December 2022

TOKENIZATION TICKET MASTER

Christopher O'Kane
Visa

Patrick Hutchinson
Visa

TITLE: “TOKENIZATION TICKET MASTER”

VISA

Christopher O'Kane

Patrick Hutchinson

TECHNICAL FIELD

[0001] This disclosure relates generally to the field data security. More particularly, the present disclosure relates to a system and method for authentication using a QR code.

BACKGROUND

[0002] With increase in technology, many people use mobile wallets for several purposes such as make-in-store payments, online purchases, pay for digital content and so on. The mobile wallet is a virtual wallet that stores the payment card information on mobile devices of the user. The mobile wallets are a convenient way for the users make in-store payments and can be used at merchants listed with the mobile wallet service provider. Before using the mobile wallets, the user has to initially add the various details in the application to perform further financial transactions. The user may add the details manually by typing the various details such as Personal Account Number (PAN) and the expiry date of card, ID details, medical details and the like. These techniques of adding the details can lead to higher level of frauds, where the fraudsters may download the provisioned credentials and provision these details to the digital wallets. Also, these techniques of entering the details are clunky process for the consumers to manually enter the details or taking a photo. Thus, there is a need for an efficient and a secure way of provisioning the details of the user. Also, there is need for the efficient and secure way for storing the credentials.

[0003] Further, in events such as conferences, conventions etc. there are various sub-events that may require additional authorization or payment at each sub-event. In the existing technology, there is no one common mode of authorization and payment that maybe used at all authorization checkpoints and payment points. Therefore there is a need for an efficient way of solving one or more of the above mentioned problems.

SUMMARY:

The proposed solution enables an event server to post sensitive details to a tokenization service that will return a token ID to represent the sensitive details. The event server will then encode the token ID in a form of QR code and is presented to the consumer. The consumer may use the QR code at various services at the event.

BRIEF DESCRIPTION OF THE DRAWINGS AND APPENDICES

[0004] The features and characteristics of the present invention, as well as the methods of operation and functions of the related elements of structures and the combination of parts and economies of manufacture, will become more apparent upon consideration of the following description and the appended claims with reference to the accompanying drawings, all of which form a part of this specification, wherein like reference numerals designate corresponding parts in the various figures. It is to be expressly understood, however, that the drawings are for the purpose of illustration and description only and are not intended as a definition of the limits of the invention. As used in the specification, the singular form of “a,” “an,” and “the” include plural referents unless the context clearly dictates otherwise.

[0005] Additional advantages and details of non-limiting embodiments are explained in greater detail below with reference to the exemplary embodiments that are illustrated in the accompanying schematic figures, in which:

[0006] Fig. 1 discloses a schematic diagram of a system and overlying process flow generating a tokenized QR code encoding sensitive details of consumer.

[0007] Fig. 2 discloses a schematic diagram of a system and overlying process flow for a consumer using a tokenized QR code encoding sensitive details at an event.

[0008] FIG. 3 is a block diagram of an exemplary computer system for implementing embodiments consistent with the present disclosure.

DESCRIPTION OF THE DISCLOSURE

[0009] 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.

[0010] 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.

[0011] 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.

[0012] 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.

[0013] The terms "including", "comprising", “having” and variations thereof mean "including but not limited to", unless expressly specified otherwise.

[0014] As used herein, the terms “communication”, “communicate”, “post”, “sent”, “return” and “returned” 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 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".

[0016] 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., 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, net books, 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).

[0017] As used herein, the term "user device" may refer to a device that is operated by a user. An example of a "user device" may be a "payment device.”,

[0018] As used herein, the term "payment device" may refer to any suitable device that may be used to conduct a financial transaction, such as to provide payment credentials to a merchant. The payment device may be a software object, a hardware object, or a physical object. As examples of physical objects, the payment device may comprise a substrate such as a paper or plastic card, and information that is printed, embossed, encoded, or otherwise included at or near a surface of an object. A hardware object can relate to circuitry (e.g., permanent voltage values), and a software object can relate to non-permanent data stored on a device. A payment device may be associated with a value such as a monetary value, a discount, or store credit, and a payment device may be associated with an entity such as a bank, a merchant, a payment processing network, or a person. A payment device may be used to make a payment transaction. Suitable payment devices can be hand-held and compact so that they can fit into a user's wallet and/or pocket (e.g., pocket-sized). Example payment devices may include smart cards, magnetic stripe cards, keychain devices (such as the Speedpass ^{TM} commercially available from Exxon-Mobil Corp.), etc. Other examples of mobile devices include pagers, payment cards, security cards, access cards, smart media, transponders, and the like. If the payment device is in the form of a debit, credit, or smartcard, the payment device may also optionally have features such as magnetic stripes. Such devices can operate in either a contact or contactless mode. In some embodiments, a mobile device can function as a payment device (e.g., a mobile device can store and be able to transmit payment credentials for a transaction).

