Technical Disclosure Commons

Defensive Publications Series

July 2020

METHOD AND SYSTEM FOR USING VIRTUAL ACCOUNT

Minghua Xu
Visa

Follow this and additional works at: https://www.tdcommons.org/dpubs_series

Recommended Citation
Xu, Minghua, "METHOD AND SYSTEM FOR USING VIRTUAL ACCOUNT", Technical Disclosure Commons, (July 21, 2020)
https://www.tdcommons.org/dpubs_series/3442

This work is licensed under a Creative Commons Attribution 4.0 License.
This Article is brought to you for free and open access by Technical Disclosure Commons. It has been accepted for inclusion in Defensive Publications Series by an authorized administrator of Technical Disclosure Commons.

TITLE “METHOD AND SYSTEM FOR USING VIRTUAL ACCOUNT”

VISA

MINGHUA XU

TECHNICAL FIELD

[0001] The present disclosure relates generally to virtual accounts. More particularly, the present disclosure relates to a method and a system for using a virtual account with invoice data.

BACKGROUND

[0002] Currently, there are different payment methods for performing transactions such as business-to-business transactions and the like. Few common payment methods include cash, check, Automated Clearing House (ACH) payment, Society for Worldwide Interbank Financial Telecommunications (SWIFT) payment, payment card (e.g., credit card, debit card, and/or the like), and online payment services (e.g., PayPal™ and/or the like). Conducting payment transactions by cash is inconvenient and cause delays. For example, a buyer may withdraw cash from a bank, may take measures to (securely) store cash, may manually count cash to match a desired transaction amount (e.g., from an invoice and/or the like), and/or may manually transfer (e.g., hand deliver, send by courier, send by mail, and/or the like). The above procedures take considerable time and/or require considerable resources (e.g., manual efforts, security measures, and/or the like). Additionally or alternatively, a supplier may manually retrieve the cash, may take measures to (securely) store the cash, may deposit cash into its bank, and/or the like, all of which takes considerable time and/or require considerable resources. Checks also may be inconvenient or cause delays. For example, a buyer must monitor the balance of checking accounts to ensure there are sufficient funds to cover outstanding checks, may have to manually write checks for desired amounts (e.g., from an invoice and/or the like), and may manually transfer (e.g., hand deliver, send by courier, send by mail, and/or the like), all of which may take considerable time and/or require considerable resources. Additionally or alternatively, a supplier may manually retrieve the check, may deposit the check into a bank, may wait several days for the check to clear, may bear some risk if the check does not clear (e.g., due to insufficient funds and/or the like), and/or the like, all of which takes considerable time and/or require considerable resources.

[0003] Electronic payments (e.g., ACH, SWIFT, and/or the like) allows direct transfers between bank accounts of the buyer and the supplier. However, the parties (e.g., buyer, supplier, and/or the like) need to closely monitor their respective account balances to avoid over drafting the account. Additionally or alternatively, the parties need to monitor their respective account balances to avoid over funding (e.g., if an excess of money is accumulated in an account, that money is not available and/or being used for other facets of the business that would benefit from additional monetary resources).

[0004] Online payment services (e.g., PayPal™ and/or the like) requires each party (e.g., buyer, supplier, and/or the like) to manually set up online accounts (e.g., in addition to their respective payment accounts), which needs to be separately monitored (e.g., manually). Additionally or alternatively, such online payment services may charge additional fees (e.g., in addition to fees of the payment accounts, such as checking accounts, credit card accounts, and/or the like), may add additional overhead to the transaction, may cause delays (e.g., waiting for the transfer to clear the payment account of each respective party). Also, the online payment services may require at least one of the parties to manually enter the transaction details (e.g., transaction amount, identities of parties, payment account information, and/or the like), and/or the like.

[0005] Conducting transactions by payment card (e.g., credit card and/or the like) between remote parties (e.g., buyer, supplier, and/or the like) may include manually conveying (e.g., by telephone, mail, courier, email, and/or the like) sensitive payment card information (e.g., account identifier, expiration date, security code (such as card verification value (CVV) code and/or the like), and/or the like). Conveyance of such sensitive information elevates the risk to the parties (e.g., risk that sensitive information is stolen, used fraudulently, and/or the like). Additionally or alternatively, manually conveying such information requires time and resources and increases the likelihood of human errors.

[0006] In traditional techniques, virtual account payments allow the buyer to send a secure message to the supplier. However, the buyer manually enters the contact information for the supplier. If the contact information is entered incorrectly, the message fails to be delivered or is delivered to an incorrect/unknown entity. Additionally or alternatively, since the buyer enters the

information about the supplier, there is no sufficient verification of the identity/authenticity of the supplier. Additionally or alternatively, the supplier manually opens, reads, and/or the like each message from each buyer to manually initiate payment associated with each message. As such, the supplier devotes considerable resources (e.g., manual efforts and/or the like), experiences delays (e.g., considerable time is associated with handling each message, receiving payment based thereon, and/or the like). Additionally or alternatively, sensitive information (e.g., account identifiers and/or the like) of both the buyer and supplier is shared between the parties. Conveyance of such sensitive information elevates the risk to the parties (e.g., risk that sensitive information is stolen, used fraudulently, and/or the like). Additionally or alternatively, data for payment requests (e.g., invoices and/or the like), payment records, receipts, and/or the like is stored in different systems (e.g., buyer's system, supplier's system, and/or the like) in different formats, which makes reconciliation based thereon difficult. For example, reconciliation requires considerable resources (e.g., manual efforts, conversion of file formats, and/or the like), time, and/or the like and is subjected to human errors. Straight Through Processing (STP) is another method used for processing the payments. STP requires the supplier to manually onboard and/or set up an account (e.g., in addition to its respective payment accounts) with a payment gateway (e.g., which may be separate from the issuer(s), bank(s), and/or the like at which the supplier has its payment accounts). Such onboarding/setup requires considerable resources, time, and/or the like; is subjected to human errors; requires sharing of sensitive information (e.g., account identifiers and/or the like); and/or the like. Conveyance of such sensitive information elevates the risk to the parties. Additionally or alternatively, such payment gateways may charge additional fees (e.g., in addition to fees of the payment accounts, such as checking accounts, credit card accounts, and/or the like), may add additional overhead to the transaction, may cause delays (e.g., waiting for the transfer to clear the payment account of each respective party), and/or the like. Additionally or alternatively, data for the payment requests, payment records, receipts, and/or the like needs to be manually generated and/or stored in different systems (e.g., supplier's system, payment gateway, and/or the like) in different formats, all of which makes reconciliation based thereon difficult.

BRIEF DESCRIPTION OF THE DRAWINGS

[0007] Additional advantages and details of the disclosed subject matter are explained in greater detail below with reference to the exemplary embodiments that are illustrated in the accompanying figures, in which:

[0008] FIG. 1 is a diagram of a non-limiting embodiment of an environment in which methods and systems are implemented, in accordance with some embodiments of the present disclosure;

[0009] FIG. 2 is a diagram of a non-limiting embodiment of components of one or more devices, in accordance with some embodiments of the present disclosure;

[0010] FIG. 3 is a flowchart of a non-limiting embodiment of a process for using a virtual account, in accordance with some embodiments of the present disclosure;

[0011] FIG. 4 is a diagram of a non-limiting embodiment of an implementation of the process for using the virtual account, in accordance with some embodiments of the present disclosure; and

[0012] Figure 5 shows a block diagram of a general-purpose computing system for using the virtual account, in accordance with embodiments of the present disclosure.

DETAILED DESCRIPTION

[0013] For purposes of the description hereinafter, the terms “end,” “upper,” “lower,” “right,” “left,” “vertical,” “horizontal,” “top,” “bottom,” “lateral,” “longitudinal,” and derivatives thereof shall relate to the disclosed subject matter as it is oriented in the drawing figures. However, it is to be understood that the disclosed subject matter may assume various alternative variations and step sequences, except where expressly specified to the contrary. It is also to be understood that the specific devices and processes illustrated in the attached drawings, and described in the following specification, are simply exemplary embodiments or aspects of the disclosed subject matter. Hence, specific dimensions and other physical characteristics related to the embodiments or

aspects disclosed herein are not to be considered as limiting unless otherwise indicated. No aspect, component, element, structure, act, step, function, instruction, and/or the like used herein should be construed as critical or essential unless explicitly described as such. Also, as used herein, the articles "a" and "an" are intended to include one or more items and may be used interchangeably with "one or more" and "at least one." Furthermore, as used herein, the term "set" is intended to include one or more items (e.g., related items, unrelated items, a combination of related and unrelated items, and/or the like) and may be used interchangeably with "one or more" or "at least one." Where only one item is intended, the term "one" or similar language is used. Also, as used herein, the terms "has," "have," "having," or the like are intended to be open-ended terms. Further, the phrase "based on" is intended to mean "based at least partially on" unless explicitly stated otherwise.

[0014] As used herein, the terms "communication" and "communicate" may refer to the reception, receipt, transmission, transfer, provision, and/or the like of information (e.g., data, signals, messages, instructions, commands, and/or the like). For one unit (e.g., a device, a system, a component of a device or system, combinations thereof, and/or the like) to be in communication with another unit means that the one unit is able to directly or indirectly receive information from and/or transmit information to the other unit. This may refer to a direct or indirect connection (e.g., a direct communication connection, an indirect communication connection, and/or the like) that is wired and/or wireless in nature. Additionally, two units may be in communication with each other even though the information transmitted may be modified, processed, relayed, and/or routed between the first and second unit. For example, a first unit may be in communication with a second unit even though the first unit passively receives information and does not actively transmit information to the second unit. As another example, a first unit may be in communication with a second unit if at least one intermediary unit (e.g., a third unit located between the first unit and the second unit) processes information received from the first unit and communicates the processed information to the second unit. In some non-limiting embodiments, a message may refer to a network packet (e.g., a data packet and/or the like) that includes data. It will be appreciated that numerous other arrangements are possible.

[0015] As used herein, the terms "issuer institution," "portable financial device issuer," "issuer," or "issuer bank" may refer to one or more entities that provide accounts to customers for conducting transactions (e.g., payment transactions), such as initiating credit and/or debit payments. For example, an issuer institution may provide an account identifier, such as a personal account number (PAN), to a customer that uniquely identifies one or more accounts associated with that customer. The account identifier may be embodied on a portable financial device, such as a physical financial instrument, e.g., a payment card, and/or may be electronic and used for electronic payments. The terms "issuer institution" and "issuer institution system" may also refer to one or more computer systems operated by or on behalf of an issuer institution, such as a server computer executing one or more software applications. For example, an issuer institution system may include one or more authorization servers for authorizing a transaction.

