August 2023

LIVE MERCHANT ENVIRONMENT

RANJIVA PRASAD
VISA

ROHIT ANAND
VISA

STANISLAVA MUSEVA
VISA

THU HUONG TRAN
VISA

PRATOMCHAI PUSAKOLCHAROENSAK
VISA

“LIVE MERCHANT ENVIRONMENT”

VISA

INVENTORS:

RANJIVA PRASAD

ROHIT ANAND

STANISLAVA MUSEVA

THU HUONG TRAN

PRATOMCHAI PUSAKOLCHAROENSAK

TECHNICAL FIELD

[0001] The present subject matter is, in general, related to the field of financial services, and particularly, but not exclusively to a system and method for operating a live merchant platform.

BACKGROUND

[0002] In general, a network payment system is utilized to authenticate and authorize any payment transaction in a user-to-merchant transaction performed over the Internet. The Internet links a merchant server, an issuer server, an acquirer server, and a user device associated with the user to a payment server. In the existing methods, the merchant server may have full access to user spending details and be able to review the performance of the user payment transaction with respect to checkout, authentication, authorization, clearing and settlement activities. However, a payment server (for example, Visa payment server) will be unable to test the end-to-end seller proposition experience without the merchant server involvement across a range of issuers.

[0003] Moreover, the existing certification environment may be able to test some of the steps in the financial transaction flow, however it is unable to test across a wide range of issuers. For example, user experience data collected from the certification environment is restricted to providing answers to the questions related to working of the transaction flow, however, it will be unable to provide information on the checkout experience with a particular issuer. Further, users who shop online base their judgments on information related to the product's objective qualities, user reviews, suggestions/recommendations, and the product and merchant comparisons via online shopping tools.

[0004] Additionally, the payment server gathers the experience information to perform a Proof-of-Concept (PoC) scheme or a pilot scheme with the merchant. For example, with linked loyalty programs, market funds may be used to incentivize a retailer to participate in the PoC scheme. However, the payment server may find it challenging to become a merchant due to the scheme rules and regulations. Therefore, there is a need for a live merchant environment in partnership with a friendly merchant and acquirer to test a range of online and offline/face-to-face payment experiences across issuers and potential schemes.

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. 1** illustrates an exemplary environment of a system for operating a live merchant platform, in accordance with some embodiments of the present disclosure.

[0007] **FIG. 2a** illustrates a schematic flow diagram indicating a method for operating a live merchant platform, in accordance with some embodiments of the present disclosure.

[0008] **FIG. 2b** shows an exemplary illustration of a live merchant platform for testing payment transaction experiences, in accordance with some embodiments of the present disclosure.

[0009] **FIG. 3** is a block diagram of an exemplary computer system for implementing embodiments consistent with the present disclosure.

[0010] 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

[0011] 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.

[0012] 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.

[0013] 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.

[0014] 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.

[0015] 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.

[0016] The terms "including", "comprising", “having” and variations thereof mean "including but not limited to" unless expressly specified otherwise.

[0017] 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.

[0018] As used herein, the term “computing device” may refer to one or more electronic devices that are configured to directly or indirectly communicate with 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. An “application” or “Application Program Interface” (API) refers 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”.

[0019] As used herein, the term "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., 3 Generation (3G), 4G or similar networks), Wireless Fidelity (Wi-Fi), Worldwide Interoperability for Microwave access (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), Personal Digital Assistants (PDAs), tablet computers, net books, laptop computers, personal music players, hand-held specialized readers, wearable devices (e.g., watches), vehicles (e.g., cars), etc. For example, 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.

[0020] As used herein, the term “server” may refer to or include one or more computing devices that are operated by or facilitate communication and processing for multiple parties in a network environment, such as the internet, although it will be appreciated that communication may be facilitated over one or more public or private network environments and that various other arrangements are possible. Further, multiple computing devices (for example, servers, POS devices, mobile devices, and so on) directly or indirectly communicating in the network environment may constitute a “system.” Reference to “a server” or “a processor,” as used herein, may refer to a previously recited server and/or processor that is recited as performing a previous step or function, a different server and/or processor, and/or a combination of servers and/or processors. For example, as used in the specification and the claims, a first server and/or a first processor that is recited as performing a first step or function may refer to the same or different server and/or a processor recited as performing a second step or function.