[0019] As used herein, the term "credential" may refer to any suitable information that serves as reliable evidence of worth, ownership, identity, or authority. An "access credential" may be a credential that may be used to gain access to a particular resource (e.g., a good, service, location, etc.). A credential may be a string of numbers, letters, or any other suitable characters, or any object or document that can serve as confirmation. Examples of credentials include identification cards, certified documents, access cards, passcodes and other login information, payment account numbers, access badge numbers, payment tokens, etc.

[0020] As used herein, the term "Payment credentials" may refer to any suitable information associated with an account (e.g. a payment account and/or payment device associated with the account). Such information may be directly related to the account or may be derived from information related to the account. Examples of account information may include a PAN (primary account number or "account number"), username, expiration date, CVV (card verification value), DCVV (dynamic card verification value), CVV2 (card verification value 2), CVC3 card verification values, etc. Payment credentials may be any information that identifies or is associated with a payment account. Payment credentials may be provided in order to make a payment from a payment account. Payment credentials can also include a user name, an expiration date, a gift card number or code, and any other suitable information.

[0021] As used herein, the term "token" may refer to a substitute value for a real credential. A token may be a type of credential, and may be a string of numbers, letters, or any other suitable characters. Examples of tokens include payment tokens, personal identification tokens, etc.

[0022] As used herein, the term "Tokenization" is a process by which data is replaced with substitute data. For example, a payment account identifier (e.g., a primary account number (PAN)) may be tokenized by replacing the primary account identifier with a substitute number (e.g. a token) that may be associated with the payment account identifier. Further, tokenization may be applied to any other information that may be replaced with a substitute value (i.e., token). Tokenization may be used to enhance transaction efficiency, improve transaction security, increase service transparency, or to provide a method for third party enablement.

[0023] As used herein, the term "consumer" may include an individual. In some embodiments, a consumer may be associated with one or more personal accounts and/or mobile devices.

[0024] As used herein, the term "authorizing entity" may be an entity that authorizes a request. Examples of an authorizing entity may be an issuer, a governmental agency, a document repository, an access administrator, etc. An "issuer" may typically refer to a business entity (e.g., a bank) that maintains an account for a user. An issuer may also issue payment credentials stored on a user device, such as a cellular telephone, smart card, tablet, or laptop to the consumer. An authorizing entity may operate an authorizing computer.

[0025] As used herein, the term "authorization-sale point" may be any suitable device that provides access to a remote system. An authorization-sale point may also be used for communicating with a merchant computer, a transaction processing computer, an authentication computer, or any other suitable system. An authorization-sale point may generally be located in any suitable location, such as at the location of a merchant. An authorization-sale point may be in any suitable form. Some examples of authorization-sale points include POS or point of sale devices (e.g., POS terminals), cellular phones, PDAs, personal computers (PCs), tablet PCs, hand-held specialized readers, set-top boxes, electronic cash registers (ECRs), automated teller machines (ATMs), virtual cash registers (VCRs), kiosks, security systems, access systems, and the like. An authorization-sale point may use any suitable contact or contactless mode of operation to send or receive data from, or associated with, a user mobile device. In some embodiments, where an authorization-sale point may comprise a POS terminal, any suitable POS terminal may be used and may include a reader, a processor, and a computer-readable medium. A reader may include any suitable contact or contactless mode of operation. For example, exemplary card readers can include radio frequency (RF) antennas, optical scanners, bar code readers, or magnetic stripe readers to interact with a payment device and/or mobile device. In some embodiments, a cellular phone, tablet, or other dedicated wireless device used as a POS terminal may be referred to as a mobile point of sale or an "mPOS" terminal.

