July 2023

SPLITTING AND AUTHORISING CARD PAYMENTS ACROSS MULTIPLE USERS ONLINE VIA A SINGLE PAYMENT TOKEN

SAMUEL OLIVER
VISA

“SPLITTING AND AUTHORISING CARD PAYMENTS ACROSS MULTIPLE USERS VIA A SINGLE PAYMENT TOKEN”

VISA

INVENTOR:

SAMUEL OLIVER

TECHNICAL FIELD

[0001] The present subject matter is, in general, related to payment transactions, and more particularly, but not exclusively to a method and system for splitting payments across multiple users utilizing a token.

BACKGROUND

[0002] Payment cards such as a credit or debit card are currently used around the world to pay for goods and services. Card payments involve a relatively standard process to process transactions initiated by a cardholder at a merchant. Card payments are an efficient and effective tool when a cardholder wishes to pay for the entirety of the good and or service themselves. However, when a cardholder wishes to buy a good or service for which multiple individuals will contribute to the end payment of the good and or service, there is increased friction in the process, particularly in case of recurring bill payment transactions.

[0003] Figure A shows one method whereby a merchant can enable multiple cardholders to contribute towards the cost of a single purchase by opening multiple merchant acceptance portals for individual cardholders to make payments towards a total amount. In this method, several authorization requests are made to the payments network (Visa)and the merchant must aggregate all authorization responses including any declined payments before the total purchase is complete. This method is complex, as it requires the merchant to undertake additional development outside the standard card payment flow to enable such functionality and therefore it is uncommon and only available at specific merchants. There is an opportunity to make this process more efficient for cardholders and to enable split functionality at any merchant regardless of whether the merchant has enabled the functionality through additional development work.

[0004] In a non-limiting embodiment, the multiple cardholders, which the splitting rules point to, could instead be made up of a single cardholder and multiple payment accounts/ types of payment methods/ funding sources.

BRIEF DESCRIPTION OF THE DRAWINGS

[0005] The accompanying drawings, which are incorporated in and constitute a part of this disclosure, illustrate exemplary embodiments and, together with the description, explain the disclosed principles. In the figures, the left-most digit(s) of a reference number identifies the

figure in which the reference number first appears. The same numbers are used throughout the figures to reference like features and components. Some embodiments of device or system and/or methods in accordance with embodiments of the present subject matter are now described, by way of example only, and with reference to the accompanying figures, in which:

[0006] **FIG. A** illustrates an exemplary flow of a traditional method for authorizing payment transactions for multiple cardholders.

[0007] **FIG. 1** and **FIG. 2** illustrate an exemplary flow of a method for generating a split payment token which can be used for both online and offline transactions, in accordance with some embodiments of the present disclosure.

[0008] **FIG. 3** illustrates an exemplary flow of a method for performing automated multi-transactions in a single process using a split payment token, in accordance with some embodiments of the present disclosure.

[0009] **FIG. 4a** and **FIG. 4b** illustrate an exemplary flow of a method for distributing split authorization among multiple contacts, in accordance with some embodiments of the present disclosure.

[0010] **FIG. 5** illustrates an exemplary flow diagram of a method for splitting payments online using a token, in accordance with some embodiments of the present disclosure. This demonstrates a more efficient splitting process than that described in Figure A.

[0011] **FIG. 6** is a block diagram of an exemplary computer system for implementing embodiments consistent with the present disclosure.

[0012] The figures depict embodiments of the disclosure for purposes of illustration only. One skilled in the art will readily recognize from the following description that alternative embodiments of the structures and methods illustrated herein may be employed without departing from the principles of the disclosure described herein.

DESCRIPTION OF THE DISCLOSURE

[0013] It is to be understood that the present disclosure 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 and non-limiting embodiments or aspects. Hence, specific dimensions and other physical characteristics related to the embodiments or aspects disclosed herein are not to be considered as limiting.

[0014] In the present document, the word "exemplary" is used herein to mean "serving as an example, instance, or illustration." Any embodiment or implementation of the present subject matter described herein as "exemplary" is not necessarily to be construed as preferred or advantageous over other embodiments.

[0015] While the disclosure is susceptible to various modifications and alternative forms, specific embodiment thereof has been shown by way of example in the drawings and will be described in detail below. It should be understood, however that it is not intended to limit the disclosure to the particular forms disclosed, but on the contrary, the disclosure is to cover all modifications, equivalents, and alternative falling within the spirit and the scope of the disclosure.

[0016] The terms “comprises”, “comprising”, or any other variations thereof, are intended to cover a non-exclusive inclusion, such that a setup, device, or method that comprises a list of components or steps does not include only those components or steps but may include other components or steps not expressly listed or inherent to such setup or device or method. In other words, one or more elements in a device or system or apparatus proceeded by “comprises… a” does not, without more constraints, preclude the existence of other elements or additional elements in the device or system or apparatus.

[0017] The terms "an embodiment", "embodiment", "embodiments", "the embodiment", "the embodiments", "one or more embodiments", "some embodiments", and "one embodiment" mean "one or more (but not all) embodiments of the invention(s)" unless expressly specified otherwise.

[0018] The terms "including", "comprising", “having” and variations thereof mean "including but not limited to" unless expressly specified otherwise.

[0019] 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 can receive information directly or indirectly 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.

[0020] As used herein, the term “computing device” may refer to one or more electronic devices that are configured to communicate with directly or indirectly or over one or more networks. A computing device may be a mobile or portable computing device, a desktop computer, a server, and/or the like. Furthermore, the term “computer” may refer to any computing device that includes the necessary components to receive, process, and output data, and normally includes a display, a processor, a memory, an input device, and a network interface. A “computing system” may include one or more computing devices or computers.

[0021] As used herein, the term “application” or “Application Program Interface” (API) may refer to computer code or other data sorted on a computer-readable medium that may be executed by a processor to facilitate the interaction between software components, such as a client-side front-end and/or server-side back-end for receiving data from the client. An “interface” refers to a generated display, such as one or more graphical user interfaces (GUIs) with which a user may interact, either directly or indirectly (e.g., through a keyboard, mouse, touchscreen, etc.). Further, multiple computers, e.g., servers, or other computerized devices, such as an autonomous vehicle including a vehicle computing system, directly or indirectly communicating in the network environment may constitute a “system” or a “computing system”.

[0022] As used herein, the term "device or mobile device" may refer to any electronic device that may be transported and 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 mobile devices include mobile phones (e.g., cellular phones), PDAs, tablet computers, netbooks, laptop computers, personal music players, hand-held specialized readers, wearable devices (e.g., watches), vehicles (e.g., cars), etc. A mobile 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 relay - both devices taken together may be considered a single mobile device).

[0023] As used herein, the term "Authentication data" may refer to any data suitable for authenticating a user or mobile device. Authentication data may be obtained from a user or a device that is operated by the user. Examples of authentication data obtained from a user may include PINs (personal identification numbers), passwords, etc. Examples of authentication data that may be obtained from a device may include device serial numbers, hardware secure element identifiers, device fingerprints, phone numbers, IMEI numbers, etc.

[0024] **FIG. 1** illustrates an exemplary flow of a method for generating a split payment token, in accordance with some embodiments of the present disclosure.

[0025] As illustrated in FIG. 1, the method for creating a split payment token in an online framework is implemented using an exemplary setup 100. The setup 100 comprises one or more cardholders 101_N, a VISA web portal 103, an authentication system 105, and a token 107. The authentication system 105 may be associated with a database 109, which is used to store details of authorized transactions and authentication messages. The method of generating the split payment token is further explained with the help of flowchart in **FIG. 2**.