[0021] 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 Personal Identification Numbers (PINs), 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, International Mobile Equipment Identity (IMEI) numbers, etc.

[0022] **FIG. 1** illustrates an exemplary environment of a system for operating a live merchant platform, in accordance with some embodiments of the present disclosure.

[0023] As shown in **FIG. 1**, the system for operating the live merchant platform may be implemented in an environment 100 comprising, without limiting to, a user device 101, a live merchant platform 103, an issuer 107, and an acquirer 109 connected via a payment system 105, for example, VISA or Visa net. A user may wish to purchase goods/items online using the user device 101. The user device 101 may be a mobile device. The user may be an individual who has a savings account, and/or current account or any other type of account with a bank and uses a bank-issued credentials to perform financial transactions. Accordingly, the user may also be referred alternatively as a cardholder, an account holder, a customer, or a consumer.

[0024] In an embodiment, the user device 101 may comprise suitable hardware and software (pre-installed Application (App)) for performing one or more functions and may also include multiple sub-devices or sub-components. Further, the payment system 105 may include, without limitation, a direct interconnection, a wireless network (for example, using Wireless Application Protocol), the Internet, and the like. As an example, the payment system 105 could be an electronic payments network like VisaNet.

[0025] In an embodiment, the issuer 107 (also referred to as an issuer server) is associated with an issuer bank, which is the customer bank that issues, for example, a credit card or a debit card on behalf of the card schemes and an issuer Access Control Server (ACS). The issuer ACS is an ACS managed by the issuer 107 and performs the requested authentication services.

[0026] In an embodiment, the acquirer 109 may include one or more devices configured to communicate with, and/or facilitate communication between, a gateway environment and a core processing environment via the payment system 105. The acquirer 109 may include a computing device, such as a server (for example, a single server), a group of servers, and/or other like devices. The server may include one or more computing devices, which are operated by or facilitate communication and processing for multiple parties in a network environment, for example, a single server and/or the Internet.

[0027] In an embodiment, the live merchant platform 103 may include one or more devices configured to communicate with, and/or facilitate communication between, the gateway environment, a security protocol environment and the user. The live merchant platform 103 may be associated with a friendly merchant, for example, a Spielfeld store, that acts as a merchant. Further, the live merchant platform 103 may interface with the gateway environment to authenticate cardholder/user information. In an embodiment, the live merchant platform 103 may be a dedicated server or maybe a cloud-based server.

[0028] **FIG. 2a** illustrates a schematic flow indicating a method for operating a live merchant platform, in accordance with some embodiments of the present disclosure.

[0029] In an exemplary scenario, a user may wish to purchase an item/goods via a live merchant platform 103. Flows involved in operating the live merchant platform 103 include a cardholder authentication flow, a payment authorization flow, and a payment reversal flow. In an embodiment, the cardholder authentication flow is carried out between the user (for

example, payment server employee or payment server client), a payment server live merchant environment, a gateway environment, a security protocol environment, a core processing environment and an issuer environment. In an embodiment, the payment authorization flow is involved between the payment server live merchant environment, the gateway environment, the security protocol environment, the core processing environment, the issuer environment, and an acquirer environment. In an embodiment, the payment reversal flow is involved between the payment server live merchant environment, the gateway environment, the issuer environment, the acquirer environment and the user. The issuer environment and the acquirer environment are connected via a payment system 105.