[0026] As used herein, the term "tokenization server" and “event server” are typically a powerful computer or cluster of computers. For example, the server computer can be a large mainframe, a minicomputer cluster, or a group of servers functioning as a unit. In one example, the server computer may be a database server coupled to a Web server.

[0027] As used herein, the term "processor" may refer to any suitable data computation device or devices. A processor may comprise one or more microprocessors working together to accomplish a desired function. The processor may include CPU comprises at least one high-speed data processor adequate to execute program components for executing user and/or system-generated requests. The CPU may be a microprocessor such as AMD's Athlon, Duron and/or Opteron; IBM and/or Motorola's PowerPC; IBM's and Sony's Cell processor; Intel's Celeron, Itanium, Pentium, Xeon, and/or XScale; and/or the like processor(s).

[0028] As used herein, the term "memory" may be any suitable device or devices that can store electronic data. A suitable memory may comprise a non-transitory computer readable medium that stores instructions that can be executed by a processor to implement a desired method. Examples of memories may comprise one or more memory chips, disk drives, etc. Such memories may operate using any suitable electrical, optical, and/or magnetic mode of operation.

[0029] It will be apparent that systems and/or methods, described herein, can be implemented in different forms of hardware, software, or a combination of hardware and software. The actual specialized control hardware or software code used to implement these systems and/or methods is not limiting of the implementations. Thus, the operation and behavior of the systems and/or methods are described herein without reference to specific software code, it being understood that software and hardware can be designed to implement the systems and/or methods based on the description herein.

[0030] Fig. 1 discloses a schematic diagram of a system and overlying process flow for generating a tokenized QR code encoding consumer sensitive data.

[0031] In FIG. 1, a schematic diagram of a system 100 shows a consumer 101, a user device 102, an event server 103, a tokenization server 104 and a QR printer 105. The consumer 101 enters sensitive data into the event checkout page which is displayed/presented on the user device 102. The event checkout page presented/displayed on the user device 102 posts the sensitive data to the event server 103. The sensitive data is then sent to the tokenization server 104, where the data is securely stored, and a token is created to represent the sensitive data. A token ID is returned to the event server 103 and the token ID is encoded as a QR code. The token may be generated using, but not limited to Universally Unique Identifier (UUID). The event server and the tokenization server may interact via Application Program Interface (API). In one embodiment, the QR code is displayed to the consumer 101 on a receipt page on the user device 102. The consumer 101 may print the QR code with the QR printer 105 or may save the QR code as a digital file in the user device 102. In an embodiment, known techniques can be used to generate the QR code.

[0032] In an embodiment the sensitive data may include, but is not limited to the consumer’s 101 name, date of birth (DOB), billing information, shipping information, personal photo, medical information, emergency contacts, payment details.

[0033] In another emodiment the consumer 101 may store/capture the QR code displayed on the receipt page of the user device 102 in another mobile user device 106 which may be, but is not limited to, a smartphone, a tablet, a smart watch. The consmer 101 may then use the QR code stored on the mobile user device 106 for easy access at various entry points or point of sale at the event.

[0034] Fig. 2 discloses a schematic diagram of a system and overlying process flow for a consumer using tokenized QR code at an event.

[0035] In FIG. 2, a schematic diagram of a system 200 shows a consumer 101, a sub-event 201, an authorization-sale point 202, the event server 103, the tokenization server 104 and a payment processor 203. The consumer 101 enters the sub-event 201 that may be an event that only admits certain authorized consumers. This type of sub-event 201 may be, but is not limited to, an event that only consumers of a certain age can enter (for e.g. it may be allowed only for consumers who are over the age of eighteen or over the age of twenty one to enter (e.g. bars)), an event that is unsuitable for consumers with certain medical conditions (which may further be for example, but is not limited to, pregnant women, consumer's with heart conditions, people who are not of a certain weight or height for sub-events which my be rides). The consumer's 101 QR code is scanned at the authorization-sale point 202. The authorization-sale point 202 decodes the QR code and sends the token ID to the event server 103. The event server 103 calls the tokenization server 104 to retrieve the sensitive information associated with the token. The tokenization server 104 returns the name, photo and other sensitive information of the consumer 101 stored in the token. The event server 103 returns this information for display on the authorization-sale point 202 and it validates if the consumer is authorized to enter the particular sub-event 201 and the person of authority present at the authorization-sale point 202 also verifies the consumer by cross checking if the person in the photo and the consumer 101 are one and the same. Once the validation is positive, then the consumer 101 may be granted entry.