[0026] In an embodiment, at step 203 of FIG. 2, the cardholder(s) 101_N upload each card and/or payment account reference into the VISA web portal 103 to set up multiple Primary Account Numbers (PANs) to split payments equally or based on one or more rules. The PAN on a credit card or debit card identifies the unique cardholder account and the issuer associated with the card. PAN is a unique identifier used to identify customers/cardholders. An “issuer” may

typically include a business entity (for example, a bank) that maintains an account for the cardholder/user associated with a portable communication device. An issuer may be associated with a host system that performs some or all of the functions of the issuer on behalf of the issuer.

[0027] One or more rules for splitting the payments may include:

(i) performing an even split amongst all cards regardless of purchase;

(ii) performing a ratio, percentage, or nominal based split for each card regardless of purchase type;

(iii) performing split on certain cards for different purchase types, for example, split 50:50 for cards A & B for the gas bill, however, split cards A, B & C equally for the Netflix subscription or any other entertainment subscriptions; and

(iv) Use specific rules based on different merchants/Merchant Category Codes (MCCs) based on the type of split mentioned above.

(v) Decline all payments that are over threshold of £100 in certain MCCs.

[0028] At step 205, the uploaded PAN is verified for authenticity by the authentication system 105 to confirm that it may be used in the split payment rules. At step 207, the authentication system 105 verifies that all cards are approved for the use or not. If the cards are not approved or rejected, a token 107 may not be generated and the procedure is aborted (i.e., process ends at step 215). Further, once the cards receive an approval message from the authentication system 105 to use in the payment transaction, the PANs and associated rules are stored in the database 109, as shown in step 209. At step 211, a token may be generated using VISA token vault, and the generated token(s) are sent to the cardholders for use in payment transactions.

[0029] In a non-limiting embodiment, the generated “token” may be provided in the form of a physical payment card that can be used in face-to-face transactions. This token may also be provisioned as a card in a digital payment wallet, for use in face-to-face transactions. In this non-limiting example the physical card acts as the token to trigger the secondary multiple payment authorisations.

[0030] **FIG. 3** illustrates an exemplary flow of a method for performing automated multi-transactions in a single process by a split payment token, in accordance with some embodiments of the present disclosure.

[0031] In an embodiment, as illustrated in FIG. 3, at step 303, the cardholder and/or a user of the card initiates card transactions at any payment device to purchase certain items or goods. Thereafter, it is determined, at step 305, whether a split payment token was used to initiate the card transactions, and specifically, if a split payment Primary Account Number (PAN) token was used. After the card transaction has been validated, VISA server sends the PAN to a split database, wherein the split database searches for the tokens associated with the rules, as well as the PANs and returns the tokens to the authorization server, at step 309. The authorization server then initiates, at step 311, unique or distinct transactions for each card transaction in accordance with the rules and approves the transactions at step 313. The lead cardholder i.e. the cardholder who is using their token to initiate the split transaction may be authorised via a full Three Domain (3D) secure authorisation based on a pass through to their personal card, whereas the other cards involved in the split transaction as according to the rules may be authorised as a pre-approved card on file transaction after the lead cardholder has been fully authenticated. For subsequent recurring transactions all cardholders may be authorised as a card on file transaction. Upon successful approval of the transactions, the authorization server sends a single authorization message to an acquirer at step 315. Further, the authorization server allocates all the transactions to a single reference link for clearing the card transactions and completing the purchase of the goods after receiving an authorized message from the acquirer, as shown in step 317. A single decline message is issued back to the acquirer if any of the transactions are not approved, as indicated in step 319. In the event of a single decline where other transactions have already been approved, all the approved transactions are 'cancelled' and not submitted for clearing, as shown in step 321.

[0032] **FIG. 4a** and **FIG. 4b** illustrate an exemplary flow of a method for distributing split authorization among multiple contacts, in accordance with some embodiments of the present disclosure.

[0033] In an embodiment, consider a cardholder 'A' as an example. Suppose the cardholder 'A' has a split payment token required for purchasing goods/items and completing the checkout process. Here, the merchant may use the token to initiate the payment transaction on an online platform, as indicated in step 405. Further, at step 407, the token of the cardholder ‘A’ is verified with the generated split token stored in a split payment vault. Once the token is verified and matched with the split payment vault, the token vault (i.e., the VISA token vault) returns contact details associated with the token at step 411. As an example, the contact details here

may include a phone number or an email address of one or more other cardholders. Subsequently, at step 413, once the original token PAN is approved, a notification message, along with the payment link, is sent by the VISA token vault or the merchant to the contact details of the cardholders, prompting the cardholder to pay a portion of the payment. The cardholders can then establish a connection via a link to make payments of a certain, predetermined amount after the original token PAN is accepted, as indicated in step 415, and transmit the payment information/confirmation data to VISA or the merchant acceptance portals (for example, portal X, portal Y and portal Z).

[0034] In some embodiments, if the cardholder ‘A’ does not receive a payment link, the cardholder’s split payment token is mapped with own personal PAN, as indicated at step 409, and the transaction is processed to the VISA server for authorization, as indicated in step 421. In one embodiment cardholder ‘A’ may have their lead PAN authorised for the total amount of the transaction, as those defined by the split payment rules are then requested for their share of the transaction and as they make their payments the total amount that is due to be submitted in clearing for cardholder ‘A’ is reduced and replaced by the payment from the other cardholders.

[0035] In some embodiments, in any instance, if the contacts need to be reauthorized, each contact is requested to perform a reauthorization of contacts and is subsequently sent to step 409 for verification with VISA/merchant's new acceptance portals. Thereafter, VISA authorizes all the payments with the issuer, received from the merchant acceptance portals X, Y and Z. Once an initial token, i.e., the split payment token is authenticated and approved for use, VISA provides the merchant with a holding authorization to enable to checkout to idle in the backend, as shown in step 427. For example, the payment portal may be closed, and wait for the complete/full authorization or subsequent decline to be transmitted to the merchant after a set period of time. After receiving the payment approval, VISA proceeds to step 431, where VISA sends an authentication approval message to the merchant linked with the original PAN and settles with the issuers of each contact's PAN separately. Further, VISA completes the financial transaction by making a single settlement with the acquirer under the split payment token PAN by aggregating the settlement amount of the additional contacts/PANs in the background, as indicated in step 435 and step 437.

[0036] In some embodiments, the individual contacts are prompted to reauthorize using the merchant's new acceptance gateway if the payment is not authorized for the first transaction. In some embodiments, the payment transactions may fail if one or more payments continue to

be declined and/or are still delinquent after a predetermined period of time. This causes the whole transaction to be declined.

[0037] This method can also be used to enable further authorisation of payments made via card. For example, say Cardholder 'A' initiates a transaction for £290 at a merchant using a generated Token. The rules behind this token may be that for the transaction to process Contact 'Y' must approve the transaction before it is approved. This method allows for dual authorisation of payments, which could be useful for corporate or business cards or in situations where two cardholders have a joint bank account.

[0038] **FIG. 5** illustrates an exemplary flow diagram of a method for splitting payments online using a token, in accordance with some embodiments of the present disclosure.

