.g., payment or financial accounts) with the network token system on behalf of the users. For example, a registered token requestor may provide a token requestor ID (e.g., received at the time of registration from the requestor registration module 508), a credential or other sensitive information or sensitive information identifier for which a token can substitute, a consumer name and contact information, device identifier of the consumer's communication device, a token type, and any other relevant information for individual account registration or bulk account registration. In some embodiments, user registration module 510 may store the account details and

sensitive information in token database 503 for all successful activation and registration requests. In some embodiments, an authorized entity may also unregister users and accounts by providing the necessary information to token server 500.

[0075] Token generation module 512 can, in conjunction with processor 501, generate a token or retrieve sensitive information in response to processing a request for a token or sensitive information from a token requestor (e.g., an application provider). In some embodiments, token generation module 512 may receive a token requestor ID and an account identifier or sensitive information identifier. In some embodiments, token generation module 512 may also receive optional information such as a user name, a user address and zip code, a requested token or sensitive information type (e.g., static, dynamic, non-payment, etc.), device identifier, and/or suitable information. In some embodiments, token generation module 512 may, in conjunction with processor 501, generate a response with the requested token or requested sensitive information, a token expiration date associated with the token, and/or a token assurance level associated with the token. In some embodiments, token generation module 512 may, in conjunction with processor 501, validate the token requestor ID and maintain the correlation between the token, the sensitive information or account identifier being substituted by the token, and the associated token requestor. In some embodiments, token generation module 512 may, in conjunction with processor 501, determine if a token already exists in token database 503 for a token request before generating a new token. In some embodiments, if a token cannot be provisioned, the token response may include a corresponding reason code. In some embodiments, token generation module 512 may also, in conjunction with processor 501, provide an interface to the token requestors to submit a bulk token request file.

[0076] In some embodiments, the token may be generated on the fly using API calls. For example, when a request is received to tokenize an account identifier or other sensitive information, token generation module 512 may, in conjunction with processor 501, determine a token range to assign the token. The token range may be assigned based on whether the issuer is provisioning the token (e.g., issuer assigned token range) or the transaction processing network is provisioning the token on behalf of the issuer (e.g., transaction processing network assigned token

range). As an example, if the transaction processing network assigned token range includes "442400000-442400250," then "4424000000005382" may be assigned as a token value. Token database 503 may store the relationship of the token range to the account identifier, and a token add record may be logged. In some embodiments, token generation module 512 may, in conjunction with processor 501, consider the token range list associated with the account identifier range before assigning a token.

[0077] Verification and authentication module 514 may, in conjunction with processor 501, execute a consumer verification and authentication process, and determine a token assurance level based on the outcome of the verification and authentication process. For example, the verification and authentication module 514 can perform consumer authentication and verification through a configured authentication scheme. In some embodiments, the authentication scheme may include verification of the account identifier, verification values, and the expiration date based on the customer information stored in a database associated with the transaction processing network. In some embodiments, the authentication scheme may include direct verification of the consumer by the issuer using consumer credentials for their online banking system.

[0078] In some embodiments, the authentication scheme may include verification of the consumer credentials through the issuer ACS (Access Control Server). For example, the issuer ACS service may be part of an authentication protocol such as 3-D secure protocol by Visa®. The ACS server may be associated with an issuer that may include registered consumer account and access information. The ACS can give issuers the ability to authenticate a consumer during an online purchase, thereby reducing the likelihood of fraudulent use of the consumer account. For example, the ACS can validate that the consumer is registered, performs consumer verification at the time of the transaction, and provides digitally signed responses to the resource providers. In some embodiments, the authentication scheme may include verification of the account using a transaction processing network consumer authentication service (e.g., Visa™ Consumer Authentication Service (VCAS)). For example, the VCAS service can authenticate the consumer on-behalf of the issuer prior to the authorization process.

[0079] In some embodiments, user registration, token generation, and verification and authentication may be performed as part of processing a single token request process. In some embodiments, for bulk requests, user registration and token generation may be performed by processing a bulk file from the token requestor. In such embodiments, consumer verification and authentication may be performed in a separate step. In some embodiments, the token requestor can request that the authentication and verification process be performed independently multiple times for a particular account to reflect any changes to the levels of assurance for the token over time.