[0016] As used herein, the term "account identifier" may include one or more types of identifiers associated with a user account (e.g., a PAN, a primary account number, a card number, a payment card number, a token, and/or the like). In some non-limiting embodiments, an issuer institution may provide an account identifier (e.g., a PAN, a token, and/or the like) to a user that uniquely identifies one or more accounts associated with that user. The account identifier may be embodied on a physical financial instrument (e.g., a portable financial instrument, a payment card, a credit card, a debit card, and/or the like) and/or may be electronic information communicated to the user that the user may use for electronic payments. In some non-limiting embodiments, the account identifier may be an original account identifier, where the original account identifier was provided to a user at the creation of the account associated with the account identifier. In some non-limiting embodiments, the account identifier may be an account identifier (e.g., a supplemental account identifier) that is provided to a user after the original account identifier was provided to the user. For example, if the original account identifier is forgotten, stolen, and/or the like, a supplemental account identifier may be provided to the user. In some non-limiting embodiments, an account identifier may be directly or indirectly associated with an issuer institution such that an account identifier may be a token that maps to a PAN or other type of identifier. Account identifiers may be alphanumeric, any combination of characters and/or symbols, and/or the like. An issuer institution may be associated with a bank identification number (BIN) that uniquely identifies the issuer institution.

[0017] As used herein, the terms "payment token" or "token" may refer to an identifier that is used as a substitute or replacement identifier for an account identifier, such as a PAN. Tokens may be associated with a PAN or other account identifiers in one or more data structures (e.g., one or more databases and/or the like) such that they can be used to conduct a transaction (e.g., a payment transaction) without directly using the account identifier, such as a PAN. In some examples, an account identifier, such as a PAN, may be associated with a plurality of tokens for different individuals, different uses, and/or different purposes. For example, a payment token may include a series of numeric and/or alphanumeric characters that may be used as a substitute for an original account identifier. For example, a payment token "4900 0000 0000 0001" may be used in place of a PAN "4147 0900 0000 1234." In some non-limiting embodiments, a payment 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 non-limiting embodiments, a payment token may be used in place of a PAN to initiate, authorize, settle, or resolve a payment transaction or represent the original credential in other systems where the original credential would typically be provided. In some non-limiting 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 (e.g., with a one-way hash or other cryptographic function). Further, in some non-limiting embodiments, the token format may be configured to allow the entity receiving the payment token to identify it as a payment token and recognize the entity that issued the token.

[0018] As used herein, the term "provisioning" may refer to a process of enabling a device to use a resource or service. For example, provisioning may involve enabling a device to perform transactions using an account. Additionally or alternatively, provisioning may include adding provisioning data associated with account data (e.g., a payment token representing an account number) to a device.

[0019] As used herein, the term "token requestor" may refer to an entity that is seeking to implement tokenization according to embodiments of the present disclosure subject. For example, the token requestor may initiate a request tokenized the PAN by submitting a token request

message to a token service provider. Additionally or alternatively, the token requestor may no longer need to store the PAN associated with the token once the token requestor has received the payment token in response to a token request message. In some non-limiting embodiments, the token requestor may be an application, a device, a process, or a system that is configured to perform actions associated with tokens. For example, the token requestor may request registration with a network token system, request token generation, token activation, token de-activation, token exchange, other token lifecycle management related processes, and/or any other token related processes. In some non-limiting embodiments, the token requestor may interface with a network token system through any suitable communication network and/or protocol (e.g., using HTTPS, SOAP and/or an XML interface among others). For example, the token requestor may include card-on-file merchants, acquirers, acquirer processors, payment gateways acting on behalf of merchants, payment enablers (e.g., original equipment manufacturers, mobile network operators, and/or the like), digital wallet providers, issuers, third-party wallet providers, payment processing networks, and/or the like. In some non-limiting embodiments, the token requestor may request tokens for multiple domains and/or channels. Additionally or alternatively, the token requestor may be registered and identified uniquely by the token service provider within the tokenization ecosystem. For example, during token requestor registration, the token service provider may formally process a token requestor's application to participate in the token service system. In some non-limiting embodiments, the token service provider may collect information pertaining to the nature of the requestor and relevant use of tokens to validate and formally approve the token requestor and establish appropriate domain restriction controls. Additionally or alternatively, successfully registered token requestors may be assigned a token requestor identifier that may also be entered and maintained within the token vault. In some non-limiting embodiments, token requestor identifiers may be revoked and/or token requestors may be assigned new token requestor identifiers. In some non-limiting embodiments, this information may be subject to reporting and audit by the token service provider.

[0020] As used herein, the term a "token service provider" may refer to an entity including one or more server computers in a token service system that generates, processes and maintains payment tokens. For example, the token service provider may include or be in communication with a token vault where the generated tokens are stored. Additionally or alternatively, the token

vault may maintain one-to-one mapping between the token and the PAN represented by the token. In some non-limiting embodiments, the token service provider may have the ability to set aside licensed BINs as token BINs to issue tokens for the PANs that may be submitted to the token service provider. In some non-limiting embodiments, various entities of the tokenization ecosystem may assume the roles of the token service provider. For example, payment networks and issuers or their agents may become the token service provider by implementing the token services according to non-limiting embodiments of the present disclosure. Additionally or alternatively, the token service provider may provide reports or data output to reporting tools regarding approved, pending, or declined token requests, including any assigned token requestor ID. The token service provider may provide data output related to token-based transactions to reporting tools and applications and present the token and/or PAN as appropriate in the reporting output. In some non-limiting embodiments, the EMVCo standards organization may publish specifications defining how tokenized systems may operate. For example, such specifications may be informative, but they are not intended to be limiting upon the present disclosure.

[0021] As used herein, the term "token vault" may refer to a repository that maintains established token-to-PAN mappings. For example, the token vault may also maintain other attributes of the token requestor that may be determined at the time of registration and/or that may be used by the token service provider to apply domain restrictions or other controls during transaction processing. In some non-limiting embodiments, the token vault may be a part of a token service system. For example, the token vault may be provided as a part of the token service provider. Additionally or alternatively, the token vault may be a remote repository accessible by the token service provider. In some non-limiting embodiments, the token vaults may be protected by strong underlying physical and logical security, due to the sensitive nature of the data mappings that are stored and managed therein. Additionally or alternatively, the token vault may be operated by any suitable entity, including a payment network, an issuer, clearing houses, other financial institutions, transaction service providers, and/or the like.

[0022] As used herein, the term "merchant" may refer to one or more entities (e.g., operators of retail businesses that provide goods and/or services, and/or access to goods and/or services, to a user (e.g., a customer, a consumer, a customer of the merchant, and/or the like) based on a

transaction (e.g., a payment transaction)). As used herein, "merchant system" may refer to one or more computer systems operated by or on behalf of the merchant, such as a server computer executing one or more software applications. As used herein, the term "product" may refer to one or more goods and/or services offered by the merchant.

[0023] As used herein, a "point-of-sale (POS) device" may refer to one or more devices, which may be used by the merchant to initiate transactions (e.g., a payment transaction), engage in transactions, and/or process transactions. For example, a POS device may include one or more computers, peripheral devices, card readers, near-field communication (NFC) receivers, radio frequency identification (RFID) receivers, and/or other contactless transceivers or receivers, contact-based receivers, payment terminals, computers, servers, input devices, and/or the like.

[0024] As used herein, a "point-of-sale (POS) system" may refer to one or more computers and/or peripheral devices used by the merchant to conduct the transaction. For example, the POS system may include one or more POS devices and/or other like devices that may be used to conduct a payment transaction. The POS system (e.g., a merchant POS system) may also include one or more server computers programmed or configured to process online payment transactions through webpages, mobile applications, and/or the like.

[0025] As used herein, the term "transaction service provider" may refer to an entity that receives transaction authorization requests from merchants or other entities and provides guarantees of payment, in some cases through an agreement between the transaction service provider and the issuer institution. In some non-limiting embodiments, the transaction service provider may include a credit card company, a debit card company, and/or the like. As used herein, the term "transaction service provider system" may also refer to one or more computer systems operated by or on behalf of a transaction service provider, such as a transaction processing server executing one or more software applications. The transaction processing server may include one or more processors and, in some non-limiting embodiments, may be operated by or on behalf of the transaction service provider.

[0026] As used herein, the term "acquirer" may refer to an entity licensed by the transaction service provider and approved by the transaction service provider to originate transactions (e.g., payment transactions) using a portable financial device associated with the transaction service provider. As used herein, the term "acquirer system" may also refer to one or more computer systems, computer devices, and/or the like operated by or on behalf of the acquirer. The transactions the acquirer may originate may include payment transactions (e.g., purchases, original credit transactions (OCTs), account funding transactions (AFTs), and/or the like). In some non-limiting embodiments, the acquirer may be authorized by the transaction service provider to assign merchant or service providers to originate transactions using a portable financial device of the transaction service provider. The acquirer may contract with payment facilitators to enable the payment facilitators to sponsor merchants. The acquirer may monitor compliance of the payment facilitators in accordance with regulations of the transaction service provider. The acquirer may conduct due diligence of the payment facilitators and ensure that proper due diligence occurs before signing a sponsored merchant. The acquirer may be liable for all transaction service provider programs that the acquirer operates or sponsors. The acquirer may be responsible for the acts of the acquirer's payment facilitators, merchants that are sponsored by an acquirer's payment facilitators, and/or the like. In some non-limiting embodiments, an acquirer may be a financial institution, such as a bank.

[0027] As used herein, the terms "electronic wallet," "electronic wallet mobile application," and "digital wallet" may refer to one or more electronic devices and/or one or more software applications configured to initiate and/or conduct transactions (e.g., payment transactions, electronic payment transactions, and/or the like). For example, the electronic wallet may include a user device (e.g., a mobile device) executing an application program and server-side software and/or databases for maintaining and providing transaction data to the user device. As used herein, the term "electronic wallet provider" may include an entity that provides and/or maintains the electronic wallet and/or an electronic wallet mobile application for a user (e.g., a customer). Examples of the electronic wallet provider include, but are not limited to, Google Wallet™, Android Pay®, Apple Pay®, and Samsung Pay®. In some non-limiting examples, a financial institution (e.g., an issuer institution) may be an electronic wallet provider. As used herein, the term "electronic wallet provider system" may refer to one or more computer systems, computer

devices, servers, groups of servers, and/or the like operated by or on behalf of the electronic wallet provider.