[0039] As illustrated in FIG. 5, a VISA process 501 may be used to set up a split token payment described in FIG. 1, wherein the cards associated with each cardholder are linked to split simultaneously and/or the tokens are associated with rules to split simultaneously. In an embodiment, at 503, a payment device initiates payment transactions for the goods purchased by cardholders (503_1 or 503_2 or 503_3). For example, cardholder 1 (503_1) or cardholder 2 (503_2) or cardholder 3 (503_3) may initiate the payment transaction using their payment splitting token PAN. An acquirer 507 receives the payment information obtained from the cardholder via a merchant acceptance portal 1 as it would a normal transaction and sends this to Visa for authorisation. Visa then performs the payment splitting process according to the rules set up in 501. The payment splitting process as indicated in step 511 (also explained with reference to FIG. 4a and FIG. 4b) and performs the separate authorisations to cardholders (503_1 or 503_2 or 503_3) as according to the rules set up in 501 and obtains authorisation from the respective issuers. After the issuer authorizes the payment transactions, the acquirer 507 sends a single message confirming authorization of the payment to the merchant acceptance portal 1. Further, the payment transaction may be completed by sending authorization information to cardholders via their issuer or through a digital communication.

Advantages of the present invention:

[0040] In an embodiment, the present disclosure provides a means for splitting payments online using a token, and thereby enables multiple transactions to be automated in a single process.

[0041] In an embodiment, the present disclosure provides a secure and controlled environment for sharing/ splitting payments via a personalised token that can be authorised among multiple contacts.

[0042] In an embodiment, the present disclosure uses a single token to process multiple payments on different PANs based on associated VISA database and cardholder input.

[0043] In an embodiment, the present disclosure improves the transaction processing speed and simplifies the payment process by triggering several authorizations from a single authorisation request and then aggregating said authorizations back into a single authorization response to enable more efficient and easier processing by the merchant and acquirer.

[0044] In an embodiment, the present disclosure enables multiple cardholders to be automatically promoted for payment/ authorisation based on a lead cardholder initiating a transaction.

[0045] In an embodiment, the present disclosure enables a method for transaction to be authorized by multiple parties to satisfy the audit requirements of transactions, notably in businesses.

General computer system:

[0046] FIG. 6 illustrates a block diagram of an exemplary computer system for implementing embodiments consistent with the present disclosure.

[0047] In an embodiment, FIG. 6 illustrates a block diagram of an exemplary computer system 600 which may be used to implement the system in accordance with the present disclosure. The computer system 600 may include a central processing unit (“CPU” or “processor”) 602. In some embodiments, the computer system 600 may be an authentication system 205 to perform authentication of all the approved transactions and assign the approved transaction into a single reference link to clear the approved transaction via a network interface 603 and communication network 609. The processor 602 may include at least one data processor for authorizing the transaction based on the inputs received from a cardholder and generated tokens associated with rules. The processor 602 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.

[0048] The processor 602 may be disposed in communication with one or more Input/Output (I/O) devices (612 and 613) via I/O interface 601. The I/O interface 601 employ communication protocols/methods such as, without limitation, audio, analog, digital, monoaural, Radio Corporation of America (RCA) connector, stereo, IEEE-1394 high-speed serial bus, serial bus, Universal Serial Bus (USB), infrared, Personal System/2 (PS/2) port, Bayonet Neill-Concelman (BNC) connector, coaxial, component, composite, Digital Visual Interface (DVI), High-Definition Multimedia Interface (HDMI), Radio Frequency (RF) antennas, S-Video, Video Graphics Array (VGA), IEEE 802.11b/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), Worldwide Interoperability for Microwave access (WiMax), or the like, etc.

[0049] Using the I/O interface 601, the computer system 600 may communicate with one or more I/O devices such as input devices 612 and output devices 613. For example, the input devices 612 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 devices 613 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.

[0050] In some embodiments, the processor 602 may be disposed in communication with a communication network 609 via a network interface 603. The network interface 603 may communicate with the communication network 609. The network interface 603 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 609 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 603 and the communication network 609, the computer system 600 may communicate with a database 614, which may be the enrolled templates database 613. The network interface 603 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.

[0051] The communication network 609 includes, but is not limited to, a direct interconnection, 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 communication network 609 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 communication network 609 may include a variety of network devices, including routers, bridges, servers, computing devices, storage devices, etc.

[0052] In some embodiments, the processor 602 may be disposed in communication with a memory 605 (e.g., RAM, ROM, etc. not shown in Fig. 6) via a storage interface 604. The storage interface 604 may connect to memory 605 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.

[0053] The memory 605 may store a collection of program or database components, including, without limitation, user interface 606, an operating system 607, a web browser 608 etc. In some embodiments, computer system 600 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.

[0054] The operating system 607 may facilitate resource management and operation of the computer system 600. Examples of operating systems include, without limitation, Apple Macintosh OS X™, UNIX™, Unix-like system distributions (e.g., Berkeley Software Distribution (BSD), FreeBSD, Net BSD™, Open BSD™, etc.), Linux distributions (e.g., Red Hat, Ubuntu, K-Ubuntu, etc.), International Business Machines (IBM™) OS/2™, Microsoft Windows (XP™, Vista/7/8, etc.), Apple iOS, Google Android, BlackBerry operating system (OS), or the like. The User Interface 606 may facilitate display, execution, interaction, manipulation, or operation of program components through textual or graphical facilities. For example, user interfaces may provide computer interaction interface elements on a display

system operatively connected to the computer system 600, such as cursors, icons, checkboxes, menus, scrollers, windows, widgets, etc. Graphical User Interfaces (GUIs) may be employed, including, without limitation, Apple® Macintosh® operating systems' Aqua®, IBM® OS/2®, Microsoft® Windows® (e.g., Aero, Metro, etc.), web interface libraries (e.g., ActiveX®, Java®, JavaScript®, AJAX, HTML, Adobe® Flash®, etc.), or the like.

[0055] In some embodiments, the computer system 600 may implement web browser 608 stored program components. Web browser 608 may be a hypertext viewing application, such as Microsoft Internet Explorer, Google Chrome, Mozilla Firefox, Apple Safari, etc. Secure web browsing may be provided using secure hypertext transport protocol (HTTPS), Secure Sockets Layer (SSL), Transport Layer Security (TLS), etc. Web browsers 608 may utilize facilities such as AJAX, DHTML, Adobe Flash, JavaScript, Application Programming Interfaces (APIs), etc.

[0056] In some embodiments, the computer system 600 may implement a mail server 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, ActiveX, ANSI C++/C#, Microsoft .NET, Common Gateway Interface (CGI) scripts, Java, JavaScript, PERL, PHP, Python, WebObjects, etc. The mail server may utilize communication protocols such as Internet Message Access Protocol (IMAP), Messaging Application Programming Interface (MAPI), Microsoft Exchange, Post Office Protocol (POP), Simple Mail Transfer Protocol (SMTP), or the like.

[0057] In some embodiments, the computer system 600 may implement a mail client stored program component. The mail client may be a mail viewing application, such as APPLE® MAIL, MICROSOFT® ENTOURAGE®, MICROSOFT® OUTLOOK®, MOZILLA® THUNDERBIRD®, etc.

[0058] 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, Compact Disc (CD) ROMs, DVDs, flash drives, disks, and any other known physical storage media.