[0030] In an embodiment, at step 1, once the goods are selected, the user provides one or more details of the cardholder using the user device 101 on a checkout page, wherein the checkout page is associated with the live merchant platform 103 and proceeds with the authorization process. The one or more details include, without limited to, a Primary Account Number (PAN), billing address, transaction details and so on (as shown in **FIG. 2b**). Thereafter, at step 2, the live merchant platform 103 makes a request to a gateway, for authentication of one or more details. At step 3, a security protocol server receives the request from the gateway for authentication of one or more details. For example, the gateway submits Primary Account Number (PAN) details to the security protocol server to check if the issuing bank is a participant in the security protocol program. The security protocol server may communicate with one another, for example, using APIs or browser interactions. The security protocol server is similar to data gathering computer device. The security protocol server is used to improve transaction performance online and to accelerate the growth of electronic commerce. The security protocol server is a technical platform that includes technical specifications and requirements for issuers, acquirers, and merchants. At step 4, a security protocol directory server receives a security protocol authentication request message from the security protocol server, wherein the authentication request message includes authentication data. The security protocol directory server extracts the authentication data from the authentication request message and transmits the extracted authentication data to an issuer ACS, as indicated at step 5. The issuer ACS then generates, based on the extracted authentication data, a cardholder authentication response and transmits the authentication response, along with a challenge indicator (ind), to the security protocol server via the security protocol directory server (as indicated in steps 6 and 7). The security protocol challenge indicator indicates whether a challenge is requested by the merchant for a particular transaction. At step 8, using the authentication response provided by

the security protocol server within the security protocol environment, the security protocol server forwards the cardholder authentication response within the ACS Uniform Resource Locator (URL) to the gateway. The ACS URL is obtained only when the issuing bank is a participant in security protocol program.

[0031] At step 9, the gateway forwards the authentication response with the ACS URL to the merchant (that is, for example, a Spielfeild store). Thereafter, at step 10, the merchant initiates the authentication request and opens a security protocol Merchant Plug-In (MPI) with the cardholder information. At step 11, the security protocol MPI may communicate with the issuer access control server by sending a challenge request to the issuer ACS. After the cardholder details are authenticated with the issuer ACS, the issuer ACS may transmit the result of the challenge to the security protocol MPI. Further, at step 12, the issuer ACS returns the ACS page, which will be displayed by the security protocol MPI. Consequently, the issuer ACS sends the challenge request to the user via an issuer mobile banking application (App) installed on a user device 101 (step 13). That is, the issuer requires additional authentication by the cardholder when the transaction is considered as high-risk.

[0032] At step 14, the user performs the challenge request using the issuer's mobile banking App. For example, the user enters a one-time password or performs biometric authentication using the issuer mobile banking App Thereafter, the issuer ACS receives the challenge response based on the user input and transmits the challenge response results to the security protocol server via the security protocol directory server (shown in steps 15-17). Subsequently, the challenge-response results are sent back from the security protocol server to the issuer ACS via the security protocol directory server (steps 18-19). That is, the response data may be transmitted to the ACS URL and contain a unique ACS transaction id associated with the original request. At step 20, the security protocol MPI receives the challenge response from the issuer ACS indicating that the cardholder details have been fully authenticated by their bank without the need for direct interaction. Once the cardholder is authenticated, the security protocol MPI may send a response back to the merchant (to the payment server live merchant environment) with the authentication results (step 21).

[0033] Upon successful completion of cardholder authentication, the payment authorization flow is initiated. In some embodiments, at step 22, the payment authorization flow is initiated by the merchant by sending a payment authorization request to the gateway. Thereafter, at step 23, the gateway transmits the request card to the security protocol server to request the Card

Authentication Verification Value (CAVV). At step 24, the security protocol server issues the CAVV to the gateway. At step 25, the gateway may submit a payment authorization request message along with the CAVV to the acquirer processor. Thereafter, the acquirer may forward the CAVV request message to an issuer host via a payment processing network, that is, a payment system 105 for authorization of a transaction (steps 26-27). Subsequently, the issuer host may generate a temporary identifier as a response to the payment authorization request and communicates the authorization response from the issuer host through the payment system 105 to the acquirer processor, wherein the temporary identifier may be linked to the authenticated user account (steps 28-29). Further, the acquirer provides the response to the merchant via the gateway (steps 30-31).