[0036] In another embodiment, the sub-event 201 may require payment (which may be, but is not limited to, a food stand, bar, other merchandise, paraphernalia etc.). In that case, after the event server 103 calls the tokenization server 104 to retrieve the sensitive information associated with the token, the tokenization server 104 may return the name along with payment information and other sensitive information associated with the consumer 101 stored in the token. The event server 103 returns this information for display on the authorization-sale point

202, and it validates if the consumer is authorized to receive the sub-event's 201 service or product. Once the validation is positive, the payment credentials may be passed to the payment processor. The payment processor 203 may approve the transaction. The person of authority may give the consumer 101 the service or product that may have been paid for.

[0037] FIG. 3 is a block diagram of an exemplary computer system for implementing embodiments consistent with the present disclosure.

[0038] In some embodiments, FIG. 3 illustrates a block diagram of an exemplary computer system 300 for implementing embodiments consistent with the present disclosure. In some embodiments, the computer system 300 may be a user device 102 or an authorization-sale point 202. The processor 302 may include at least one data processor for executing program components for executing user or system-generated business processes. A consumer 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.

[0039] The processor 302 may be disposed in communication with input devices 311 and output devices 312 via I/O interface 301. The I/O interface 301 may employ communication protocols/methods such as, without limitation, audio, analog, digital, stereo, IEEE-1393, serial bus, Universal Serial Bus (USB), infrared, PS/2, BNC, coaxial, component, composite, Digital Visual Interface (DVI), high-definition multimedia interface (HDMI), Radio Frequency (RF) antennas, S-Video, Video Graphics Array (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.

[0040] Using the I/O interface 301, the computer system 300 may communicate with the input devices 311 and the output devices 312.

[0041] 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. Using the network interface 303 and the communication network 209, the computer system 300 may communicate with an event server 103. The event server 103 in-turn communicates with the tokenization server 104. The communication network 309 can be implemented as one of the different types of networks, such as intranet or Local Area Network (LAN), Closed Area Network (CAN) 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), CAN Protocol, Transmission Control Protocol/Internet Protocol (TCP/IP), Wireless Application Protocol (WAP), etc., to communicate with each other. Further, the communication network 309 may include a variety of network devices, including routers, bridges, servers, computing devices, storage devices, etc. In some embodiments, the processor 302 may be disposed in communication with a memory 305 (e.g., RAM, ROM, etc. not shown in FIG.3) via a storage interface 303. The storage interface 303 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-1393, Universal Serial Bus (USB), fibre 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.

[0042] The memory 305 may store a collection of program or database components, including, without limitation, a user interface 306, an operating system 307, a web browser 308 etc. In some embodiments, the computer system 300 may store consumer/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.

[0043] The operating system 307 may facilitate resource management and operation of the computer system 200. Examples of operating systems include, without limitation, APPLE® MACINTOSH® OS X®, UNIX®, UNIX-like system distributions (E.G., BERKELEY SOFTWARE DISTRIBUTION® (BSD), FREEBSD®, NETBSD®, OPENBSD, etc.), LINUX® DISTRIBUTIONS (E.G., RED HAT®, UBUNTU®, KUBUNTU®, etc.), IBM®OS/2®, MICROSOFT® WINDOWS® (XP®, VISTA®/7/8, 10 etc.), APPLE® IOS®, GOOGLE™

ANDROID^{TM}, BLACKBERRY® OS, or the like. The User interface 206 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 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.

[0044] In some embodiments, the computer system 300 may implement the web browser 308 stored program components. The web browser 308 may be a hypertext viewing application, such as MICROSOFT® INTERNET EXPLORER®, GOOGLE^{TM} CHROME^{TM}, 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®, JAVA®, Application Programming Interfaces (APIs), etc. In some embodiments, the computer 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 Active Server Pages (ASP), ACTIVEX®, ANSI® C++/C#, MICROSOFT®, .NET, 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. In some embodiments, the computer 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., non-transitory. Examples include Random Access Memory (RAM), Read-Only Memory (ROM), volatile memory, non-volatile memory, hard drives, Compact Disc (CD) ROMs, Digital Video Disc (DVDs), flash drives, disks, and any other known physical storage media.

[0046] 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.