[0028] As used herein, the term "portable financial device" may refer to a payment card (e.g., a credit or debit card), a gift card, a smartcard, smart media, a payroll card, a healthcare card, a wrist band, a machine-readable medium containing account information, a keychain device or fob, an RFID transponder, a retailer discount or loyalty card, a cellular phone, an electronic wallet mobile application, a personal digital assistant (PDA), a pager, a security card, a computer, an access card, a wireless terminal, a transponder, and/or the like. In some non-limiting embodiments, the portable financial device may include volatile or non-volatile memory to store information (e.g., an account identifier, a name of the account holder, and/or the like).

[0029] As used herein, the term "payment gateway" may refer to an entity and/or a payment processing system operated by or on behalf of such an entity (e.g., a merchant service provider, a payment service provider, a payment facilitator, a payment facilitator that contracts with an acquirer, a payment aggregator, and/or the like), which provides payment services (e.g., transaction service provider payment services, payment processing services, and/or the like) to one or more merchants. The payment services may be associated with the use of portable financial devices managed by a transaction service provider. As used herein, the term "payment gateway system" may refer to one or more computer systems, computer devices, servers, groups of servers, and/or the like operated by or on behalf of a payment gateway and/or to a payment gateway itself. The term "payment gateway mobile application" may refer to one or more electronic devices and/or one or more software applications configured to provide payment services for transactions (e.g., payment transactions, electronic payment transactions, and/or the like).

[0030] As used herein, the terms "client" and "client device" may refer to one or more client-side devices or systems (e.g., remote from a transaction service provider) used to initiate or facilitate the transaction. As an example, the "client device" may refer to the one or more POS devices used by the merchant, one or more acquirer host computers used by the acquirer, one or more mobile devices used by the user, and/or the like. In some non-limiting embodiments, the client device may be an electronic device configured to communicate with one or more networks and initiate or facilitate transactions. For example, the client device may include one or more

computers, portable computers, laptop computers, tablet computers, mobile devices, cellular phones, wearable devices (e.g., watches, glasses, lenses, clothing, and/or the like), PDAs, and/or the like. Moreover, the "client" may also refer to an entity (e.g., the merchant, the acquirer, and/or the like) that owns, utilizes, and/or operates the client device for initiating transactions (e.g., for initiating transactions with the transaction service provider).

[0031] As used herein, the term "server" may refer to one or more computing devices (e.g., processors, storage devices, similar computer components, and/or the like) that communicate with client devices and/or other computing devices over a network (e.g., a public network, the Internet, a private network, and/or the like) and, in some examples, facilitate communication among other servers and/or the client devices. It will be appreciated that various other arrangements are possible. As used herein, the term "system" may refer to one or more computing devices or combinations of computing devices (e.g., processors, servers, client devices, software applications, components of such, and/or the like). Reference to "a device," "a server," "a processor," and/or the like, as used herein, may refer to a previously-recited device, server, or processor that is recited as performing a previous step or function, a different server or processor, and/or a combination of servers and/or processors. For example, as used in the specification and the claims, a first server or a first processor that is recited as performing a first step or a first function may refer to the same or different server or the same or different processor recited as performing a second step or a second function.

[0032] Non-limiting embodiments of the present disclosure are directed to systems, and methods for using a virtual account, including, but not limited to, using the virtual account with invoice data. The method comprises generating first (e.g., supplier and/or the like) and second (e.g., buyer and/or the like) tokens. Further, the method comprises generating the virtual account (e.g., lodged account and/or the like) based on the tokens for automatic handling of payment requests (e.g., invoices and/or the like) and/or automatic transfer of funds (e.g., debiting the virtual account, crediting the supplier's account, push payment, pull payment, payment transaction, and/or the like) between the first party (e.g., supplier and/or the like) and second party (e.g., buyer and/or the like). Such embodiments provide techniques and systems that reduce (e.g., eliminate, decrease, and/or the like) manual efforts (e.g., manual actions, security measures, account monitoring, and/or

the like) of the parties in handling invoices and/or transferring funds. Thus, such techniques and system conserves resources (e.g., manual efforts, security measures, account monitoring, and/or the like), reduce human errors, and improve efficiency. Additionally or alternatively, such embodiments provide techniques and systems that reduce wait time (e.g., time from when the invoice is generated and/or communicated to the buyer until funds become available in the supplier's account and/or the like). For example, funds may be transferred to and/or available in the supplier's account in real time (e.g., instantaneously, virtually immediately, at the same approximate time the invoice is processed and/or the funds are transferred, and/or the like). Additionally or alternatively, such embodiments provide techniques and systems that improve security. For example, because the tokens, virtual accounts, and/or the like eliminate the need to exchange sensitive information (e.g., account identifier, PAN, bank account number, payment card number, expiration date, security code, and/or the like) between the parties. Moreover, the virtual account (e.g., lodged account and/or the like) may be generated to exclusively transfer funds to the first party's (e.g., supplier's) account (e.g., based on the first (supplier) token) and/or prohibit any other transfers of funds from the virtual account, which may further improve security. Additionally or alternatively, such embodiments provide techniques and systems that automatically generate the tokens, virtual accounts, and/or the like. Thus, the parties needs not (manually) establish separate accounts (e.g., online accounts, which may charge separate fees). Additionally or alternatively, such embodiments provide techniques and systems that generate the tokens, virtual accounts, and/or the like based on existing accounts of the parties (e.g., buyer, supplier, and/or the like), thus providing assurance of the identity/authenticity of the party/account holder associated with such token, virtual account, and/or the like. Additionally or alternatively, such embodiments provide techniques and systems that store data for payment requests (e.g., invoices and/or the like), generate payment records, generate receipts, and/or the like in the same system in formats that may facilitate reconciliation based thereon. Additionally or alternatively, such embodiments provide techniques and systems that allow onboarding, set up, and/or generation of accounts, tokens, virtual accounts, and/or the like based on information (e.g., account identifier data and/or the like) received from an issuer system associated with a party/account holder, which may conserve resources (e.g., manual efforts and/or the like), reduce human errors, improve efficiency, provide assurance of the identity/authenticity of the party/account holder, uses/maintains the relationship between the party/account holder and the issuer, and reduces (e.g.,

eliminates) the need to create a new relationship with the party/account holder. Additionally or alternatively, such embodiments provide techniques and systems that allow the supplier to have an account with reduced (e.g., low) risk as the supplier's account may be primarily (e.g., exclusively) to receive funds.

[0033] For the purpose of illustration, in the following description, while the presently disclosed subject matter is described with respect to methods, systems, and computer program products for using a virtual account, e.g., with invoice data, one skilled in the art will recognize that the disclosed subject matter is not limited to the illustrative embodiments. For example, the methods, systems, and computer program products described herein may be used with a wide variety of settings, such as using a virtual account in any suitable setting, e.g., person-to-person transactions, cross-border transactions, business-to-business transactions, automatic bill payments, consumer-to-business transactions, business-to-consumer disbursements, and/or the like.

[0034] Figure 1 is a diagram of a non-limiting embodiment of an environment (100) in which systems and/or methods, as described herein, is implemented. The environment (100) comprises a transaction service provider system (102), an issuer system (104), a customer device (106), a merchant system (108), an acquirer system (110), and a network (112). The transaction service provider system (102) may include one or more devices capable of receiving information from and/or communicating information to other devices in the environment (100). For example, the transaction service provider system (102) may include a computing device, such as a server (e.g., a transaction processing server), a group of servers, and/or other like devices. In some non-limiting embodiments, the transaction service provider system (102) may be associated with the transaction service provider as described herein. In some non-limiting embodiments, the transaction service provider system (102) may be in communication with a data storage device, which may be local or remote to the transaction service provider system (102). In some non-limiting embodiments, the transaction service provider system (102) may be capable of receiving information from, storing information in, communicating information to, or searching information stored in the data storage device.

[0035] The issuer system (104) may include one or more devices capable of receiving information and/or communicating information to other devices in the environment (100). For example, the issuer system (104) may include a computing device, such as a server, a group of servers, and/or other like devices. In some non-limiting embodiments, the issuer system (104) may be associated with an issuer institution as described herein. For example, the issuer system (104) may be associated with an issuer institution that issued a credit account, debit account, credit card, debit card, and/or the like to a user associated with the customer device (106). The customer device (106) may include one or more devices capable of receiving information to other devices in the environment (100). Additionally or alternatively, each customer device (106) may include a device capable of receiving information from and/or communicating information to other customer devices (106) via the network (112), another network (e.g., an ad hoc network, a local network, a private network, a virtual private network, and/or the like), and/or any other suitable communication technique. For example, the customer device (106) may include the client device and/or the like. In some non-limiting embodiments, the customer device (106) may or may not be capable of receiving information (e.g., from the merchant system (108) or from another customer device 106) via a short-range wireless communication connection (e.g., an NFC communication connection, an RFID communication connection, a Bluetooth® communication connection, a Zigbee® communication connection, and/or the like), and/or communicating information (e.g., to merchant system 108) via a short-range wireless communication connection.

[0036] The merchant system (108) may include one or more devices capable of receiving information from and/or communicating information to other devices in the environment (100). The merchant system (108) may also include a device capable of receiving information from the customer device (106) via the network (112), a communication connection (e.g., an NFC communication connection, an RFID communication connection, a Bluetooth® communication connection, a Zigbee® communication connection, and/or the like) with the customer device (106), and/or the like, and/or communicating information to the customer device (106) via the network (112), the communication connection, and/or the like. In some non-limiting embodiments, the merchant system (108) may include a computing device, such as a server, a group of servers, the client device, a group of client devices, and/or other like devices. In some non-limiting embodiments, merchant system 108 may be associated with the merchant as

described herein. In some non-limiting embodiments, the merchant system (108) may include one or more client devices. For example, the merchant system (108) may include the client device that allows the merchant to communicate information to the transaction service provider system (102). In some non-limiting embodiments, the merchant system (108) may include one or more devices, such as computers, computer systems, and/or peripheral devices capable of being used by a merchant to conduct a transaction with a user. For example, the merchant system (108) may include the POS device and/or the POS system.