[0080] Token exchange and routing module 516 may, in conjunction with processor 501, process requests for the underlying sensitive information (e.g., a credential) associated with a given token. For example, a transaction processing network, acquirer, issuer, etc. may issue a request for a token exchange during processing of a transaction. Token exchange and routing module 516 may, in conjunction with processor 501, validate that the requesting entity is entitled to make a request for a token exchange. In some embodiments, token exchange and routing module 516 may, in conjunction with processor 501, validate the credential (or other sensitive information) to token mapping and presentment mode based on the transaction timestamp and the token expiration timestamp. Token exchange and routing module 516 may, in conjunction with processor 501, retrieve the credential (or other sensitive information) from token database 503, and provide it along with the assurance level to the requesting entity. In some embodiments, if the credential (or other sensitive information) to token mapping is not valid for the transaction timestamp and presentment mode, an error message may be provided.

[0081] Token life-cycle management module 518 may, in conjunction with processor 501, perform life-cycle operations on the tokens managed by token server 500. Life-cycle operations may include canceling a token, activating or deactivating a token, updating token attributes, renewing token with a new expiration date, etc. In some embodiments, a token requestor entity may provide a token requestor ID, a token number, a life-cycle operation identifier and one or more token attributes to token server 500 to perform the requested life-cycle operation on a given token. Token life-cycle management module 518 may, in conjunction with processor 501, verify the token requestor ID and the token association based on information in token

database 503. Token life-cycle management module 518 may, in conjunction with processor 501, perform the requested life-cycle operation on a given token, and update the corresponding associations in token database 503. Examples of life-cycle operations may include a token activation operation to activate an inactive, suspended, or temporarily locked token and its associations; a token de-activation operation to temporarily lock or suspend a token; a cancel token operation to permanently mark a token and its associations as deleted to prevent any future transactions, etc. In some embodiments, a deleted token may be used during returns/chargebacks if the same token was used to submit the corresponding original transactions.

[0082] Threshold transaction input value determination module 519 may, in conjunction with processor 501, determine a threshold transaction input value for a particular transaction in one embodiment. The threshold transaction input value (e.g., a capped amount) may be determined based on a type of resource provider associated with resource provider computer 130, and/or based on a location associated with the resource provider ID. For example, the capped amount may be set at $50 if the resource provider is a coffee shop, while the capped amount may be set at $3,000 if the resource provider is an electronics store. In another example, the capped amount may be set at $500 if the resource provider ID indicates that the resource provider is located in the United States, but may be set at $100 if the resource provider ID indicates that the resource provider is located outside of the United States. In one embodiment, the threshold transaction input value is determined based on a fraud risk.

[0083] According to some embodiments, token server 500 may include a HSM 520 to perform secure functions such as encryption and decryption operations and generation of cryptographic keys used for the encryption and decryption operations. For example, HSM 520 may include a cryptography engine 522 to, in conjunction with processor 501, execute encryption algorithms such as AES, DES, TDES/TDEA, or other suitable encryption algorithms using cryptographic keys of any length (e.g., 56-bit, 128-bit, 169-bit, 192-bit, 256-bit, etc.). HSM 520 may also implement a session key generator 524 to, in conjunction with processor 501, generate a session key for each token or sensitive information request that token server 500 processes. The generated session key can be used to encrypt a token or sensitive information

generated or retrieved for the request, and the token or sensitive information can be provided to the token requestor in an encrypted form. For example, for each request that token server 500 receives and processes, session key generator 524 may, in conjunction with processor 501, generate a session key that can be unique for each request received from the particular token requestor, or unique to each request associate with a particular user or account. In some embodiments, the session key can be the same or different than the encryption key that is used to establish the secure communication channel (e.g., TLS, SSL, etc.) between the token requestor and token server computer 500. Token generation module 512 may generate or otherwise retrieve a token or sensitive information to fulfill the request. The session key can be used by cryptographic engine 522 to encrypt that token or sensitive information using an encryption algorithm, and the encrypted token or sensitive information can be provided to the token requestor. In some embodiments, the generated session key is also provided to the token requestor with the encrypted token or sensitive information.

[0084] Although token server 500 has been described with a HSM implementing only some of their functions, it should be understood that other functionalities of the respective computers (e.g., token generation) can be implemented inside a HSM as well. Furthermore, some or all of the respective HSM functionalities can also be implemented outside of a HSM.

[0085] A computer system may be used to implement any of the entities or components described above. The subsystems of the computer system may be interconnected via a system bus. Additional subsystems such as a printer, keyboard, fixed disk (or other memory comprising computer readable media), monitor, which is coupled to display adapter, and others may be used. 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 a serial port. For example, a 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.

[0086] A computer system can include a plurality of the same components or subsystems, e.g., connected together by an 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.