[0059] The described operations may be implemented as a method, system or article of manufacture using standard programming and/or engineering techniques to produce software, firmware, hardware, or any combination thereof. The described operations may be implemented as code maintained in a “non-transitory computer-readable medium”, where a processor may read and execute the code from the computer-readable medium. The processor is at least one of a microprocessor and a processor capable of processing and executing the queries. A non-transitory computer-readable medium may include media such as magnetic storage medium (e.g., hard disk drives, floppy disks, tape, etc.), optical storage (CD-ROMs, DVDs, optical disks, etc.), volatile and non-volatile memory devices (e.g., EEPROMs, ROMs, PROMs, RAMs, DRAMs, SRAMs, Flash Memory, firmware, programmable logic, etc.), etc. Further, non-transitory computer-readable media may include all computer-readable media except for transitory. The code implementing the described operations may further be implemented in hardware logic (e.g., an integrated circuit chip, Programmable Gate Array (PGA), Application Specific Integrated Circuit (ASIC), etc.).

[0060] The illustrated steps are set out to explain the exemplary embodiments shown, and it should be anticipated that ongoing technological development will change the manner in which particular functions are performed. These examples are presented herein for purposes of illustration, and not limitation. Further, the boundaries of the functional building blocks have been arbitrarily defined herein for the convenience of the description. Alternative boundaries can be defined so long as the specified functions and relationships thereof are appropriately performed. Alternatives (including equivalents, extensions, variations, deviations, etc., of those described herein) will be apparent to persons skilled in the relevant art(s) based on the teachings contained herein. Such alternatives fall within the scope and spirit of the disclosed embodiments. Also, the words "comprising," "having," "containing," and "including," and other similar forms are intended to be equivalent in meaning and be open ended in that an item or items following any one of these words is not meant to be an exhaustive listing of such item or items or meant to be limited to only the listed item or items. It must also be noted that as

used herein, the singular forms “a,” “an,” and “the” include plural references unless the context clearly dictates otherwise.

[0061] 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., are 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.

[0062] 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.

[0063] 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.

"SPLITTING AND AUTHORISING CARD PAYMENTS ACROSS MULTIPLE USERS ONLINE VIA A SINGLE PAYMENT TOKEN"

ABSTRACT

The present disclosure relates to a method for splitting and authorizing payments online using tokens. The present disclosure demonstrates how a token based on card or payment account reference of a cardholder can be used to trigger payments from multiple accounts to split the total transaction cost based on a set of pre-determined rules. The method allows users to link multiple payment accounts to a single lead token, which in turn can be used to make payments from said accounts according to a set of rules. Generating a single lead token, allows this payment splitting method to be used at an existing card-based point of sale without the need for multi-party ecosystem enablement. The method can also enable dual/ multiple authorizations of a payment based on the lead token, for example a payment card, by requesting further authorization from another party. The method works by mapping the generated token, rules, and the payment account, for example a Primary Account Number (PAN) together in a lookup fashion to be read and processed by an authorization system. Based on the rules associated with the tokens, the authorization system initiates separate transactions and approves them or seeks further authorisation for a transaction. Initiating a single token payment, matching the format, and processing requirements of existing payment methods, triggering additional authorizations compliant with existing payment methods to receive appropriate authorizations from multiple accounts and then returning a single authorisation response tied to a single reference for the transaction, allows instant operability of the solution without the need for multi-party ecosystem enablement.

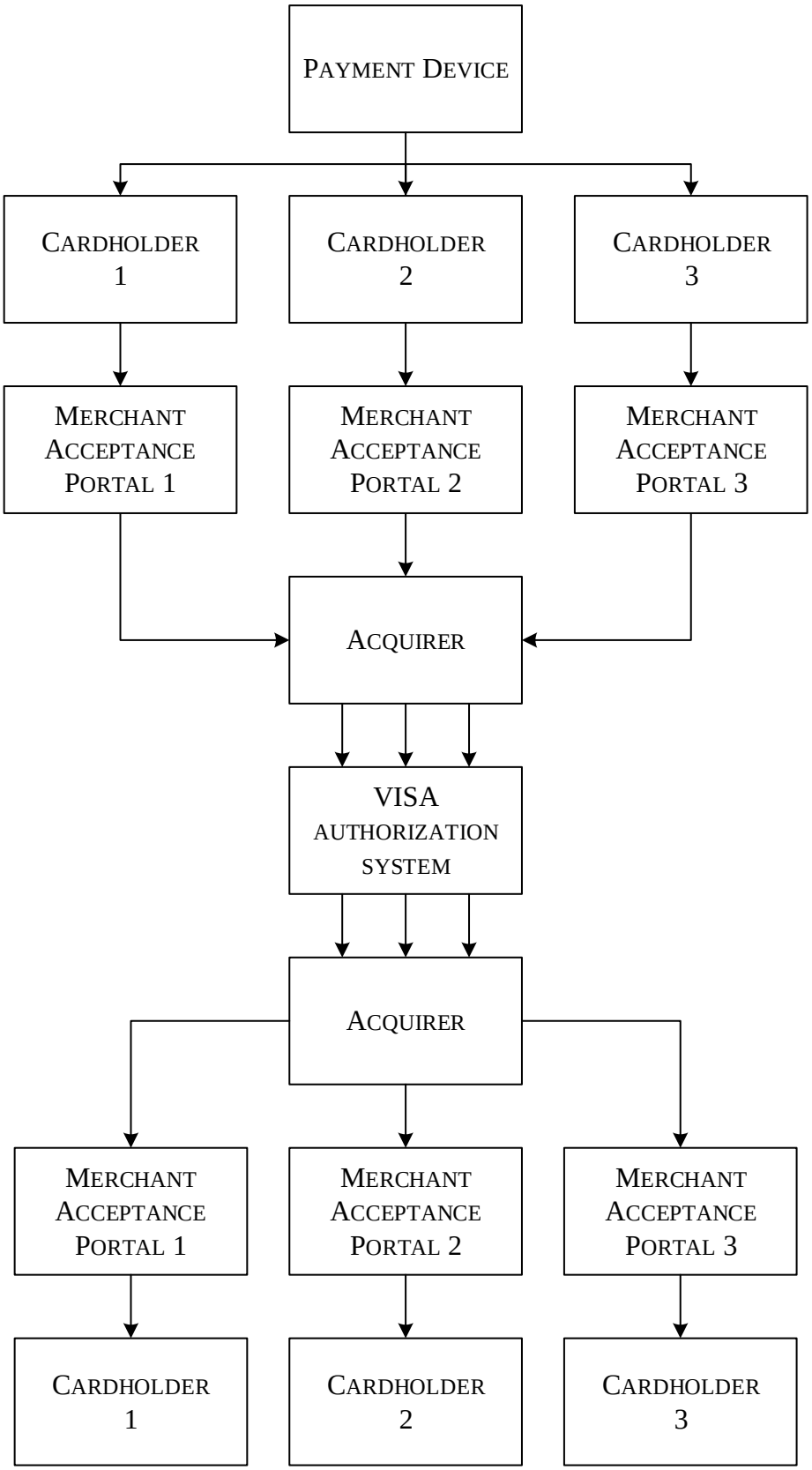
PAYMENT DEVICE
CARDHOLDER 1
CARDHOLDER 2
CARDHOLDER 3
MERCHANT ACCEPTANCE PORTAL 1
MERCHANT ACCEPTANCE PORTAL 2
MERCHANT ACCEPTANCE PORTAL 3
ACQUIRER
VISA AUTHORIZATION SYSTEM
ACQUIRER
MERCHANT ACCEPTANCE PORTAL 1
MERCHANT ACCEPTANCE PORTAL 2
MERCHANT ACCEPTANCE PORTAL 3
CARDHOLDER 1
CARDHOLDER 2
CARDHOLDER 3