[0047] 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.

[0048] Any of the software components or functions described in this application, may be implemented as software code to be executed by a processor using any suitable computer language such as, for example, Java, C++ or Perl using, for example, conventional or object-oriented techniques. The software code may be stored as a series of instructions, or commands on a computer readable medium, such as a random access memory (RAM), a read only memory (ROM), a magnetic medium such as a hard-drive or a floppy disk, or an optical medium such as a CD-ROM. Any such computer readable medium may reside on or within a single computational apparatus, and may be present on or within different computational apparatuses within a system or network.

[0049] The above description is illustrative and is not restrictive. Many variations of the invention may become apparent to those skilled in the art upon review of the disclosure. The scope of the invention can, therefore, be determined not with reference to the above description, but instead can be determined with reference to the pending claims along with their full scope or equivalents.

[0050] One or more features from any embodiment may be combined with one or more features of any other embodiment without departing from the scope of the invention.

[0051] A recitation of "a", "an" or "the" is intended to mean "one or more" unless specifically indicated to the contrary.

[0052] Although the invention has been described in detail for the purpose of illustration based on what is currently considered to be the most practical and preferred embodiments, it is to be understood that such detail is solely for that purpose and that the invention is not limited to the disclosed embodiments, but, on the contrary, is intended to cover modifications and equivalent arrangements that are within the spirit and scope of the appended claims. For example, it is to be understood that the present invention contemplates that, to the extent possible, one or more features of any embodiment can be combined with one or more features of any other embodiment.

ABSTRACT

The present invention discloses a tokenization ticket master system where in which a consumer 101 enters sensitive data into an event checkout page which is displayed/presented on a user device 102. The event checkout page presented/displayed on the user device 102 posts the sensitive data to an event server 103. The sensitive data is then sent to a tokenization server 104, where the data is securely stored, and a token is created to represent the sensitive data. A token ID is returned to the event server 103 and the token ID is encoded as a QR code. The token may be generated using, but not limited to Universally Unique Identifier (UUID). The event server and the tokenization server may interact via Application Program Interface (API). In one embodiment, the QR code is displayed to the consumer 101 on a receipt page on the user device 102. The consumer 101 may print the QR code with a QR printer 105 or may save the QR code as a digital file in the user device 102. In an embodiment, known techniques can be used to generate the QR code.