[0087] 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.

[0088] 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.

[0089] 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.

[0090] 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. For example, although specific functions and methods have been described with respect to token server 500 in FIG. 5, such functions could be performed by other computers such as the transaction processing computer 150.

[0091] 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.

[0092] A recitation of "a", "an" or "the" is intended to mean "one or more" unless specifically indicated to the contrary.

[0093] 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:

receiving, at a server computer from a communication device operated by a user, a transaction request including a credential and a resource provider ID associated with a resource provider computer, wherein the communication device did not initiate the transaction request in response to a communication from the resource provider computer;

transmitting a token corresponding to the credential to the resource provider computer using the resource provider ID, wherein a transaction input value is entered into the resource provider computer after the token is received at the resource provider computer;

receiving the token and the transaction input value; and

processing the transaction request in accordance with the transaction input value.

2. The method of claim 1, wherein the resource provider ID comprises at least one of an identifier code and a location.

3. The method of claim 1, wherein processing the transaction request comprises:

converting the token into the credential; and

initiating authorization of the transaction request using the credential in accordance with the transaction input value.

4. The method of claim 1, further comprising:

sending a completion message for the transaction request to the communication device.

5. The method of claim 1, further comprising:

determining a threshold transaction input value; and

initiating preauthorization for the threshold transaction input value using the credential,

wherein the transaction input value is within the threshold transaction input value.

6. The method of claim 5, wherein the threshold transaction input value is determined based on at least one of a type of resource provider associated with the resource provider computer and a location associated with the resource provider ID.

7. A server computer comprising:

a processor; and

a memory coupled to the processor, the memory storing instructions, which when executed by the processor, cause the server computer to perform operations including:

receiving, from a communication device operated by a user, a transaction request including a credential and a resource provider ID associated with a resource provider computer, wherein the communication device did not initiate the transaction request in response to a communication from the resource provider computer;

transmitting a token corresponding to the credential to the resource provider computer using the resource provider ID, wherein a transaction input value is entered into the resource provider computer after the token is received at the resource provider computer;

receiving the token and the transaction input value; and

processing the transaction request in accordance with the transaction input value.

8. The server computer of claim 7, wherein the resource provider ID comprises at least one of an identifier code and a location.

9. The server computer of claim 7, wherein processing the transaction request comprises:

converting the token into the credential; and

initiating authorization of the transaction request using the credential in accordance with the transaction input value.

10. The server computer of claim 7, wherein the operations further include:

sending a completion message for the transaction request to the communication device.

11. The server computer of claim 7, wherein the operations further include:

determining a threshold transaction input value; and

initiating preauthorization for the threshold transaction input value using the credential,

wherein the transaction input value is within the threshold transaction input value.

12. The server computer of claim 11, wherein the threshold transaction input value is determined based on at least one of a type of resource provider associated with the resource provider computer and a location associated with the resource provider ID.

13. A method comprising:

providing, by a resource provider computer to a communication device, transaction data including a resource provider ID associated with the resource provider computer, wherein the communication device thereafter sends a transaction request including a credential and the resource provider ID to a server computer;

receiving, by the resource provider computer, a token corresponding to the credential from the server computer, wherein the server computer sends the token to the resource provider computer using the resource provider ID; and

sending, by the resource provider computer, a transaction input value and the token to the server computer, wherein the server computer thereafter processes the transaction request in accordance with the transaction input value.

14. The method of claim 13, wherein the resource provider ID comprises at least one of an identifier code and a location.

15. The method of claim 13, wherein the server computer processes the transaction request by:

converting the token into the credential; and

initiating authorization of the transaction request using the credential in accordance with the transaction input value.

16. The method of claim 13, wherein the server computer sends a completion message for the transaction request to the communication device after processing the transaction request.

17. The method of claim 13, wherein before sending the token to the resource provider computer, the server computer determines a threshold transaction input value, and initiates preauthorization for the threshold transaction input value using the credential,

wherein the transaction input value is within the threshold transaction input value.

18. The method of claim 17, wherein the threshold transaction input value is determined based on at least one of a type of resource provider associated with the resource provider computer and a location associated with the resource provider ID.

19. A first server computer comprising:

a processor; and

a memory coupled to the processor, the memory storing instructions, which when executed by the processor, cause the server computer to perform operations including:

providing, to a communication device, transaction data including a resource provider ID associated with the resource provider computer, wherein the communication device thereafter sends a transaction request including a credential and the resource provider ID to a second server computer;

receiving a token corresponding to the credential from the second server computer, wherein the second server computer sends the token to the first server computer using the resource provider ID; and

sending a transaction input value and the token to the second server computer, wherein the second server computer thereafter processes the transaction request in accordance with the transaction input value.