FIG. A

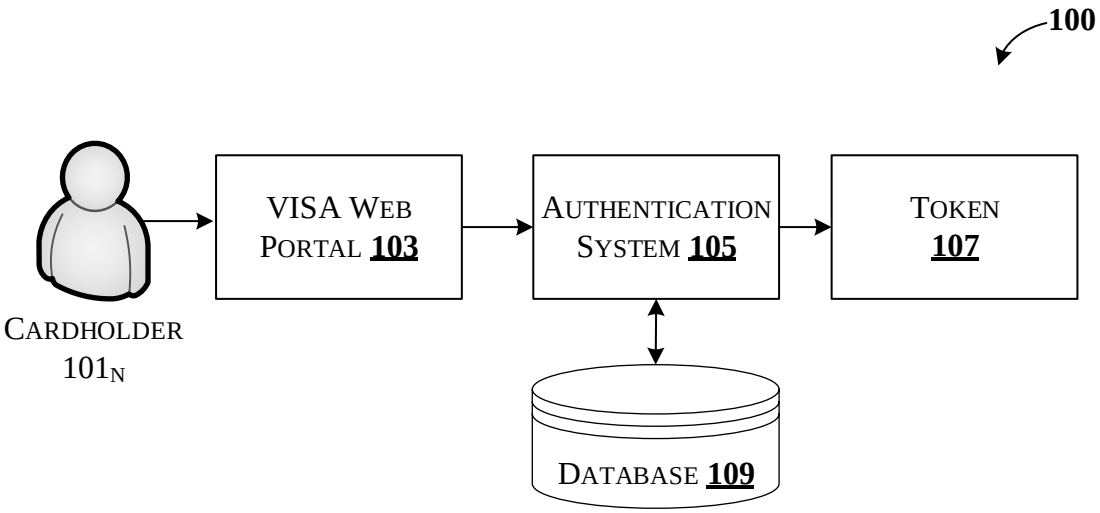
100
CARDHOLDER
101N
VISA WEB PORTAL 103
AUTHENTICATION SYSTEM 105
TOKEN 107
DATABASE 109

FIG. 1

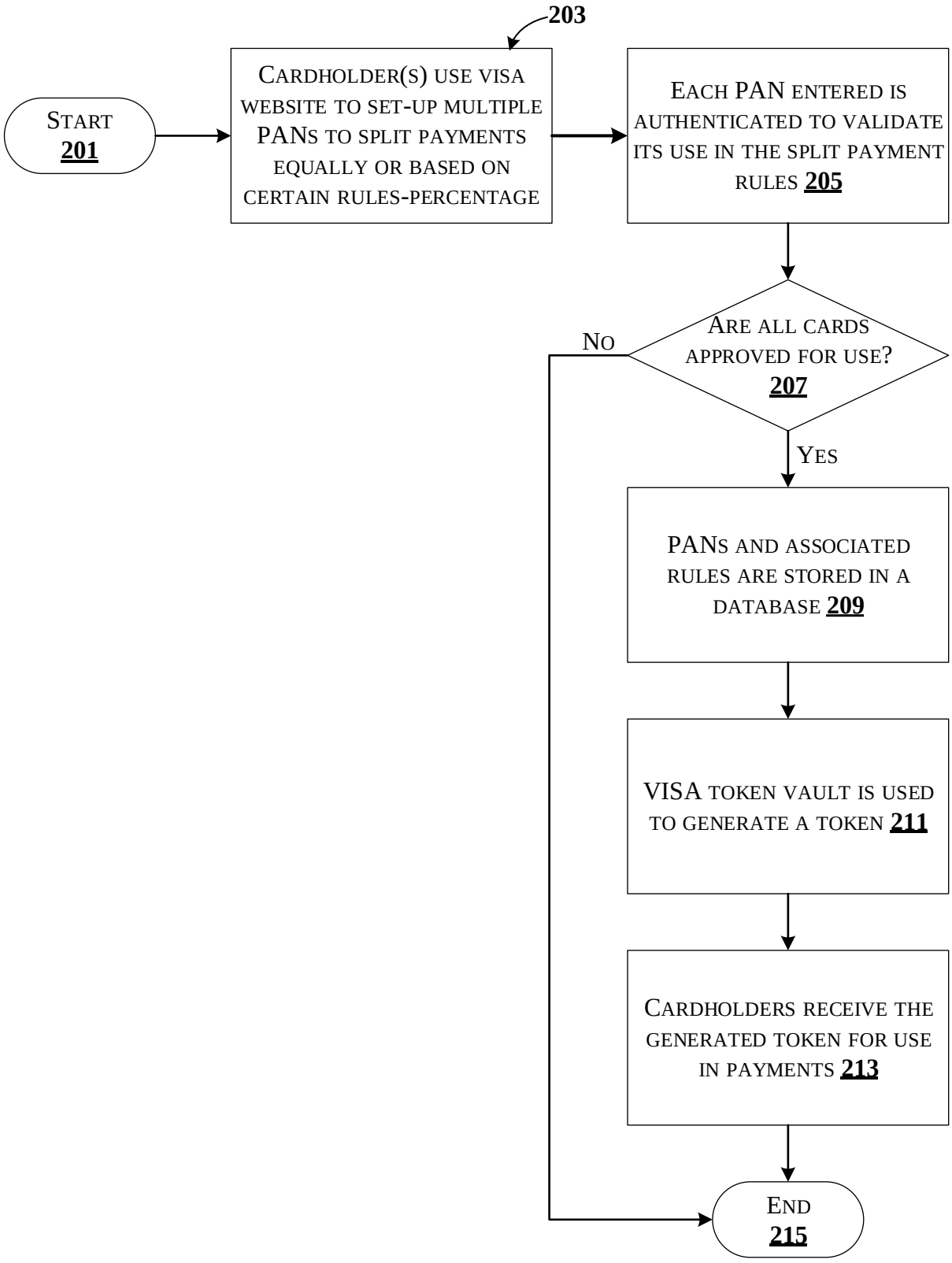
203
START
201
CARDHOLDER(S) USE VISA WEBSITE TO SET-UP MULTIPLE PANS TO SPLIT PAYMENTS EQUALLY OR BASED ON CERTAIN RULES-PERCENTAGE
EACH PAN ENTERED IS AUTHENTICATED TO VALIDATE ITS USE IN THE SPLIT PAYMENT RULES 205
ARE ALL CARDS APPROVED FOR USE? 207
NO
YES
PANS AND ASSOCIATED RULES ARE STORED IN A DATABASE 209
VISA TOKEN VAULT IS USED TO GENERATE A TOKEN 211
CARDHOLDERS RECEIVE THE GENERATED TOKEN FOR USE IN PAYMENTS 213
END
215