[0037] The acquirer system (110) may include one or more devices capable of receiving information from and/or communicating information to other devices in the environment (100). For example, the acquirer system (110) may include a computing device, a server, a group of servers, and/or the like. In some non-limiting embodiments, the acquirer system (110) may be associated with the acquirer as described herein.

[0038] The network (112) may include one or more wired and/or wireless networks. For example, the network (112) may include a cellular network (e.g., a long-term evolution (LTE) network, a third generation (3G) network, a fourth generation (4G) network, a code division multiple access (CDMA) network, and/or the like), a public land mobile network (PLMN), a local area network (LAN), a wide area network (WAN), a metropolitan area network (MAN), a telephone network (e.g., the public switched telephone network (PSTN)), a private network (e.g., a private network associated with a transaction service provider), an ad hoc network, an intranet, the Internet, a fiber optic-based network, a cloud computing network, and/or the like, and/or a combination of these or other types of networks.

[0039] The number and arrangement of systems, devices, and/or networks shown in Figure 1 are provided as an example. There may be additional systems, devices, and/or networks; fewer systems, devices, and/or networks; different systems, devices, and/or networks; and/or differently arranged systems, devices, and/or networks than those shown in Figure 1. Furthermore, two or more systems or devices shown in Figure 1 may be implemented within a single system or device, or a single system or device shown in Figure 1 may be implemented as multiple, distributed systems or devices. Additionally or alternatively, a set of systems (e.g., one or more systems) or a

set of devices (e.g., one or more devices) of the environment (100) may perform one or more functions described as being performed by another set of systems or another set of devices of the environment (100).

[0040] Figure 2 is a diagram of example components of a device (200). The device (200) may correspond to one or more devices of the transaction service provider system (102), one or more devices of the issuer system (104), the customer device (106), one or more devices of the merchant system (108), and/or one or more devices of the acquirer system (110). In some non-limiting embodiments, the transaction service provider system (102), the issuer system (104), the customer device (106), the merchant system (108), and/or the acquirer system (110) may include at least one device (200) and/or at least one component of the device (200). The device (200) may include a bus (202), a processor (204), a memory (206), a storage component (208), an input component (210), an output component (212), and a communication interface (214).

[0041] The bus (202) may include a component that permits communication among the components of the device (200). In some non-limiting embodiments, the processor (204) may be implemented in hardware, firmware, or a combination of hardware and software. For example, processor (204) may include a processor (e.g., a central processing unit (CPU), a graphics processing unit (GPU), an accelerated processing unit (APU), and/or the like), a microprocessor, a digital signal processor (DSP), and/or any processing component (e.g., a field-programmable gate array (FPGA), an application-specific integrated circuit (ASIC), and/or the like), and/or the like, which can be programmed to perform a function. The memory (206) may include random access memory (RAM), read only memory (ROM), and/or another type of dynamic or static storage device (e.g., flash memory, magnetic memory, optical memory, and/or the like) that stores information and/or instructions for use by the processor (204).

[0042] The storage component (208) may store information and/or software related to the operation and use of the device (200). For example, the storage component (208) may include a hard disk (e.g., a magnetic disk, an optical disk, a magneto-optic disk, a solid state disk, and/or the like), a compact disc (CD), a digital versatile disc (DVD), a floppy disk, a cartridge, a magnetic tape, and/or another type of computer-readable medium, along with a corresponding drive.

[0043] The input component (210) may include a component that permits the device (200) to receive information, such as via user input (e.g., a touch screen display, a keyboard, a keypad, a mouse, a button, a switch, a microphone, a camera, and/or the like). Additionally or alternatively, the input component (210) may include a sensor for sensing information (e.g., a global positioning system (GPS) component, an accelerometer, a gyroscope, an actuator, and/or the like). The output component (212) may include a component that provides output information from the device (200) (e.g., a display, a speaker, one or more light-emitting diodes (LEDs), and/or the like).

[0044] The communication interface (214) may include a transceiver-like component (e.g., a transceiver, a receiver and transmitter that are separate, and/or the like) that enables the device (200) to communicate with other devices, such as via a wired connection, a wireless connection, or a combination of wired and wireless connections. The communication interface (214) may permit the device (200) to receive information from another device and/or provide information to another device. For example, the communication interface (214) may include an Ethernet interface, an optical interface, a coaxial interface, an infrared interface, a radio frequency (RF) interface, a universal serial bus (USB) interface, a Wi-Fi® interface, a Bluetooth® interface, a Zigbee® interface, a cellular network interface, and/or the like.

[0045] The device (200) may perform one or more processes described herein. The device (200) may perform these processes based on the processor (204) executing software instructions stored by a computer-readable medium, such as the memory (206) and/or the storage component (208). A computer-readable medium (e.g., a non-transitory computer-readable medium) is defined herein as a non-transitory memory device. A non-transitory memory device includes memory space located inside of a single physical storage device or memory space spread across multiple physical storage devices.

[0046] Software instructions may be read into the memory (206) and/or the storage component (208) from another computer-readable medium or from another device via the communication interface (214). When executed, software instructions stored in the memory (206) and/or the storage component (208) may cause the processor (204) to perform one or more processes

described herein. Additionally or alternatively, hardwired circuitry may be used in place of or in combination with software instructions to perform one or more processes described herein. Thus, embodiments described herein are not limited to any specific combination of hardware circuitry and software.

[0047] The number and arrangement of components shown in Figure 2 are provided as an example. In some non-limiting embodiments, the device (200) may include additional components, fewer components, different components, or differently arranged components than those shown in Figure 2. Additionally or alternatively, a set of components (e.g., one or more components) of the device (200) may perform one or more functions described as being performed by another set of components of the device (200).

[0048] Figure 3 is a flowchart of a non-limiting embodiment of a process (300) for using the virtual account. In some non-limiting embodiments, one or more of the steps of process (300) may be performed (e.g., completely, partially, and/or the like) by the transaction service provider system (102) (e.g., one or more devices of the transaction service provider system 102). In some non-limiting embodiments, one or more of the steps of the process (300) may be performed (e.g., completely, partially, and/or the like) by another system, another device, another group of systems, or another group of devices, separate from or including the transaction service provider system (102), such as the issuer system (104) (e.g., one or more devices of the issuer system 104), the customer device (106), the merchant system (108) (e.g., one or more devices of the merchant system 108), the acquirer system (110) (e.g., one or more devices of the acquirer system 110) and/or the like. In some non-limiting embodiments, a first party (e.g., supplier) system may be implemented (e.g., completely, partially, and/or the like) as a first merchant system (108). In some non-limiting embodiments, a second party (e.g., buyer) system may be implemented (e.g., completely, partially, and/or the like) as a second merchant system (108). In some non-limiting embodiments, the second party system may be implemented (e.g., completely, partially, and/or the like) by another system, another device, another group of systems, or another group of devices, separate from or including the second merchant system (108), such as the customer device (106), and/or the like.

[0049] At step (302), the process (300) may include receiving a first account identifier. For example, the transaction service provider system (102) may receive a first account identifier data. In some non-limiting embodiments, the first account identifier data may be associated with a first account of the first party (e.g., supplier). In some non-limiting embodiments, the transaction service provider system (102) may receive the first account identifier data from a first party system (e.g., the first merchant system (108) of the supplier and/or the like). Additionally or alternatively, the transaction service provider system (102) may receive the first account identifier data from the issuer system (104), which may be associated with (e.g., the issuer of and/or the like) the first account of the first party (e.g., supplier).

[0050] At step (304), the process (300) may include generating a first token. For example, the transaction service provider system (102) may generate a first token based on the first account identifier (e.g., of the supplier). In some non-limiting embodiments, the transaction service provider system (102) may communicate the first token to the first party system.

[0051] At step (306), the process (300) may include receiving a second account identifier. For example, the transaction service provider system (102) may receive second account identifier data. In some non-limiting embodiments, the second account identifier data may be associated with a second account of a second party (e.g., buyer). In some non-limiting embodiments, the transaction service provider system (102) may receive the second account identifier data from a second party system (e.g., the second merchant system (108) of the buyer and/or the like). Additionally or alternatively, the transaction service provider system (102) may receive the second account identifier data from the issuer system (104), which may be associated with (e.g., an issuer of and/or the like) the second account of the second party.

[0052] At step (308), the process (300) may include generating a second token. For example, the transaction service provider system (102) may generate a second token based on the second account identifier (e.g., of the buyer). In some non-limiting embodiments, the transaction service provider system (102) communicate the second token to the second party system.

[0053] At step (310), the process (300) may include receiving a request for establishing the virtual account. For example, the transaction service provider system (102) may receive first request data associated with a request to establish the virtual account. The first request data may include the first token, the second token, and/or the like. In some non-limiting embodiments, the transaction service provider system (102) may receive the first request data from the second party system. Additionally or alternatively, the transaction service provider system (102) may receive the first request data from the first party system. In some non-limiting embodiments, the transaction service provider system (102) (or a device of the first party such as the first merchant system (108) of the supplier and/or the like) may communicate the first token to a device of the second party (e.g., a device of the second merchant system (108) of the buyer and/or the like) before the transaction service provider system (102) receives the first request data. For example, the transaction service provider system (102) (or the first merchant system (108) of the supplier and/or the like) may communicate supplier identification data to the device of the second party (e.g., of the second merchant system (108) of the buyer and/or the like). Additionally or alternatively, the supplier identification data may include a plurality of tokens, and each token may be associated with a respective supplier. For example, the plurality of tokens may include the first token associated with the first party (e.g., the supplier). In some non-limiting embodiments, the device of the second party may generate the first request data based on the first token, the second token, and/or the like.

[0054] In some non-limiting embodiments, the virtual account (e.g., lodged account and/or the like) may include a connection (e.g., logical connection and/or the like) between two tokens (e.g., the first token and the second token). Additionally or alternatively, given the virtual account and one of the tokens (e.g., either the first token or the second token), the other token (e.g., the second token or the first token, respectively) may be determined (e.g., inferred, looked up, and/or the like) based on the virtual account the given one of the tokens. For example, given the virtual account and the first token, the second token may be determined (e.g., inferred, looked up, and/or the like), and vice versa.

[0055] In some non-limiting embodiments, the request to establish the virtual account may be automatically received (e.g., automatically generated, implicitly derived, and/or the like) based on

at least one transaction between the first token and the second token. For example, after the second token associated with the second party is used to make the transaction with the first token associated with the first party (e.g., supplier), the request to establish the virtual account may be automatically received (e.g., automatically generated, implicitly derived, and/or the like) based thereon.