[0034] In some embodiments, the gateway receives a payment reversal request by the merchant (step 32) and submits the request to the acquirer processor (step 33). Thereafter, the issuer host receives the payment reversal request message from the acquirer processor via the payment system 105. For example, the payment system 105 receives a "0400" message from the acquirer processor (step 34) and the issuer host receives a "0400" request message from the payment system 105 (step 35). At step 36, the payment system 105 receives the "0410" response from the issuer host. At step 37, the gateway receives a "0410" message as a response from the payment system 105 via the acquirer processor, wherein the "0410" message includes a payment reversal approval message. At step 38, the merchant receives the approval message from the gate way. Further, upon the payment reversal request approval, the merchant displays the order confirmation page with the payment reversal status to the user (step 39). As a result, the live merchant platform 103 may be able to test a range of online payment transaction experiences across issuers using the data collected in the authorization flow and payment reversal flow. Also, the live merchant platform may be able to test end-to-end seller proposition experiences without merchant involvement.

General computer system:

[0035] **FIG. 3** illustrates a block diagram of an exemplary payment processor system for implementing embodiments consistent with the present disclosure.

[0036] In an embodiment, **FIG. 3** illustrates a block diagram of an exemplary payment processor system 300 that may be used to implement the system. In some embodiments, the payment processor system 300 is used to operate the live merchant platform 103 for testing payment transaction experiences. In some embodiments, the payment processor system 300

may include a central processing unit ("CPU" or "processor") 302. The processor 302 may include at least one data processor for executing processes in Virtual Storage Area Network. The processor 302 may include at least one data processor for executing program components for executing user or system-generated business processes. A user may include a person, a person using a device such as those included in this disclosure, or such a device itself. The processor 302 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.

[0037] The processor 302 may be disposed in communication with one or more Input/Output (I/O) devices (312 and 313) via I/O interface 301. The I/O interface 301 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, Bbayonet 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.

[0038] Using the I/O interface 301, the payment processor system 300 may communicate with one or more I/O devices such as input devices 312 and output devices 313. For example, the input devices 312 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 313 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.

[0039] In some embodiments, the processor 302 may be disposed in communication with a communication network 309 via a network interface 303. The network interface 303 may communicate with the communication network 309. The network interface 303 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 309 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 303 and the communication network 309, the payment processor system 300 may communicate with a database 314, which may be the enrolled templates database 313. The network interface 303 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.

[0040] The communication network 309 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 309 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, communication network 309 may include a variety of network devices, including routers, bridges, servers, computing devices, storage devices, etc.

[0041] In some embodiments, the processor 302 may be disposed of in communication with a memory 305 (e.g., RAM, ROM, etc. not shown in **FIG. 3**) via a storage interface 304. The storage interface 304 may connect to memory 305 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. Memory 305 may store a collection of program or database components, including, without limitation, user interface 306, an operating system 307, a web browser 308 etc. In some embodiments, payment processor system 300 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.

[0042] The operating system 307 may facilitate resource management and operation of the payment processor system 300. 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 306 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 payment processor system 300, 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.

[0043] In some embodiments, the payment processor system 300 may implement web browser 308 stored program components. Web browser 308 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 308 may utilize facilities such as AJAX, DHTML, Adobe™ Flash, Javascript, Application Programming Interfaces (APIs), etc. In some embodiments, the payment processor system 300 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.

[0044] In some embodiments, the payment processor system 300 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.

[0045] 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.

[0046] 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.).

[0047] 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.

[0048] 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.

[0049] 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.

[0050] 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 the sake of clarity.