FIG. 2

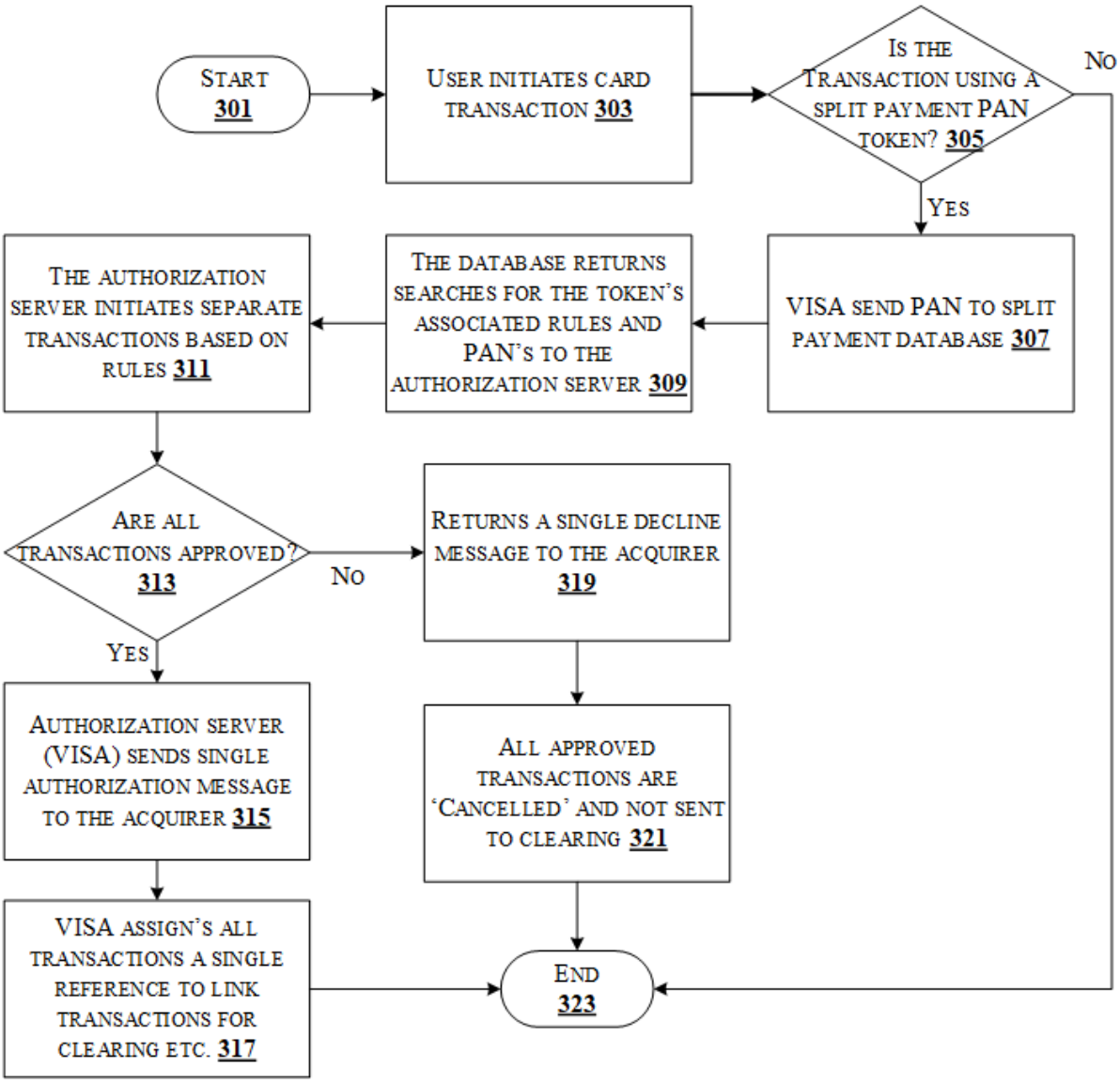
START 301
USER INITIATES CARD TRANSACTION 303
IS THE TRANSACTION USING A SPLIT PAYMENT PAN TOKEN? 305
No
Yes
VISA SEND PAN TO SPLIT PAYMENT DATABASE 307
THE DATABASE RETURNS SEARCHES FOR THE TOKEN'S ASSOCIATED RULES AND PAN'S TO THE AUTHORIZATION SERVER 309
THE AUTHORIZATION SERVER INITIATES SEPARATE TRANSACTIONS BASED ON RULES 311
ARE ALL TRANSACTIONS APPROVED? 313
No
Yes
RETURNS A SINGLE DECLINE MESSAGE TO THE ACQUIRER 319
AUTHORIZATION SERVER (VISA) SENDS SINGLE AUTHORIZATION MESSAGE TO THE ACQUIRER 315
ALL APPROVED TRANSACTIONS ARE 'CANCELLED' AND NOT SENT TO CLEARING 321
VISA ASSIGN'S ALL TRANSACTIONS A SINGLE REFERENCE TO LINK TRANSACTIONS FOR CLEARING ETC. 317
END 323

FIG. 3

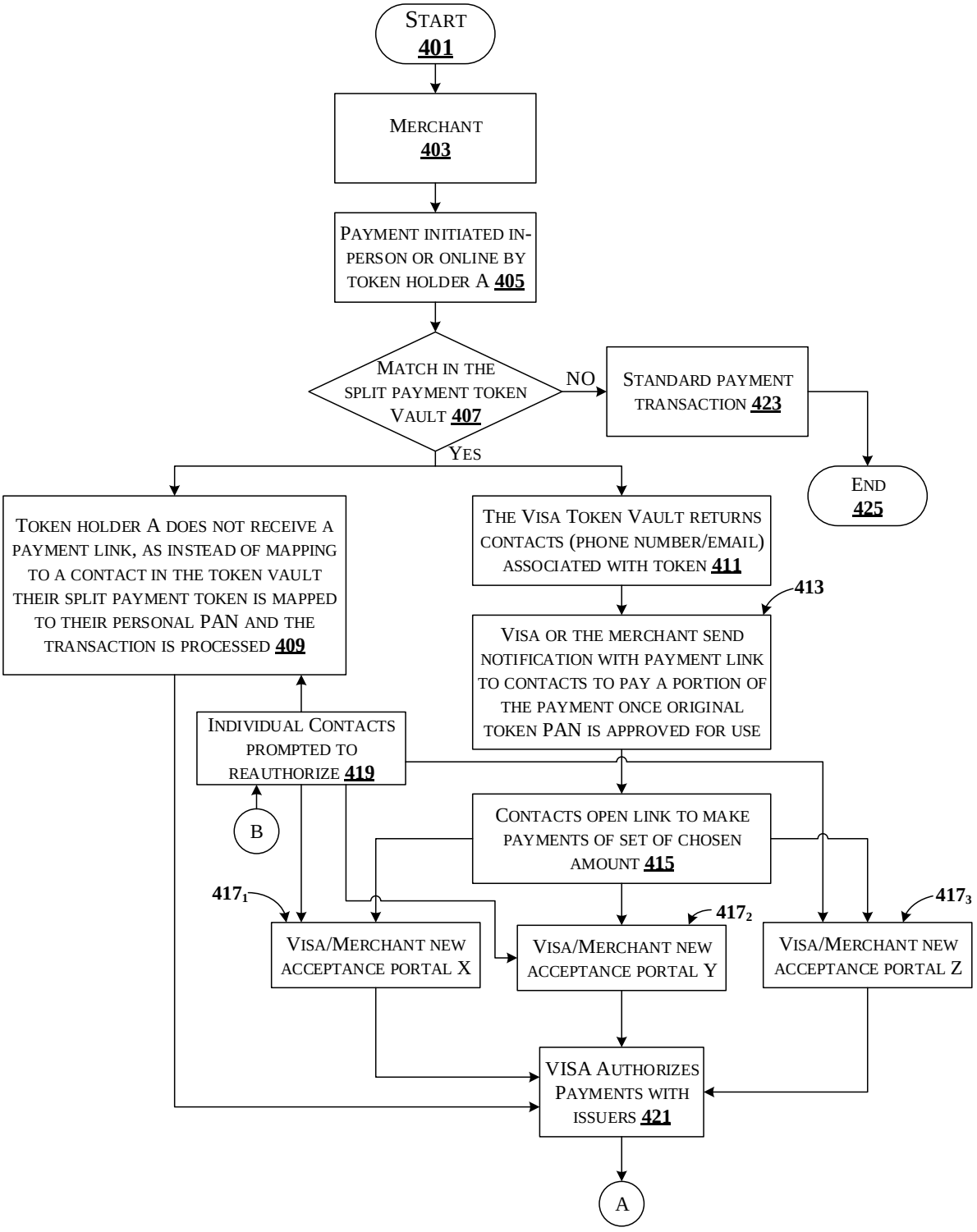
START 401
MERCHANT 403
PAYMENT INITIATED IN-PERSON OR ONLINE BY TOKEN HOLDER A 405
MATCH IN THE SPLIT PAYMENT TOKEN VAULT 407
NO
STANDARD PAYMENT TRANSACTION 423
END 425
YES
TOKEN HOLDER A DOES NOT RECEIVE A PAYMENT LINK, AS INSTEAD OF MAPPING TO A CONTACT IN THE TOKEN VAULT THEIR SPLIT PAYMENT TOKEN IS MAPPED TO THEIR PERSONAL PAN AND THE TRANSACTION IS PROCESSED 409
THE VISA TOKEN VAULT RETURNS CONTACTS (PHONE NUMBER/EMAIL) ASSOCIATED WITH TOKEN 411
413
VISA OR THE MERCHANT SEND NOTIFICATION WITH PAYMENT LINK TO CONTACTS TO PAY A PORTION OF THE PAYMENT ONCE ORIGINAL TOKEN PAN IS APPROVED FOR USE
INDIVIDUAL CONTACTS PROMPTED TO REAUTHORIZE 419
B
CONTACTS OPEN LINK TO MAKE PAYMENTS OF SET OF CHOSEN AMOUNT 415
417₁
417₂
417₃
VISA/MERCHANT NEW ACCEPTANCE PORTAL X
VISA/MERCHANT NEW ACCEPTANCE PORTAL Y
VISA/MERCHANT NEW ACCEPTANCE PORTAL Z
VISA AUTHORIZES PAYMENTS WITH ISSUERS 421
A