[0056] In some non-limiting embodiments, the first request data may include at least one criterion for withdrawing (e.g., debiting) funds from the virtual account (e.g., lodged account). For example, first request data may include at least one criterion associated with which party or parties (e.g., which token associated with each party and/or the like) may request and/or receive payment from the virtual account (e.g., lodged account). In some non-limiting embodiments, the at least one criterion may include the first token of the first party (e.g., supplier).

[0057] At step (312), the process 300 may include generating the virtual account. For example, the transaction service provider system (102) may generate the virtual account based on the first request data (e.g., based on the first token, the second token, and/or the like). In some non-limiting embodiments, the virtual account may be funded by the second account associated with the second party.

[0058] In some non-limiting embodiments, the virtual account may be a lodged account, special-purpose account, and/or the like. Additionally or alternatively, the virtual account may be generated (e.g., set, configured, and/or the like) exclusively for transferring funds to the first party's account (e.g., based on the first (supplier) token). Additionally or alternatively, the virtual account may be generated (e.g., set, configured, and/or the like) to prohibit any transfers of funds from the virtual account other than to the first party's account (e.g., based on the first (supplier) token). For example, the virtual account may be limit which party or parties may request and/or receive payment from the virtual account based on at least one criterion of the first request data. In some non-limiting embodiments, the at least one criterion may include the first token of the first party.

[0059] At step (314), the process (300) may include receiving a payment request. For example, the transaction service provider system (102) may receive payment request data associated with the transaction between the first party and the second party. In some non-limiting embodiments, the payment request data may include a transaction amount. In some non-limiting embodiments, the payment request data may include invoice data associated with a transaction between the first party and the second party. For example, the invoice data may include a transaction amount. In some non-limiting embodiments, the invoice data may include first party identification data (e.g., first token, name, first account identifier, and/or the like), second party identification data (e.g., second token, name, second account identifier, and/or the like). In some non-limiting embodiments, the invoice data may include an image (e.g., digital image file, such as Portable Document Format (PDF), Tag Image File Format (TIFF), Joint Photographic Experts Group (JPEG or JPG), and/or the like) of an invoice. For example, the image may be a reproduction (e.g., scanned, photographed, captured, and/or the like) of a paper invoice. In some non-limiting embodiments, the invoice data may include renderable (e.g., editable, computer-readable, and/or the like) text. Additionally or alternatively, the transaction service provider system (102) may determine (e.g., identify, recognize, detect, and/or the like) text, e.g., from the image of the invoice data (e.g., using optical character recognition (OCR) and/or the like).

[0060] In some non-limiting embodiments, the transaction service provider system (102) may receive payment request data from the first party system. For example, the first party system may communicate the payment request data (e.g., invoice data) to the transaction service provider system (102) (e.g., supplier-initiated payment, pull payment, and/or the like).

[0061] In some non-limiting embodiments, the transaction service provider system (102) may receive payment request data from the second party system. For example, the second party system may communicate the payment request data (e.g., invoice data) to the transaction service provider system (102) (e.g., buyer-initiated payment, push payment, and/or the like). In some non-limiting embodiments, the payment request data may be associated with the transaction between the first party and the second party (e.g., the buyer), and the payment request data may include the first token of the first party, and a transaction amount.

[0062] At step (316), the process (300) may include transferring funds. For example, the transaction service provider system (102) may debit the transaction amount from the virtual account and/or second account associated with the second party. Additionally or alternatively, the transaction service provider system (102) may credit the transaction amount to the first account associated with the first party.

[0063] In some non-limiting embodiments, in the scenario of a supplier-initiated payment, pull payment, and/or the like, the transaction service provider system (102) may debit the transaction amount from the virtual account associated with the second party and credit the transaction amount to the first account associated with the first party based on the first token. For example, the transaction service provider system (102) may invoke a pull payment application programming interface (API). In some non-limiting embodiments, the transaction service provider system (102) may input to (e.g., populate fields of, provide input into, communicate to, and/or the like) the pull payment API virtual account identifier data (e.g., third token and/or the like) of the virtual account, the first token, the transaction amount, and/or the like. In some non-limiting embodiments, the pull payment API may debit the transaction amount from the virtual account and credit the transaction amount to the first account based on the inputs of the pull payment API. Additionally or alternatively, the pull payment API may populate a funding account field of a push payment API with the virtual account identifier data, populate a receiving account field of the push payment API with the first token, and invoke the push payment API to debit the transaction amount from the virtual account based on the funding account field and credit the transaction amount to the first account based on the receiving account field.

[0064] In some non-limiting embodiments, in the scenario of a buyer-initiated payment, push payment, and/or the like, the transaction service provider system (102) may select the second token from a plurality of tokens associated with the second party based on at least one criterion selected by the second party. Additionally or alternatively, the transaction service provider system (102) debiting the transaction amount from the second account associated with the second party based on the second token and credit the transaction amount to the first account associated with the first party based on the first token. For example, the transaction service provider system (102) populate a funding account field of a push payment API with the second token, populate a receiving account

field of the push payment API with the first token, and invoke the push payment API to debit the transaction amount from the second account based on the funding account field and credit the transaction amount to the first account based on the receiving account field.

[0065] Figure 4 is a diagram of an exemplary implementation (400) of a non-limiting embodiment relating to the process (300) shown in Figure 3. As shown in Figure 4, the implementation (400) may include the transaction service provider system (402), the issuer system (404), a supplier system (408a), a buyer system (408b), and/or the like. In some non-limiting embodiments, the transaction service provider system (402) may be the same as, similar to, or part of the transaction service provider system (102) (e.g., one or more devices of the transaction service provider system 102). In some non-limiting embodiments, the issuer system (404) may be the same as, similar to, or part of the issuer system (104) (e.g., one or more devices of issuer system 104). In some non-limiting embodiments, the supplier system (408a) may be the same as, similar to, or part of the first merchant system (108) (e.g., one or more devices of the first merchant system 108). In some non-limiting embodiments, the buyer system (408b) may be the same as, similar to, or part of the second merchant system (108) (e.g., one or more devices of the second merchant system 108). Additionally or alternatively, the buyer system (408b) may be may be implemented (e.g., completely, partially, and/or the like) by another system, another device, another group of systems, or another group of devices, separate from or including the second merchant system (108), such as the customer device (106) and/or the like.

[0066] In some non-limiting embodiments, the transaction service provider system (402) may receive (e.g., via onboarding/token generation module 402m) first account identifier data associated with the first account of the supplier (e.g., from the supplier system (408a), from the issuer system (404), and/or the like), as described herein. Additionally or alternatively, the transaction service provider system (402) (e.g., the onboarding/token generation module (402m) of the transaction service provider system (402)) may generate a supplier token (402a) based on the first account identifier, as described herein.

[0067] In some non-limiting embodiments, the transaction service provider system (402) may receive (e.g., via the onboarding/token generation module (402m)) second account identifier data

associated with the second account of the buyer (e.g., from buyer system (408b), from the issuer system (404), and/or the like), as described herein. Additionally or alternatively, the transaction service provider system (402) (e.g., the onboarding/token generation module (402m) of the transaction service provider system (402)) may generate a buyer token (402b) based on the first account identifier, as described herein.

[0068] In some non-limiting embodiments, the transaction service provider system (402) may receive (e.g., via lodged account creation module (402c)) the first request data associated with the request to establish the virtual account (e.g., from the buyer system (408b), and/or the like), as described herein. For example, the first request data may include the supplier token (402a), the buyer token (402b), and/or the like, as described herein. Additionally or alternatively, the transaction service provider system (402) may generate the virtual account based on the supplier token (402a), the buyer token (402b), and/or the like, as described herein. In some non-limiting embodiments, the virtual account may be funded by the second account associated with the second party/buyer token (402b), as described herein.

[0069] In some non-limiting embodiments, the transaction service provider system (402) may receive (e.g., via a pull payment API (402e)) the payment request data (402d) from the supplier system (408a), as described herein. In some non-limiting embodiments, the payment request data (402d) may include invoice data associated with the transaction between the first party and the second party, as described herein. Additionally or alternatively, the payment request data (402d) (e.g., the invoice data) may include the transaction amount, as described herein.

[0070] In some non-limiting embodiments, the transaction service provider system (402) may transfer the transaction amount from the virtual account to the first account associated with the first party, as described herein. For example, the transaction service provider system (402) may debit the transaction amount (e.g., of the payment request data (402d)) from the virtual account, as described herein. Additionally or alternatively, the transaction service provider system (402) may credit the transaction amount to the first account associated with the first party based on the first token, as described herein. In some non-limiting embodiments, the transaction service provider system (402) (e.g., pull payment API 402e) may populate a funding account field of a

push payment API (402f) with virtual account identifier data associated with the virtual account, as described herein. Additionally or alternatively, the transaction service provider system (402) (e.g., the pull payment API (402e)) may populate a receiving account field of the push payment API (402f) with the first token, as described herein. Additionally or alternatively, the transaction service provider system (402) (e.g., the pull payment API (402e)) may invoke the push payment API (402f) to debit the transaction amount from the virtual account based on the funding account field and credit the transaction amount to the first account based on the receiving account field, as described herein.

[0071] In some non-limiting embodiments, the transaction service provider system (402) (e.g., the onboarding/token generation module (402m)) may communicate the first token to the buyer system (408b) of the second party before receiving the first request data, as described herein. For example, the transaction service provider system (402) (e.g., the onboarding/token generation module 402m) may communicate the supplier identification data to the buyer system (408b) of the second party, as described herein. In some non-limiting embodiments, the supplier identification data may include a plurality of tokens, each token associated with a respective supplier, the plurality of tokens comprising the first token associated with the first party, as described herein.

[0072] In some non-limiting embodiments, the transaction service provider system (402) (e.g., payment instruction module (402h)) may receive the payment request data (402g) from the buyer system (408b) associated with the second party, as described herein. In some non-limiting embodiments, the payment request data (402d) may include invoice data associated with a transaction (e.g., second transaction) between the first party and the second party, as described herein. Additionally or alternatively, the payment request data may include the first token (402a) and the transaction amount (e.g., second transaction amount), as described herein.