20. The first server computer of claim 19, wherein the resource provider ID comprises at least one of an identifier code and a location.

21. The first server computer of claim 19, wherein the second server computer processes the transaction request by:

converting the token into the credential; and

initiating authorization of the transaction request using the credential in accordance with the transaction input value.

22. The first server computer of claim 19, wherein the second server computer sends a completion message for the transaction request to the communication device after processing the transaction request.

23. The first server computer of claim 19, wherein before sending the token to the first server computer, the second server computer determines a threshold transaction input value, and initiates preauthorization for the threshold transaction input value using the credential,

wherein the transaction input value is within the threshold transaction input value.

24. The first server computer of claim 23, wherein the threshold transaction input value is determined based on at least one of a type of resource provider associated with the first server computer and a location associated with the resource provider ID.

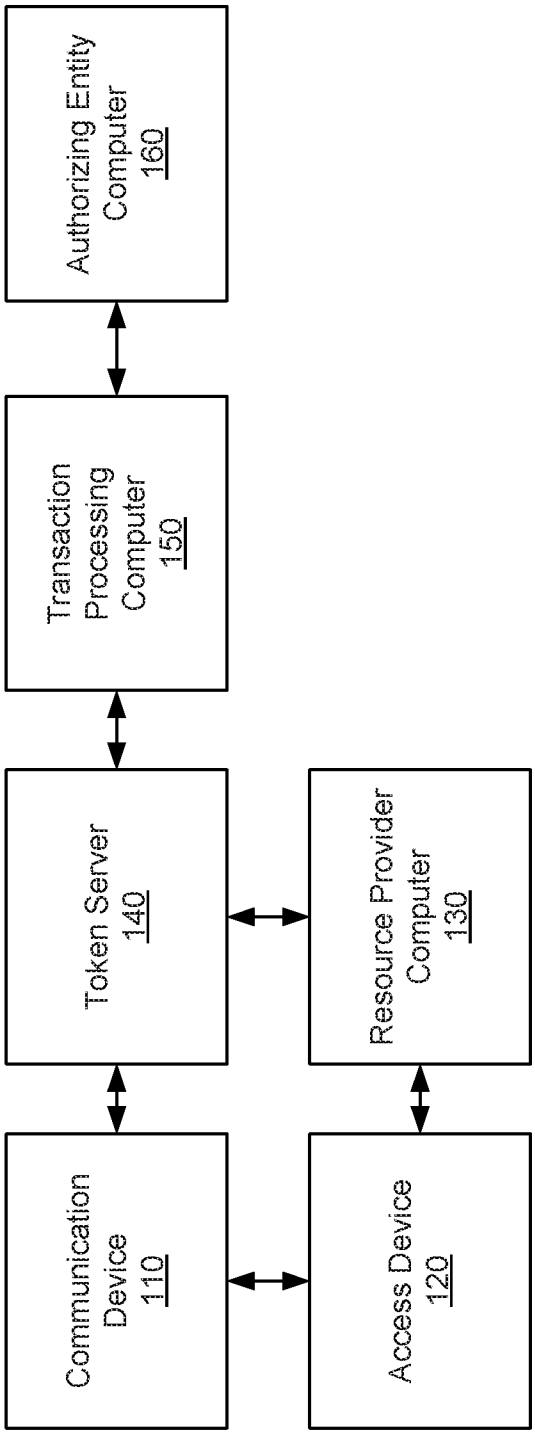
Authorizing Entity Computer 160
Transaction Processing Computer 150
Token Server 140
Resource Provider Computer 130
Communication Device 110
Access Device 120
100