FIG. 4a

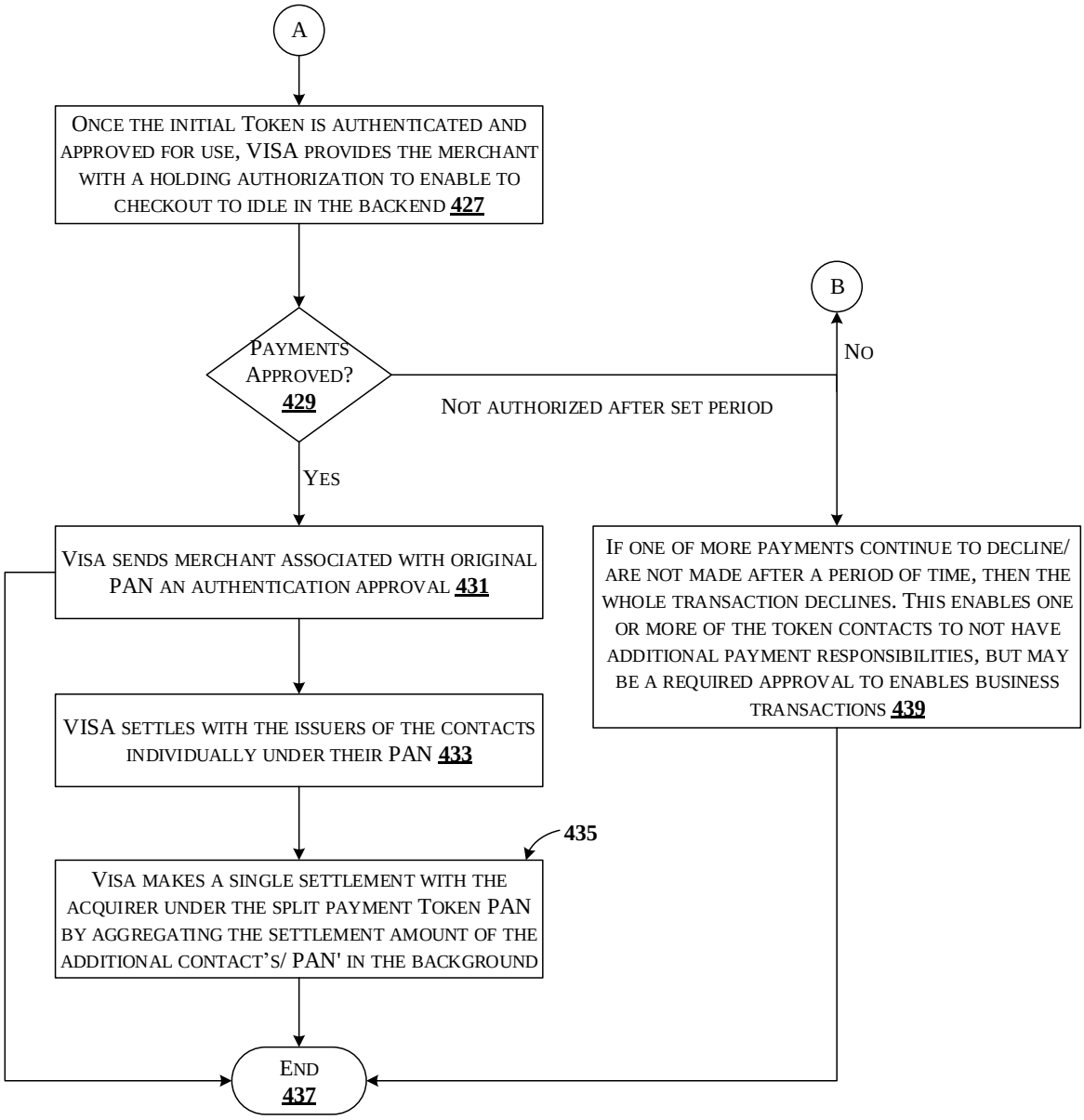
A
ONCE THE INITIAL TOKEN IS AUTHENTICATED AND APPROVED FOR USE, VISA PROVIDES THE MERCHANT WITH A HOLDING AUTHORIZATION TO ENABLE TO CHECKOUT TO IDLE IN THE BACKEND 427
B
PAYMENTS APPROVED? 429
NO
NOT AUTHORIZED AFTER SET PERIOD
YES
VISA SENDS MERCHANT ASSOCIATED WITH ORIGINAL PAN AN AUTHENTICATION APPROVAL 431
IF ONE OF MORE PAYMENTS CONTINUE TO DECLINE/ ARE NOT MADE AFTER A PERIOD OF TIME, THEN THE WHOLE TRANSACTION DECLINES. THIS ENABLES ONE OR MORE OF THE TOKEN CONTACTS TO NOT HAVE ADDITIONAL PAYMENT RESPONSIBILITIES, BUT MAY BE A REQUIRED APPROVAL TO ENABLES BUSINESS TRANSACTIONS 439
VISA SETTLES WITH THE ISSUERS OF THE CONTACTS INDIVIDUALLY UNDER THEIR PAN 433
435
VISA MAKES A SINGLE SETTLEMENT WITH THE ACQUIRER UNDER THE SPLIT PAYMENT TOKEN PAN BY AGGREGATING THE SETTLEMENT AMOUNT OF THE ADDITIONAL CONTACT'S/ PAN' IN THE BACKGROUND
END 437