[0073] In some non-limiting embodiments, the transaction service provider system (402) (e.g., token selection module (402i)) may select the second token from a plurality of tokens associated with the second party, as described herein. For example, the second party may select (and/or the transaction service provider system (402) may receive from the buyer system (408b)) at least one criterion associated with selecting the second token from the plurality of tokens (e.g., based on the

payment request data (402g), identification of the first party, and/or the like), as described herein. Additionally or alternatively, the transaction service provider system (402) (e.g., the token selection module (402i)) may select the second token from the plurality of tokens based on the at least one criterion selected by the second party before debiting the second transaction amount from the second account.

[0074] In some non-limiting embodiments, the transaction service provider system (402) may transfer the transaction amount from the second account associated with the second party based on the second token to the first account associated with the first party, as described herein. For example, the transaction service provider system (402) may debit the transaction amount (e.g., of the payment request data (402g)) from the second account associated with the second party based on the second token, as described herein. Additionally or alternatively, the transaction service provider system (402) may credit the transaction amount to the first account associated with the first party based on the first token, as described herein. In some non-limiting embodiments, the transaction service provider system (402) may populate a funding account field of a push payment API (402j) with the second token, as described herein. Additionally or alternatively, the transaction service provider system (402) (e.g., the pull payment API (402e)) may populate the receiving account field of the push payment API (402f) with the first token, as described herein. Additionally or alternatively, the transaction service provider system (402) may invoke the push payment API (402j) to debit the transaction amount from the second account based on the funding account field and credit the transaction amount to the first account based on the receiving account field, as described herein. In some non-limiting embodiments, the push payment API (402j) may be the same as or similar to the push payment API (402f).

[0075] In some non-limiting embodiments, the transaction service provider system (402) (e.g., the push payment API (402f), the push payment API (402j), and/or the like) may generate receipt data (402k) associated with a receipt for each transaction. In some non-limiting embodiments, the transaction service provider system (402) (e.g., reconciliation module (402l) and/or the like) may receive the payment request data (402d), the payment request data (402g), transaction record(s) from the push payment API (402f), transaction record(s) from the push payment API (402j), at least one of the receipt data (402k), a combination thereof, and/or the like. Additionally or

alternatively, the transaction service provider system (402) (e.g., the reconciliation module (402l) and/or the like) may reconcile all such data/records. Additionally or alternatively, the transaction service provider system (402) (e.g., the reconciliation module (402l) and/or the like) may generate reconciliation reports based on reconciling, may communicate reconciliation reports (e.g., to the supplier system (408a), the buyer system (408b), the issuer system (404), and/or the like), and/or the like.

[0076] Figure 5 illustrates a block diagram of an exemplary computer system (500) for implementing embodiments consistent with the present disclosure. In an embodiment, the computer system (500) is used for using the virtual account. The computer system (500) may comprise a central processing unit ("CPU" or "processor") (502). The processor (502) may comprise at least one data processor. The processor (502) may include specialized processing units such as integrated system (bus) controllers, memory management control units, floating point units, graphics processing units, digital signal processing units, etc.

[0077] The processor (502) may be disposed in communication with one or more input/output (I/O) devices (not shown) via I/O interface (501). The I/O interface (501) may employ communication protocols/methods such as, without limitation, audio, analog, digital, monoaural, RCA, stereo, IEEE-1394, serial bus, universal serial bus (USB), infrared, PS/2, BNC, coaxial, component, composite, digital visual interface (DVI), high-definition multimedia interface (HDMI), RF antennas, S-Video, VGA, IEEE 802.n /b/g/n/x, Bluetooth, cellular (e.g., code-division multiple access (CDMA), high-speed packet access (HSPA+), global system for mobile communications (GSM), long-term evolution (LTE), WiMax, or the like), etc.

[0078] Using the I/O interface (501), the computer system (500) may communicate with one or more I/O devices. For example, the input device (510) may be an antenna, keyboard, mouse, joystick, (infrared) remote control, camera, card reader, fax machine, dongle, biometric reader, microphone, touch screen, touchpad, trackball, stylus, scanner, storage device, transceiver, video device/source, etc. The output device (511) may be a printer, fax machine, video display (e.g., cathode ray tube (CRT), liquid crystal display (LCD), light-emitting diode (LED), plasma, Plasma display panel (PDP), Organic light-emitting diode display (OLED) or the like), audio speaker, etc.

[0079] In some embodiments, the computer system (500) is connected to the remote devices (512) through a communication network (509). The remote devices (512) may provide the user reviews to the computer system (500). The processor (502) may be disposed in communication with the communication network (509) via a network interface (503). The network interface (503) may communicate with the communication network (509). The network interface (503) may employ connection protocols including, without limitation, direct connect, Ethernet (e.g., twisted pair 10/100/1000 Base T), transmission control protocol/internet protocol (TCP/IP), token ring, IEEE 802.11a/b/g/n/x, etc. The communication network (509) may include, without limitation, a direct interconnection, local area network (LAN), wide area network (WAN), wireless network (e.g., using Wireless Application Protocol), the Internet, etc. Using the network interface (503) and the communication network (509), the computer system (500) may communicate with the scene remote devices (512). The network interface (503) may employ connection protocols include, but not limited to, direct connect, Ethernet (e.g., twisted pair 10/100/1000 Base T), transmission control protocol/internet protocol (TCP/IP), token ring, IEEE 802.11a/b/g/n/x, etc.

[0080] The communication network (509) includes, but is not limited to, a direct interconnection, an e-commerce network, a peer to peer (P2P) network, local area network (LAN), wide area network (WAN), wireless network (e.g., using Wireless Application Protocol), the Internet, Wi-Fi and such. The first network and the second network may either be a dedicated network or a shared network, which represents an association of the different types of networks that use a variety of protocols, for example, Hypertext Transfer Protocol (HTTP), Transmission Control Protocol/Internet Protocol (TCP/IP), Wireless Application Protocol (WAP), etc., to communicate with each other. Further, the first network and the second network may include a variety of network devices, including routers, bridges, servers, computing devices, storage devices, etc.

[0081] In some embodiments, the processor (502) may be disposed in communication with a memory (505) (e.g., RAM, ROM, etc. not shown in Figure 5) via a storage interface (504). The storage interface (504) may connect to memory (505) including, without limitation, memory drives, removable disc drives, etc., employing connection protocols such as serial advanced technology attachment (SATA), Integrated Drive Electronics (IDE), IEEE-1394, Universal Serial Bus (USB), fiber channel, Small Computer Systems Interface (SCSI), etc. The memory drives

may further include a drum, magnetic disc drive, magneto-optical drive, optical drive, Redundant Array of Independent Discs (RAID), solid-state memory devices, solid-state drives, etc.

[0082] The memory (505) may store a collection of program or database components, including, without limitation, user interface (506), an operating system (507), web browser (508) etc. In some embodiments, computer system (500) may store user/application data, such as, the data, variables, records, etc., as described in this disclosure. Such databases may be implemented as fault-tolerant, relational, scalable, secure databases such as Oracle ® or Sybase®.

[0083] The operating system (507) may facilitate resource management and operation of the computer system (500). Examples of operating systems include, without limitation, APPLE MACINTOSH^{R} OS X, UNIX^{R}, UNIX-like system distributions (E.G., BERKELEY SOFTWARE DISTRIBUTION^{TM} (BSD), FREEBSD^{TM}, NETBSD^{TM}, OPENBSD^{TM}, etc.), LINUX DISTRIBUTIONS^{TM} (E.G., RED HAT^{TM}, UBUNTU^{TM}, KUBUNTU^{TM}, etc.), IBM^{TM} OS/2, MICROSOFT^{TM} WINDOWS^{TM} (XP^{TM}, VISTA^{TM}/7/8, 10 etc.), APPLE^{R} IOS^{TM}, GOOGLE^{R} ANDROID^{TM}, BLACKBERRY^{R} OS, or the like.

[0084] In some embodiments, the computer system (500) may implement the web browser (508) stored program component. The web browser (508) may be a hypertext viewing application, for example MICROSOFT^{R} INTERNET EXPLORER^{TM}, GOOGLE^{R} CHROME^{TM0}, MOZILLA^{R} FIREFOX^{TM}, APPLE^{R} SAFARI^{TM}, etc. Secure web browsing may be provided using Secure Hypertext Transport Protocol (HTTPS), Secure Sockets Layer (SSL), Transport Layer Security (TLS), etc. Web browsers (508) may utilize facilities such as AJAX^{TM}, DHTML^{TM}, ADOBE^{R} FLASH^{TM}, JAVASCRIPT^{TM}, JAVA^{TM}, Application Programming Interfaces (APIs), etc. In some embodiments, the computer system (500) may implement a mail server (not shown in Figure) stored program component. The mail server may be an Internet mail server such as Microsoft Exchange, or the like. The mail server may utilize facilities such as ASP^{TM}, ACTIVEX^{TM}, ANSI^{TM} C++/C#, MICROSOFT^{R}, .NET^{TM}, CGI SCRIPTS^{TM}, JAVA^{TM}, JAVASCRIPT^{TM}, PERL^{TM}, PHP^{TM}, PYTHON^{TM}, WEBOBJECTS^{TM}, etc. The mail server may utilize communication protocols such as Internet Message Access Protocol (IMAP), Messaging Application Programming Interface (MAPI), MICROSOFT^{R} exchange, Post Office Protocol (POP), Simple Mail Transfer Protocol (SMTP), or the like. In some embodiments, the computer system (500)

may implement a mail client stored program component. The mail client (not shown in Figure) may be a mail viewing application, such as APPLE® MAIL™, MICROSOFT® ENTOURAGE™, MICROSOFT® OUTLOOK™, MOZILLA® THUNDERBIRD™, etc.

[0085] Furthermore, one or more computer-readable storage media may be utilized in implementing embodiments consistent with the present disclosure. A computer-readable storage medium refers to any type of physical memory on which information or data readable by a processor may be stored. Thus, a computer-readable storage medium may store instructions for execution by one or more processors, including instructions for causing the processor(s) to perform steps or stages consistent with the embodiments described herein. The term "computer-readable medium" should be understood to include tangible items and exclude carrier waves and transient signals, i.e., be non-transitory. Examples include Random Access Memory (RAM), Read-Only Memory (ROM), volatile memory, non-volatile memory, hard drives, CD ROMs, DVDs, flash drives, disks, and any other known physical storage media.

[0086] Finally, the language used in the specification has been principally selected for readability and instructional purposes, and it may not have been selected to delineate or circumscribe the inventive subject matter. Accordingly, the disclosure of the embodiments of the disclosure is intended to be illustrative, but not limiting, of the scope of the disclosure.