FIG. 1

1/3

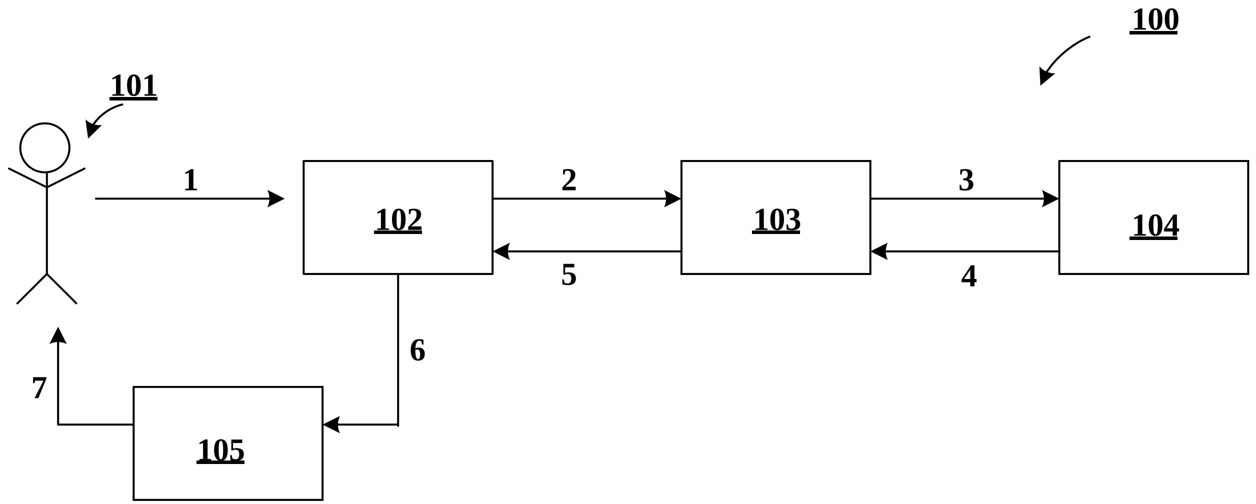

Fig. 1

2/3

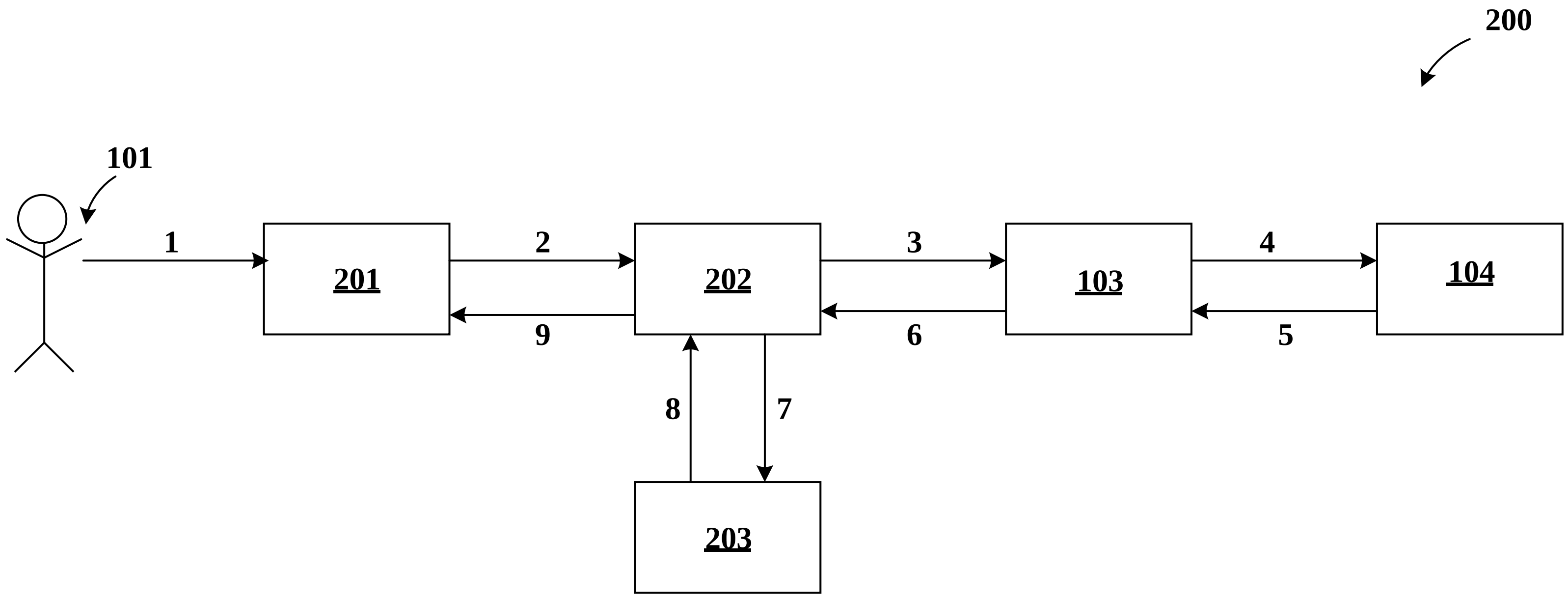

Fig. 2

3/3

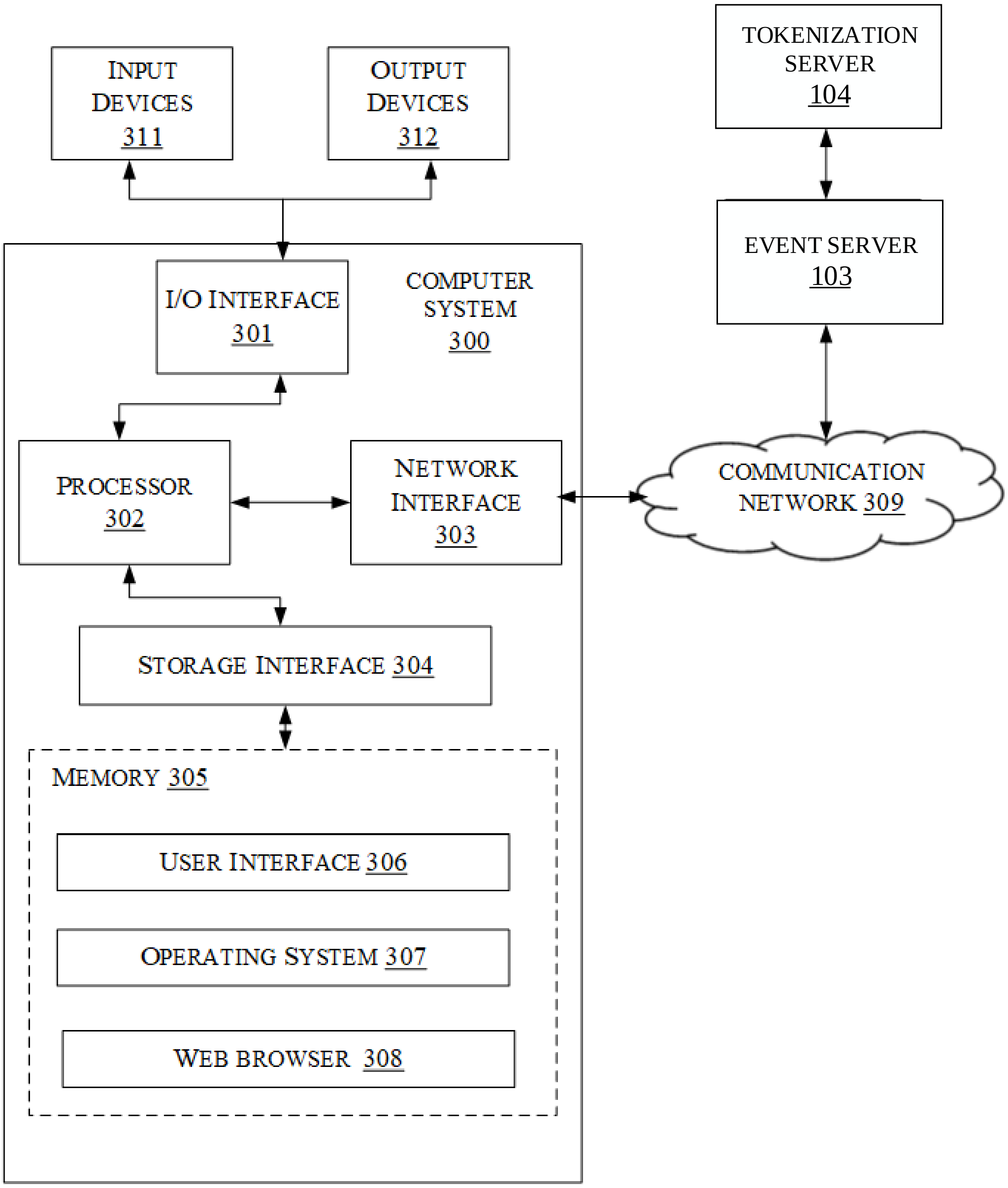
INPUT DEVICES 311
OUTPUT DEVICES 312
TOKENIZATION SERVER 104
EVENT SERVER 103
I/O INTERFACE 301
COMPUTER SYSTEM 300
PROCESSOR 302
NETWORK INTERFACE 303
COMMUNICATION NETWORK 309
STORAGE INTERFACE 304
MEMORY 305
USER INTERFACE 306
OPERATING SYSTEM 307
WEB BROWSER 308