FIG. 1

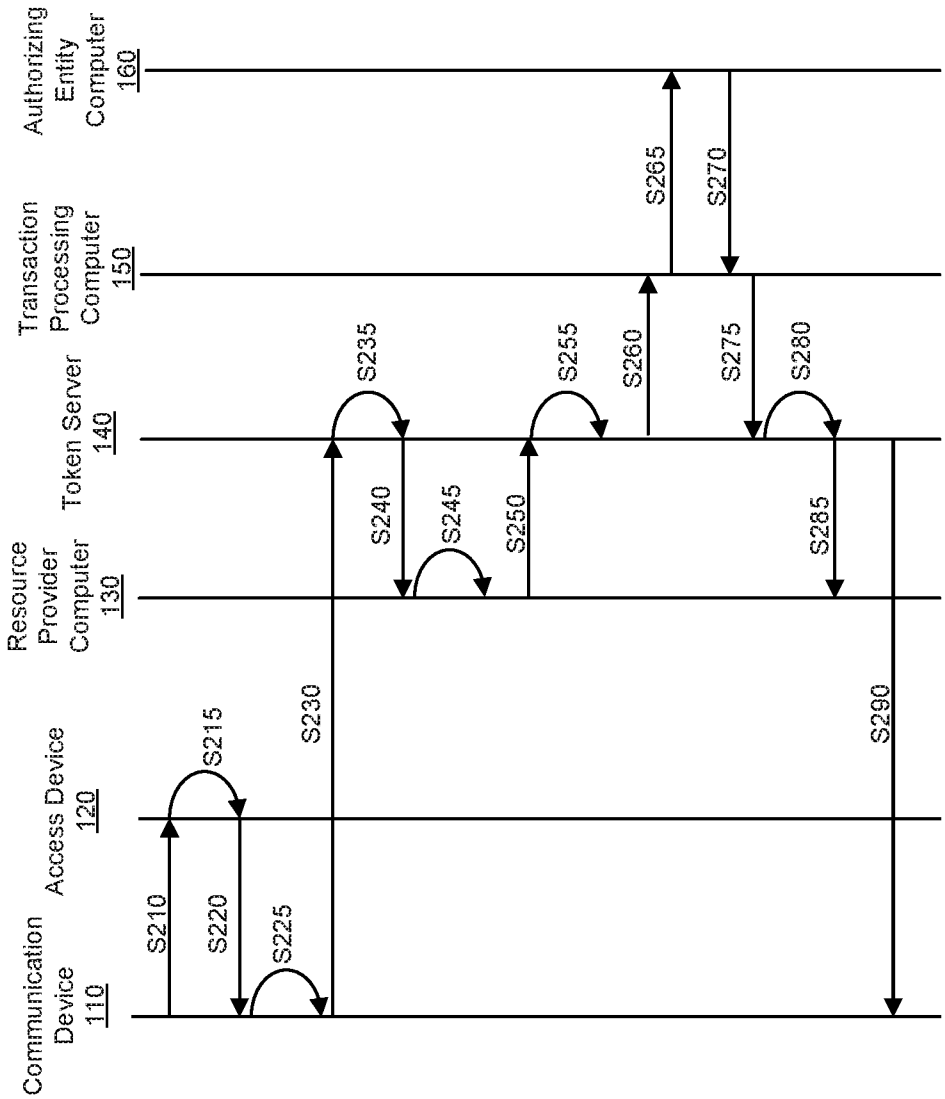
Communication Device 110
Access Device 120
Resource Provider Computer 130
Token Server 140
Transaction Processing Computer 150
Authorizing Entity Computer 160
S210
S215
S220
S225
S230
S235
S240
S245
S250
S255
S260
S265
S270
S275
S280
S285
S290