[0087] With respect to the use of substantially any plural and/or singular terms herein, those having skill in the art can translate from the plural to the singular and/or from the singular to the plural as is appropriate to the context and/or application. The various singular/plural permutations may be expressly set forth herein for sake of clarity.

METHOD AND SYSTEM FOR USING A VIRTUAL ACCOUNT

ABSTRACT

The present disclosure provides a method and a system for using a virtual account. The method comprises receiving first account identifier data associated with a first account of a first party. A first token may be generated based on the first account identifier. Second account identifier data associated with a second account of a second party may be received. A second token may be generated based on the second account identifier. First request data associated with a request to establish a virtual account may be received. A virtual account may be generated and may be funded by the second account associated with the second party. Invoice data associated with a transaction between the first party and the second party may be received. A transaction amount (e.g., from the invoice) may be debited from the virtual account and/or credited to the first account.

1/5

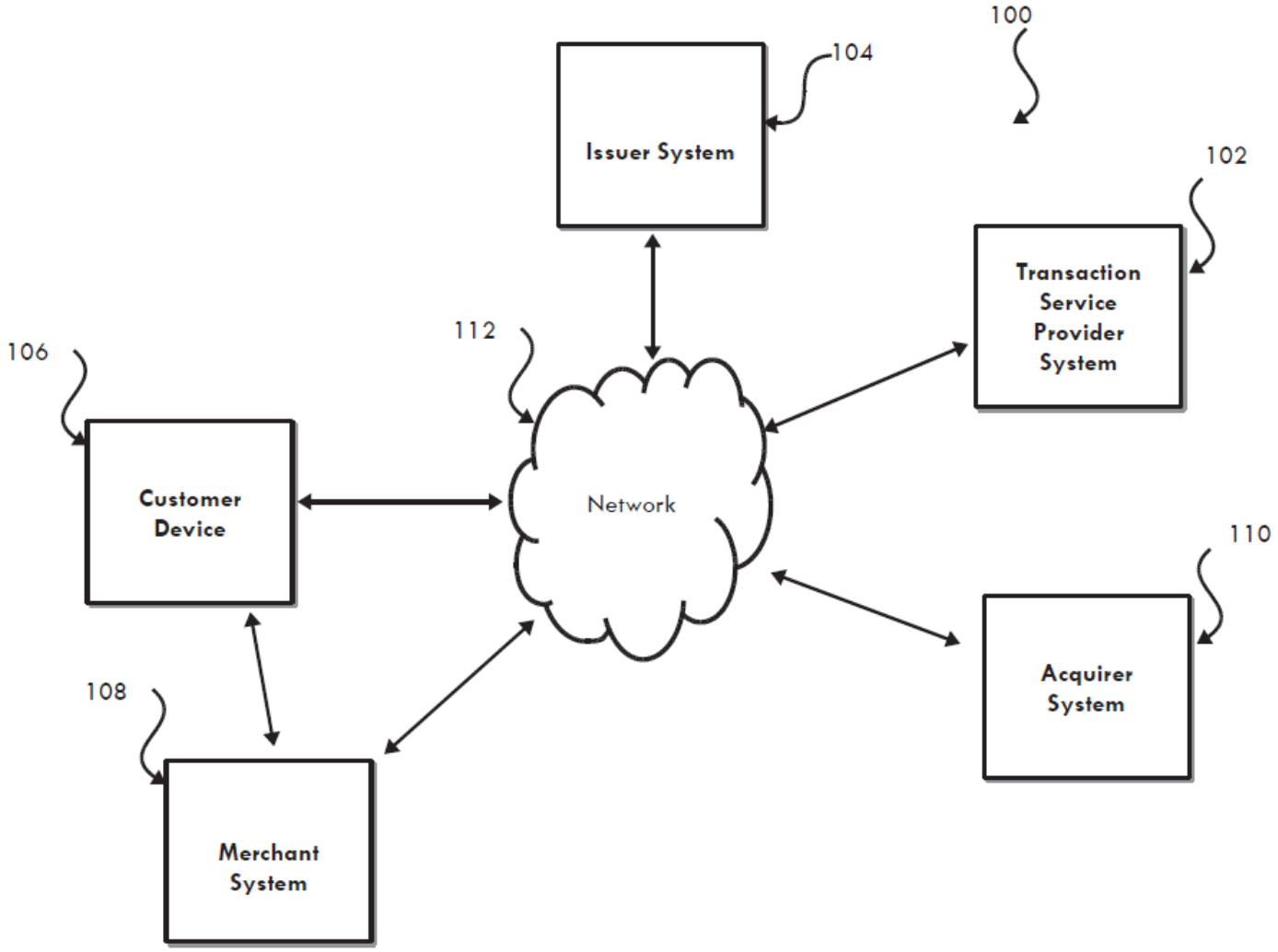
100
104
Issuer System
102
Transaction Service Provider System
112
106
Customer Device
Network
110
Acquirer System
108
Merchant System

FIGURE 1

2/5

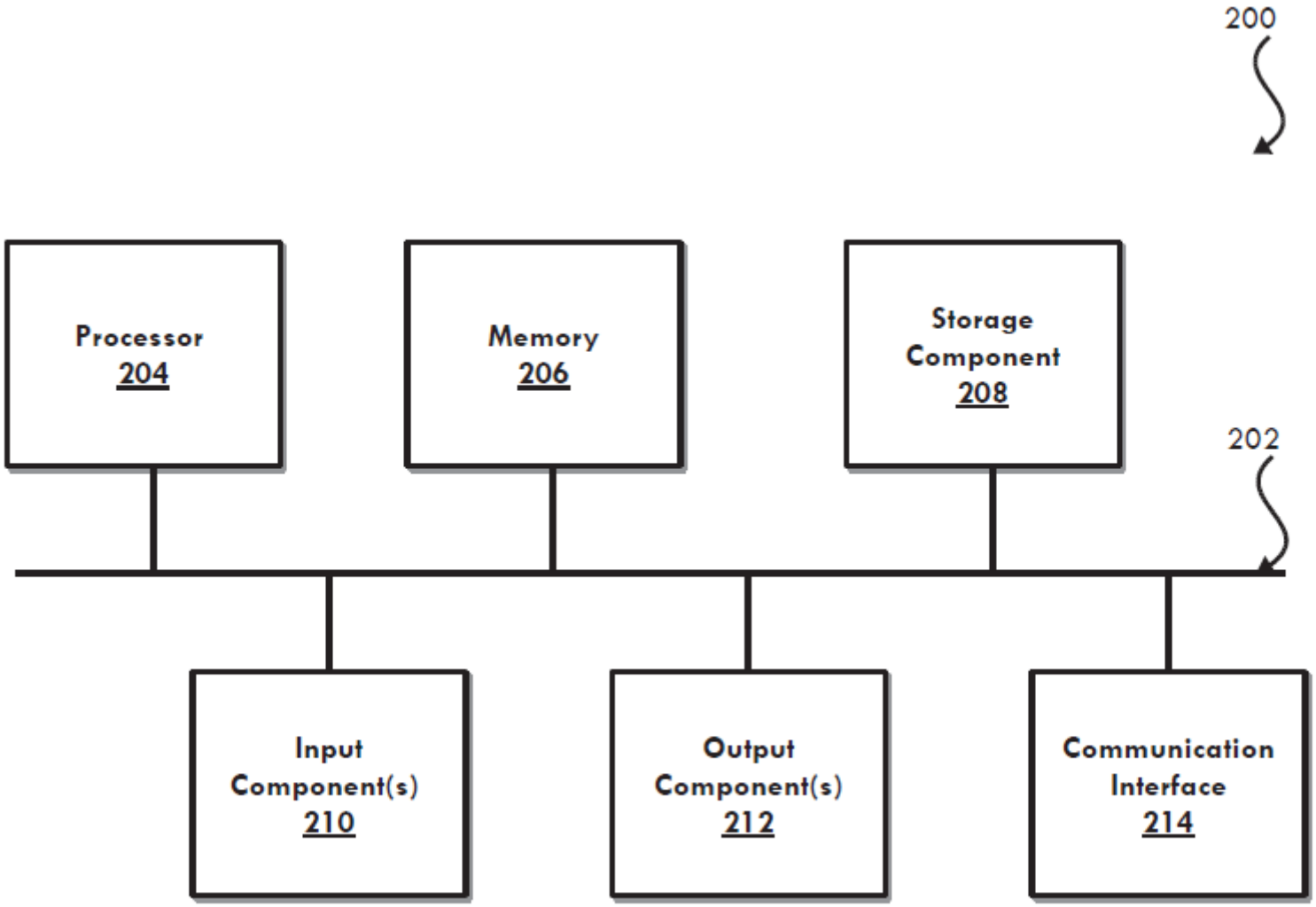
200
Processor
204
Memory
206
Storage
Component
208
202
Input
Component(s)
210
Output
Component(s)
212
Communication
Interface
214