“LIVE MERCHANT ENVIRONMENT”

ABSTRACT

The present disclosure provides a system and a method for operating a live merchant platform. The disclosure proposes using a live merchant platform, associated with a merchant and an acquirer, to test a range of payment experiences across issuers. The live merchant platform is utilized for authenticating cardholder details and authorizing payment details. The live merchant platform sends an authentication request message to an issuer via a payment network. Thereafter, the request message is forwarded to the core processing environment from a security protocol environment via a gateway environment. Further, the live merchant platform receives authenticated response from an issuer environment via the payment network.

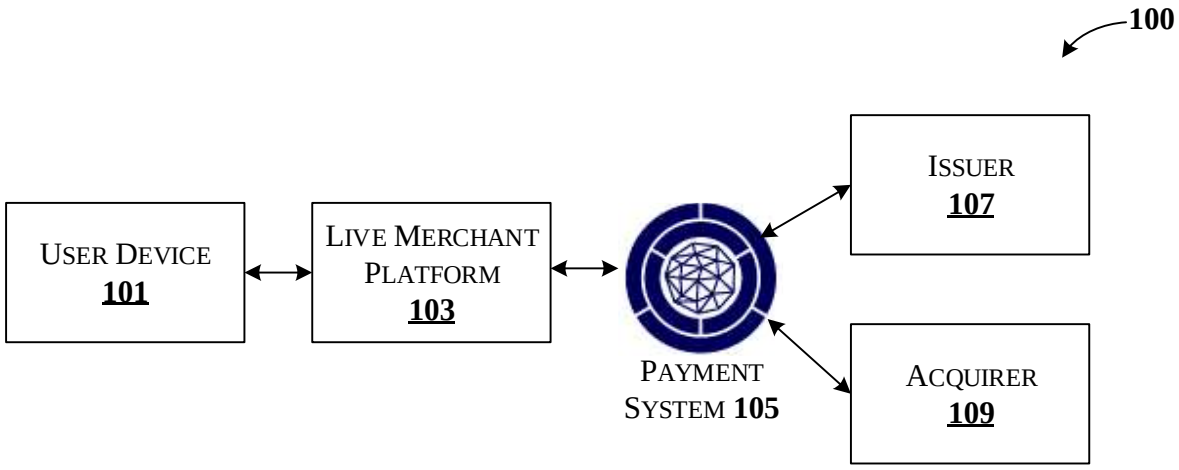
100
USER DEVICE
101
LIVE MERCHANT PLATFORM
103
PAYMENT SYSTEM 105
ISSUER
107
ACQUIRER
109