FIG. 2

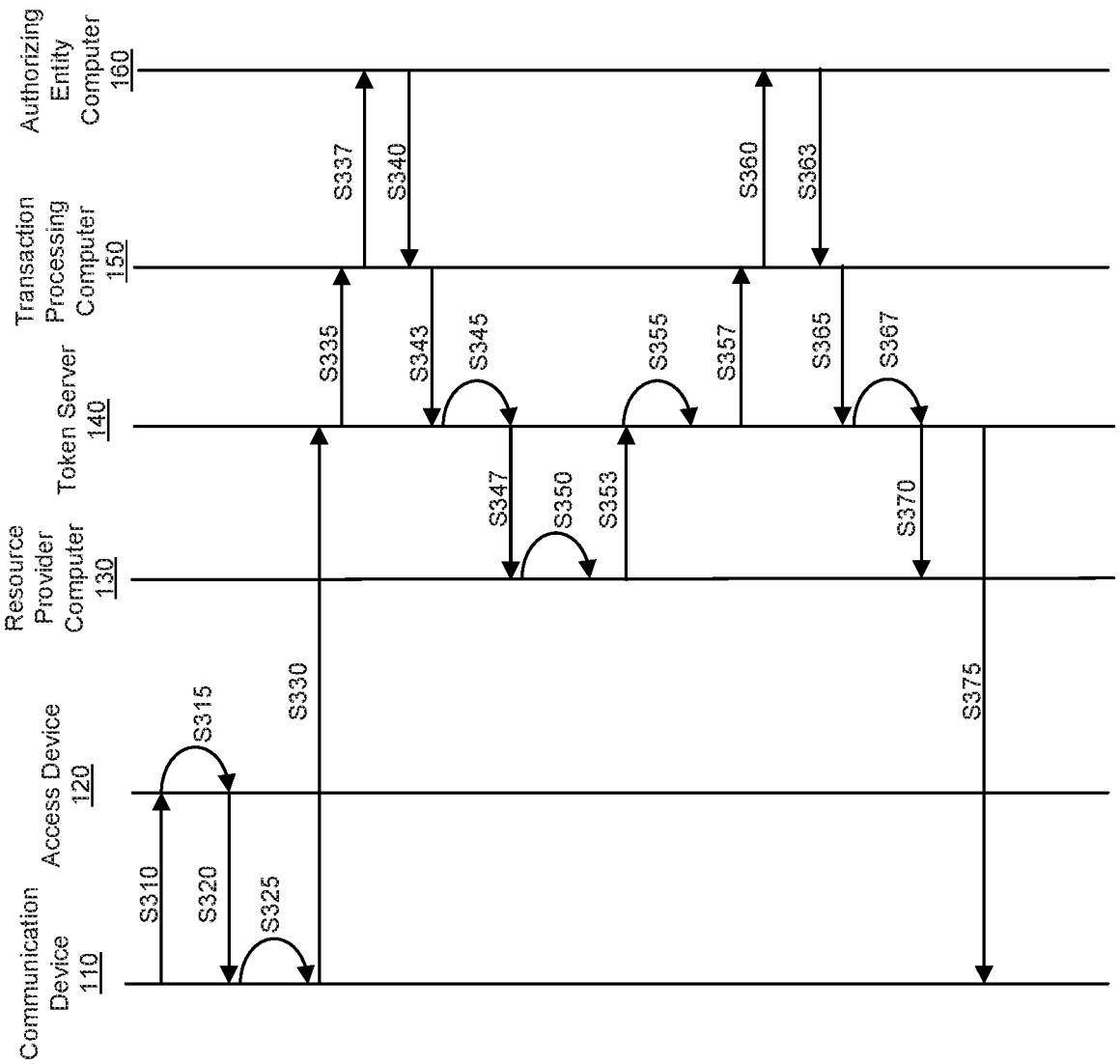
Communication Device 110
Access Device 120
Resource Provider Computer 130
Token Server 140
Transaction Processing Computer 150
Authorizing Entity Computer 160
S310
S315
S320
S325
S330
S335
S337
S340
S343
S345
S347
S350
S353
S355
S357
S360
S363
S365
S367
S370
S375

FIG. 3

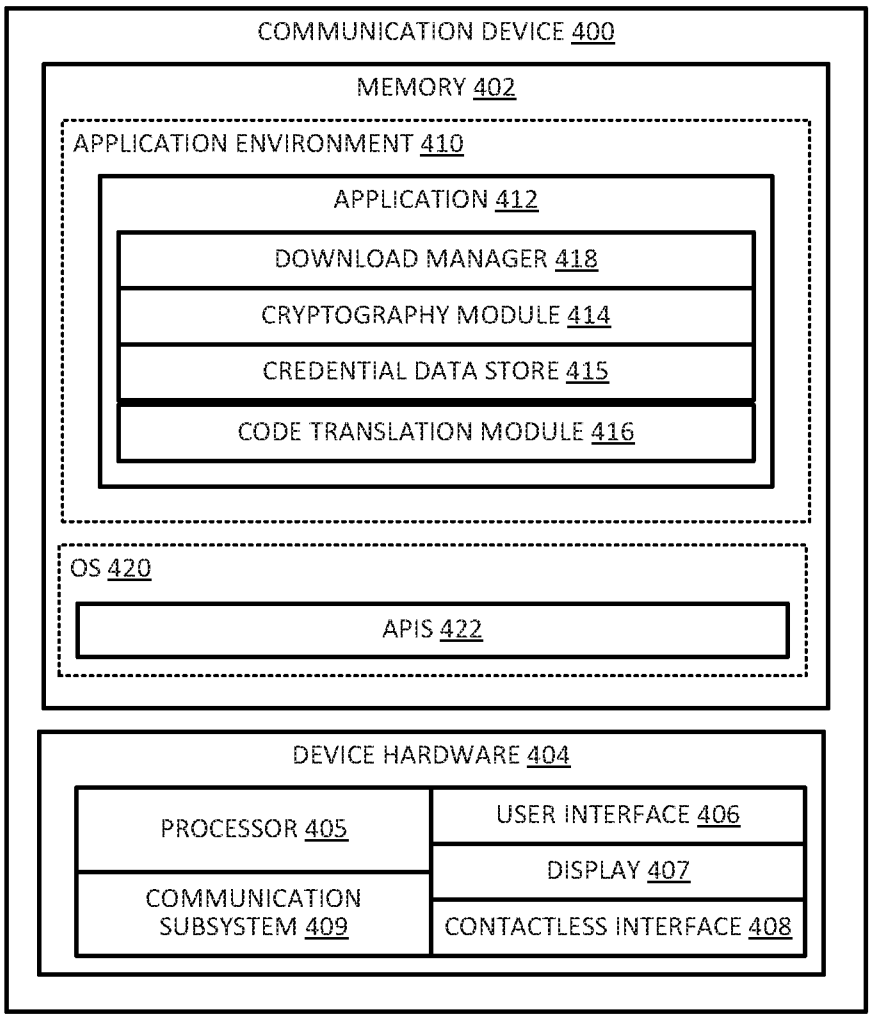
COMMUNICATION DEVICE 400
MEMORY 402
APPLICATION ENVIRONMENT 410
APPLICATION 412
DOWNLOAD MANAGER 418
CRYPTOGRAPHY MODULE 414
CREDENTIAL DATA STORE 415
CODE TRANSLATION MODULE 416
OS 420
APIS 422
DEVICE HARDWARE 404
PROCESSOR 405
USER INTERFACE 406
DISPLAY 407
COMMUNICATION SUBSYSTEM 409
CONTACTLESS INTERFACE 408