FIGURE 2

3/5

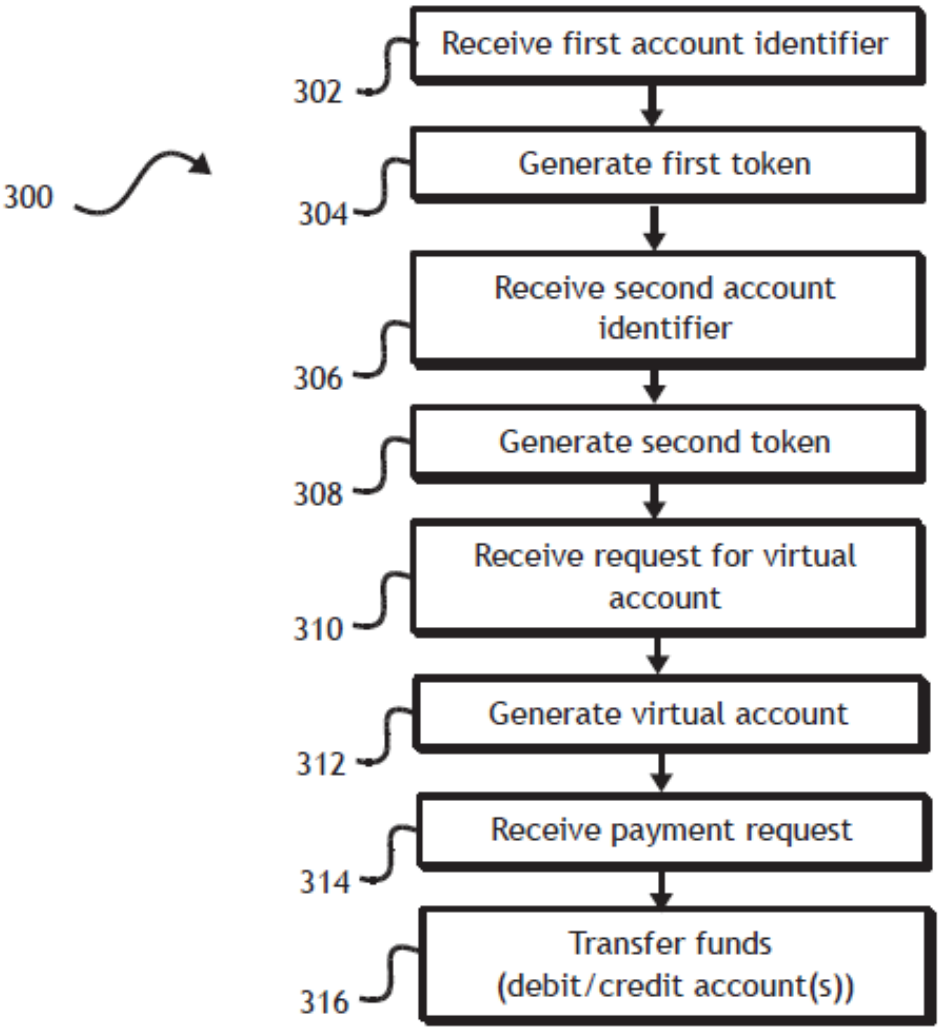
300
302
Receive first account identifier
304
Generate first token
306
Receive second account identifier
308
Generate second token
310
Receive request for virtual account
312
Generate virtual account
314
Receive payment request
316
Transfer funds (debit/credit account(s))

FIGURE 3

`

4/5

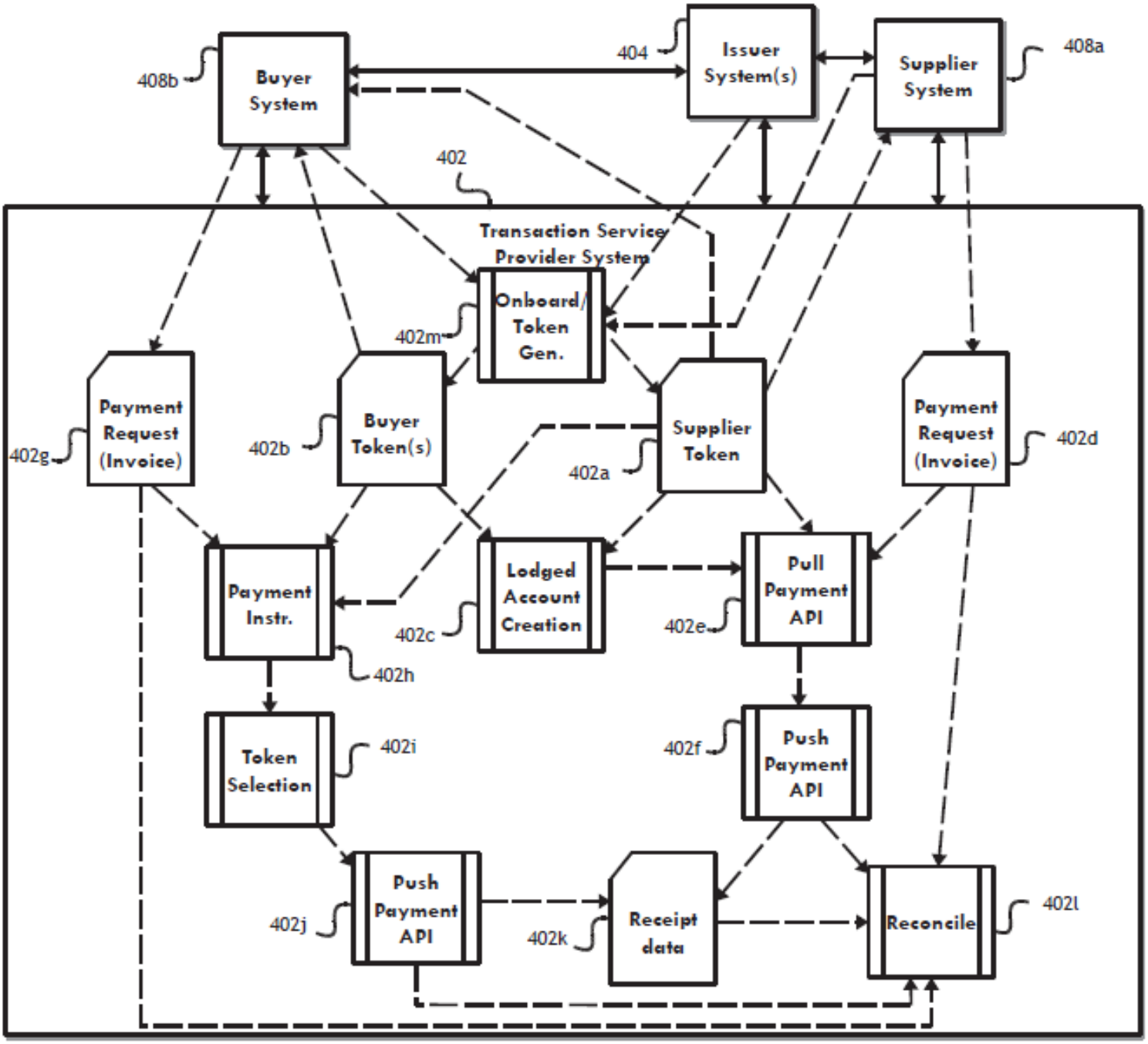
Buyer System
408b
Issuer System(s)
404
Supplier System
408a
402
Transaction Service Provider System
Onboard/ Token Gen.
402m
Payment Request (Invoice)
402g
Buyer Token(s)
402b
Supplier Token
402a
Payment Request (Invoice)
402d
Payment Instr.
Lodged Account Creation
402c
Pull Payment API
402e
402h
Token Selection
402i
402f
Push Payment API
Push Payment API
402j
Receipt data
402k
Reconcile
402l

FIGURE 4

5/5

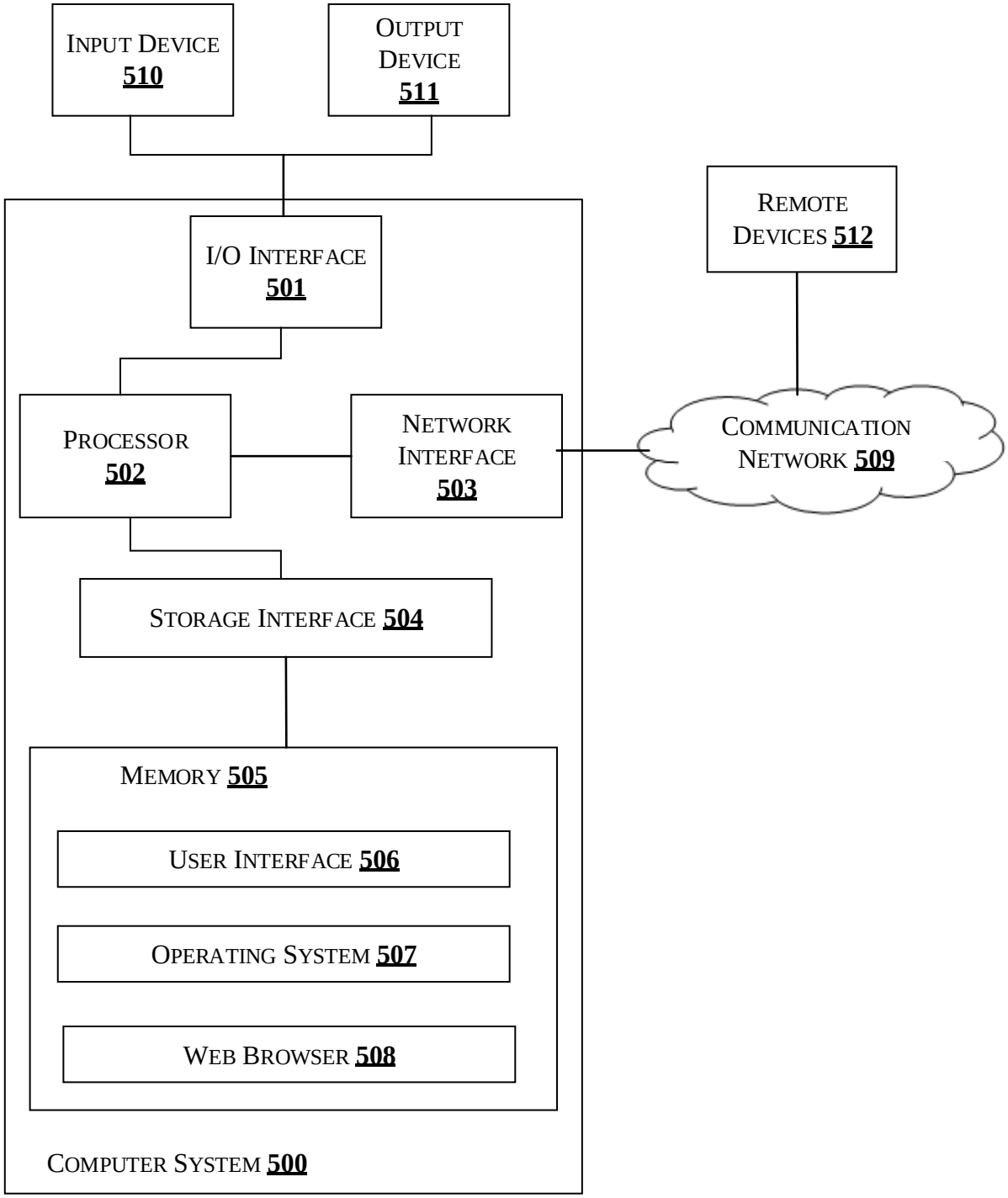
INPUT DEVICE 510
OUTPUT DEVICE 511
REMOTE DEVICES 512
I/O INTERFACE 501
PROCESSOR 502
NETWORK INTERFACE 503
COMMUNICATION NETWORK 509
STORAGE INTERFACE 504
MEMORY 505
USER INTERFACE 506
OPERATING SYSTEM 507
WEB BROWSER 508
COMPUTER SYSTEM 500

FIGURE 5