FIG. 1

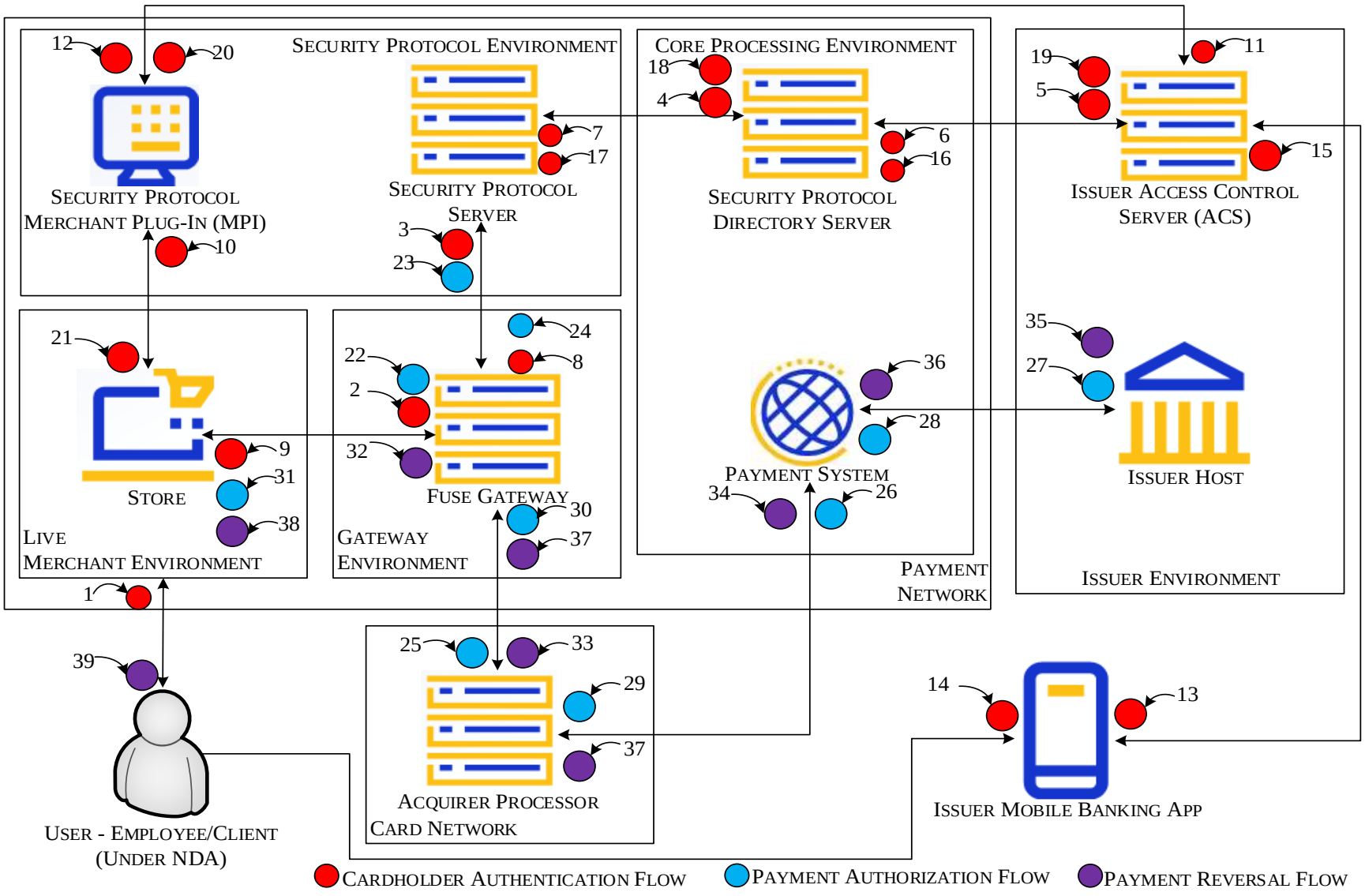
SECURITY PROTOCOL ENVIRONMENT
CORE PROCESSING ENVIRONMENT
SECURITY PROTOCOL MERCHANT PLUG-IN (MPI)
SECURITY PROTOCOL SERVER
SECURITY PROTOCOL DIRECTORY SERVER
ISSUER ACCESS CONTROL SERVER (ACS)
STORE
LIVE MERCHANT ENVIRONMENT
FUSE GATEWAY
GATEWAY ENVIRONMENT
PAYMENT SYSTEM
ISSUER HOST
PAYMENT NETWORK
ISSUER ENVIRONMENT
USER - EMPLOYEE/CLIENT (UNDER NDA)
ACQUIRER PROCESSOR CARD NETWORK
ISSUER MOBILE BANKING APP
CARDHOLDER AUTHENTICATION FLOW
PAYMENT AUTHORIZATION FLOW
PAYMENT REVERSAL FLOW