FIG. 4

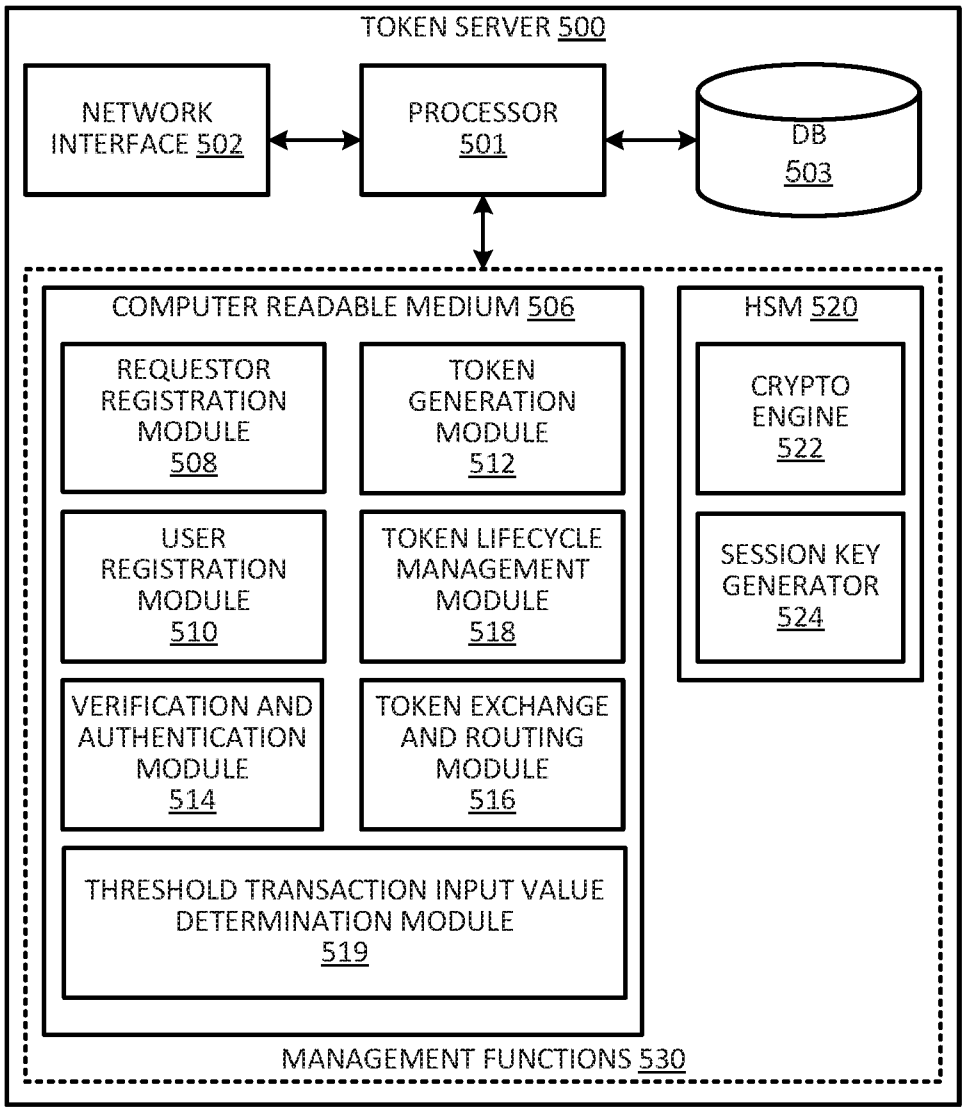
TOKEN SERVER 500
NETWORK INTERFACE 502
PROCESSOR 501
DB 503
COMPUTER READABLE MEDIUM 506
REQUESTOR REGISTRATION MODULE 508
TOKEN GENERATION MODULE 512
USER REGISTRATION MODULE 510
TOKEN LIFECYCLE MANAGEMENT MODULE 518
VERIFICATION AND AUTHENTICATION MODULE 514
TOKEN EXCHANGE AND ROUTING MODULE 516
THRESHOLD TRANSACTION INPUT VALUE DETERMINATION MODULE 519
HSM 520
CRYPTO ENGINE 522
SESSION KEY GENERATOR 524
MANAGEMENT FUNCTIONS 530