FIG. 4b

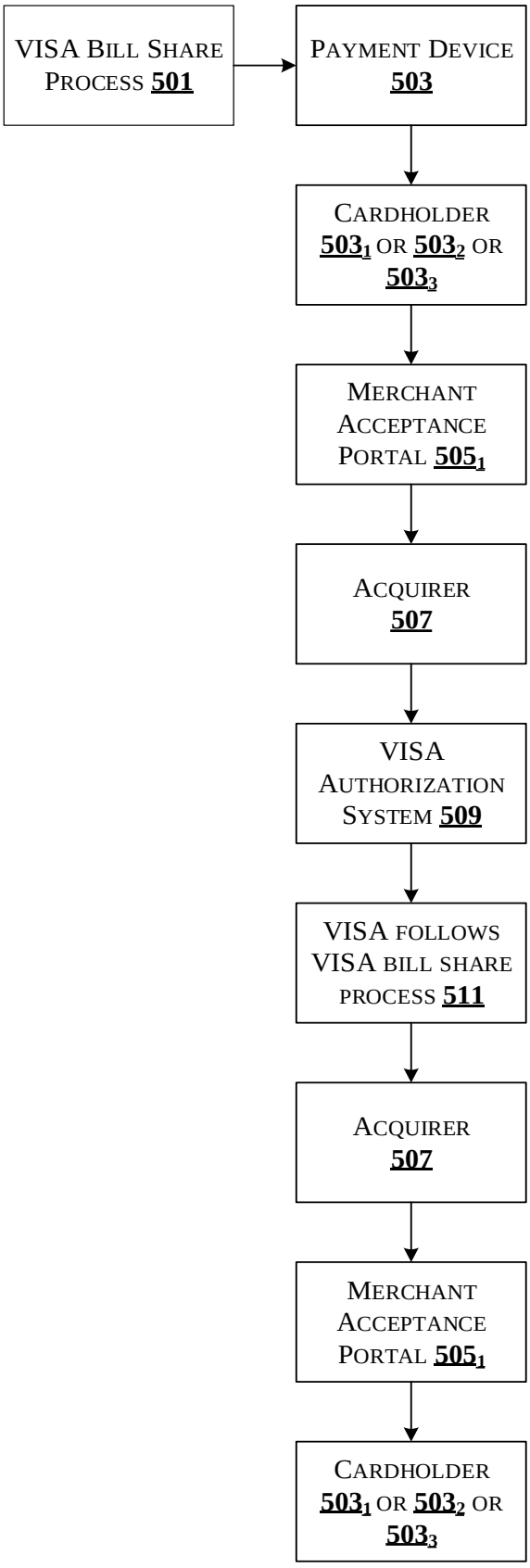
VISA BILL SHARE PROCESS 501
PAYMENT DEVICE 503
CARDHOLDER 503$_1$ OR 503$_2$ OR 503$_3$
MERCHANT ACCEPTANCE PORTAL 505$_1$
ACQUIRER 507
VISA AUTHORIZATION SYSTEM 509
VISA FOLLOWS VISA BILL SHARE PROCESS 511
ACQUIRER 507
MERCHANT ACCEPTANCE PORTAL 505$_1$
CARDHOLDER 503$_1$ OR 503$_2$ OR 503$_3$

FIG. 5

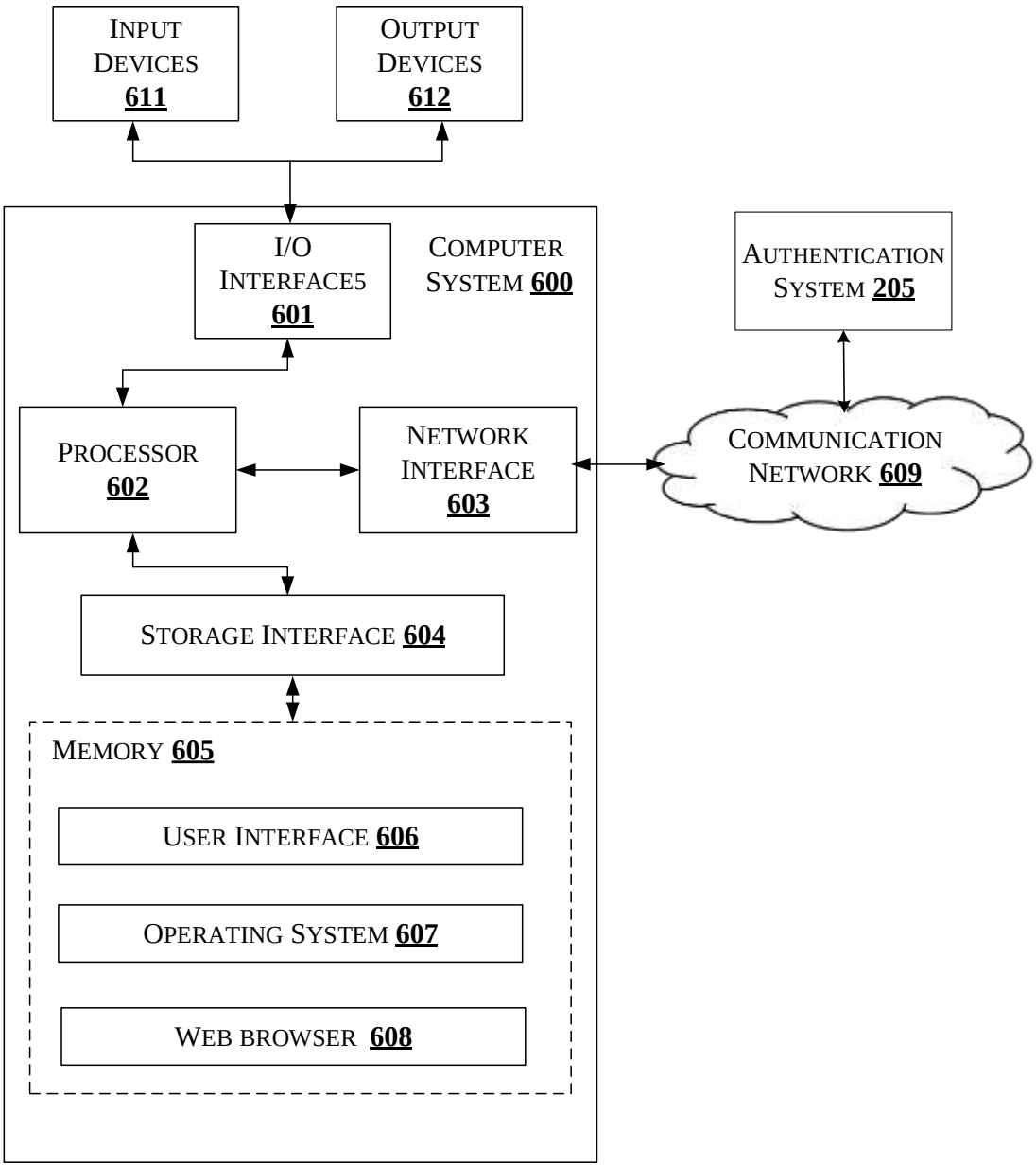
INPUT DEVICES 611
OUTPUT DEVICES 612
I/O INTERFACE5 601
COMPUTER SYSTEM 600
AUTHENTICATION SYSTEM 205
PROCESSOR 602
NETWORK INTERFACE 603
COMMUNICATION NETWORK 609
STORAGE INTERFACE 604
MEMORY 605
USER INTERFACE 606
OPERATING SYSTEM 607
WEB BROWSER 608

FIG. 6