FIG. 2A

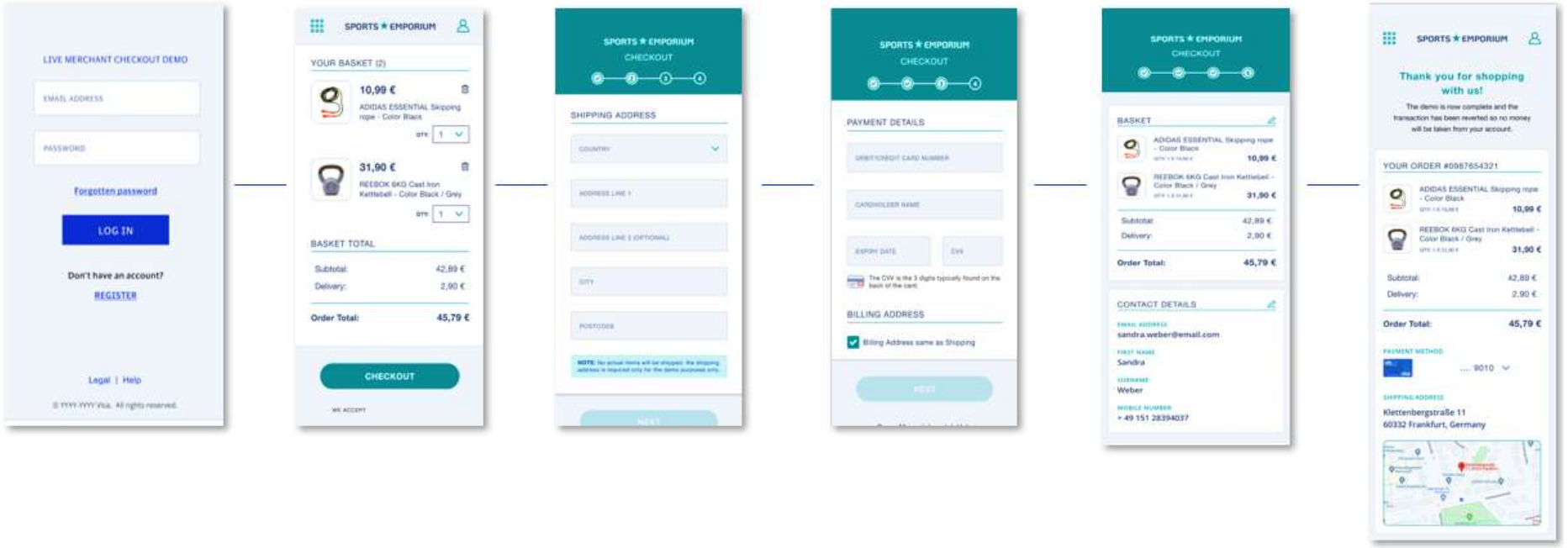
LIVE MERCHANT CHECKOUT DEMO
EMAIL ADDRESS
PASSWORD
Forgotten password
LOG IN
Don't have an account?
REGISTER
Legal | Help
SPORTS ★ EMPORIUM
YOUR BASKET (2)
10,99 €
ADIDAS ESSENTIAL Skipping rope - Color Black
31,90 €
REEBOK 6KG Cast Iron Kettlebell - Color Black / Grey
BASKET TOTAL
Subtotal: 42,89 €
Delivery: 2,90 €
Order Total: 45,79 €
CHECKOUT
SPORTS ★ EMPORIUM
CHECKOUT
SHIPPING ADDRESS
SPORTS ★ EMPORIUM
CHECKOUT
PAYMENT DETAILS
BILLING ADDRESS
Billing Address same as Shipping
SPORTS ★ EMPORIUM
CHECKOUT
BASKET
Subtotal: 42,89 €
Delivery: 2,90 €
Order Total: 45,79 €
CONTACT DETAILS
sandra.weber@email.com
Sandra
Weber
+ 49 151 28394037
SPORTS ★ EMPORIUM
Thank you for shopping with us!
YOUR ORDER #09876543321
Subtotal: 42,89 €
Delivery: 2,90 €
Order Total: 45,79 €
Klettenbergstraße 11
60332 Frankfurt, Germany