FIG. 5

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2016/028276

A. CLASSIFICATION OF SUBJECT MATTER

G06Q 20/38(2012.01)i, G06Q 20/08(2012.01)i

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06Q 20/38; G06Q 20/40; G06F 12/14; G06Q 20/32; H04L 9/32; G06Q 20/00; G06Q 20/08

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Korean utility models and applications for utility models
Japanese utility models and applications for utility models

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
eKOMPASS(KIPO internal) & Keywords: transaction, processing, resource, provider, ID, token, input, value

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2014-0040148 A1 (MERCURY PAYMENT SYSTEMS, LLC) 06 February 2014 See paragraphs [0016],[0045],[0057],[0106], claim 1 and figures 1,4.	1-24
Y	US 2014-0149293 A1 (KEVIN LARACEY) 29 May 2014 See paragraphs [0015],[0030],[0038],[0044],[0060], claims 1,6,10 and figure 1.	1-24
A	US 6327578 B1 (MARK LINEHAN) 04 December 2001 See abstract, claims 1-2 and figures 2A-3.	1-24
A	KR 10-2016-0015375 A (VISA INTERNATIONAL SERVICE ASSOCIATION) 12 February 2016 See abstract, claims 1-2,10-11 and figure 1.	1-24
A	US 2009-0198617 A1 (CHRISTOPHER SOGHOIAN et al.) 06 August 2009 See abstract, claims 1,3,5 and figure 1.	1-24

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

☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents,such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
09 January 2017 (09.01.2017)	**10 January 2017 (10.01.2017)**

Name and mailing address of the ISA/KR
International Application Division
Korean Intellectual Property Office
189 Cheongsa-ro, Seo-gu, Daejeon, 35208, Republic of Korea
Facsimile No. +82-42-481-8578

Authorized officer
JANG, Gijeong
Telephone No. +82-42-481-8364

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/US2016/028276

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2014-0040148 A1	06/02/2014	WO 2015-017736 A1	05/02/2015
US 2014-0149293 A1	29/05/2014	US 2016-0048830 A1	18/02/2016
		US 9208482 B2	08/12/2015
US 6327578 B1	04/12/2001	EP 1017030 A2	05/07/2000
		EP 1017030 A3	03/12/2003
		JP 2000-194770 A	14/07/2000
		KR 10-0349779 B1	22/08/2002
		KR 10-2000-0048436 A	25/07/2000
		US RE40444 E1	29/07/2008
KR 10-2016-0015375 A	12/02/2016	AU 2014-285774 A1	07/01/2016
		CN 105518732 A	20/04/2016
		EP 3017413 A1	11/05/2016
		EP 3017413 A4	13/07/2016
		US 2016-0132880 A1	12/05/2016
		WO 2015-001473 A1	08/01/2015
US 2009-0198617 A1	06/08/2009	CN 101388095 A	18/03/2009
		EP 2026266 A1	18/02/2009
		EP 2026266 B1	16/02/2011
		JP 2009-048627 A	05/03/2009