FIG. 2B

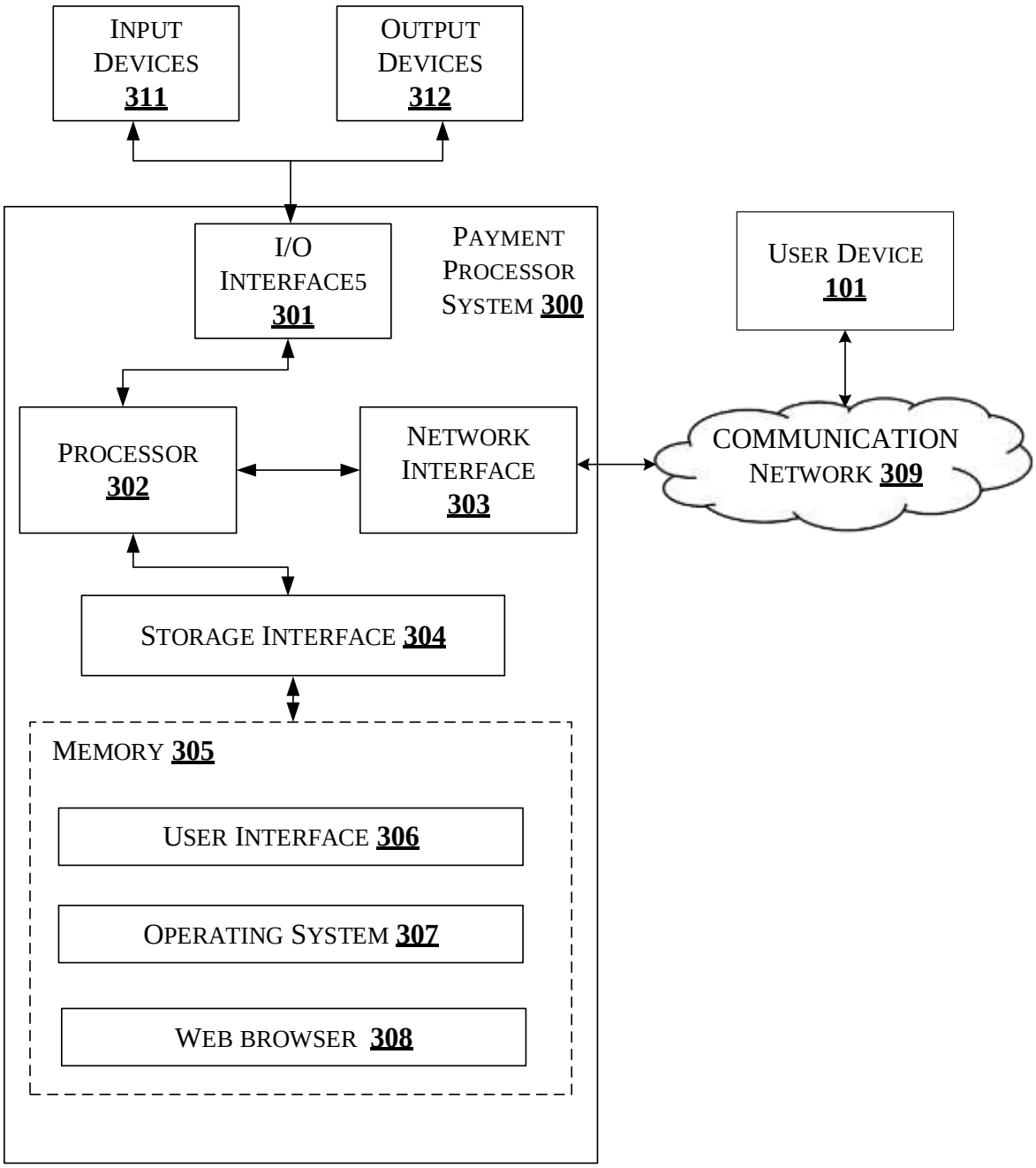
INPUT DEVICES 311
OUTPUT DEVICES 312
I/O INTERFACE5 301
PAYMENT PROCESSOR SYSTEM 300
USER DEVICE 101
PROCESSOR 302
NETWORK INTERFACE 303
COMMUNICATION NETWORK 309
STORAGE INTERFACE 304
MEMORY 305
USER INTERFACE 306
OPERATING SYSTEM 307
WEB BROWSER 308

FIG. 3