Fig. 3

1/3

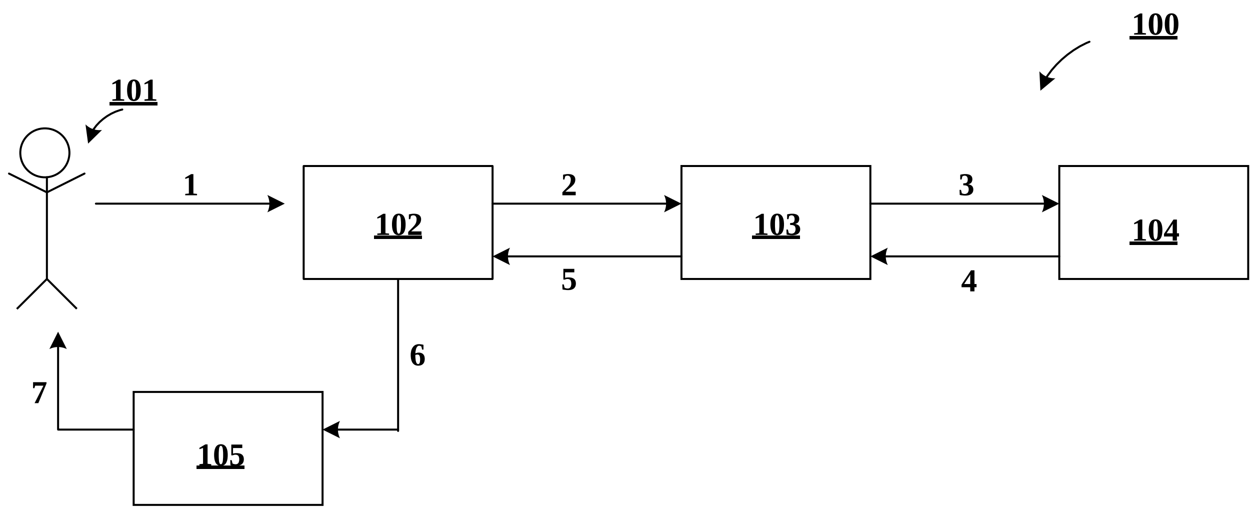

Fig. 1

2/3

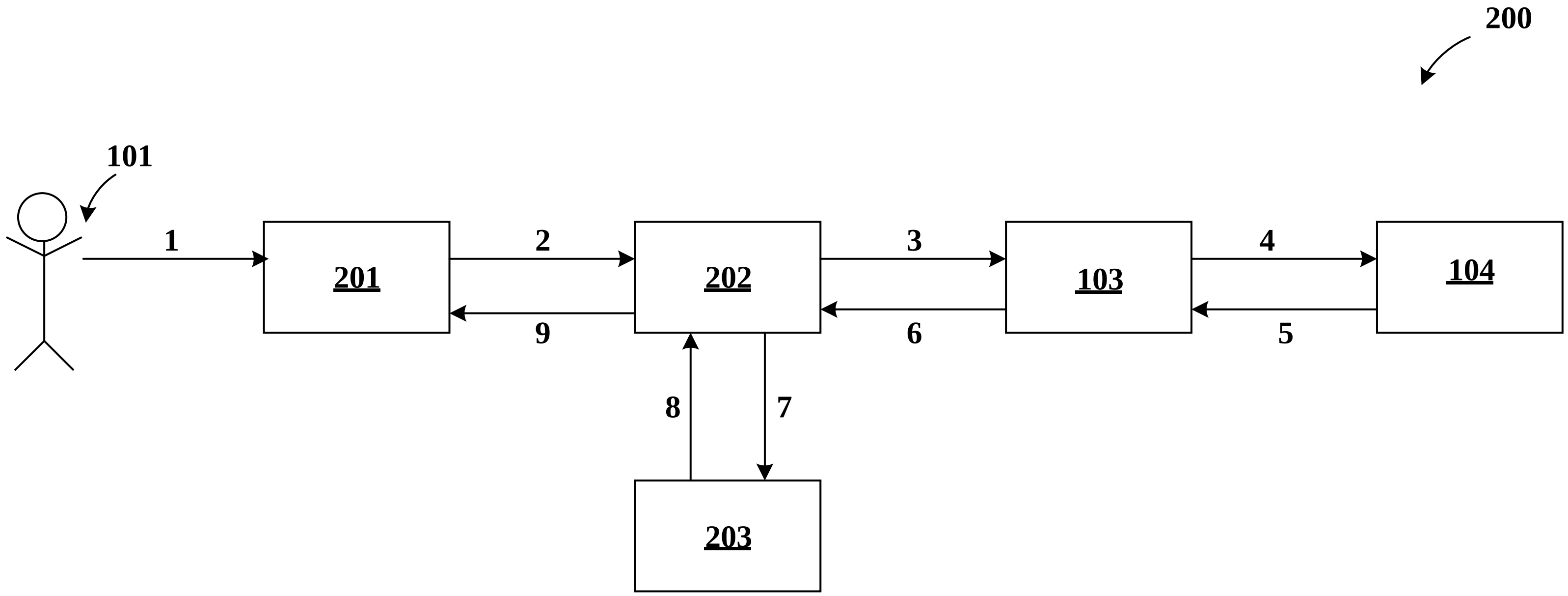

Fig. 2

3/3

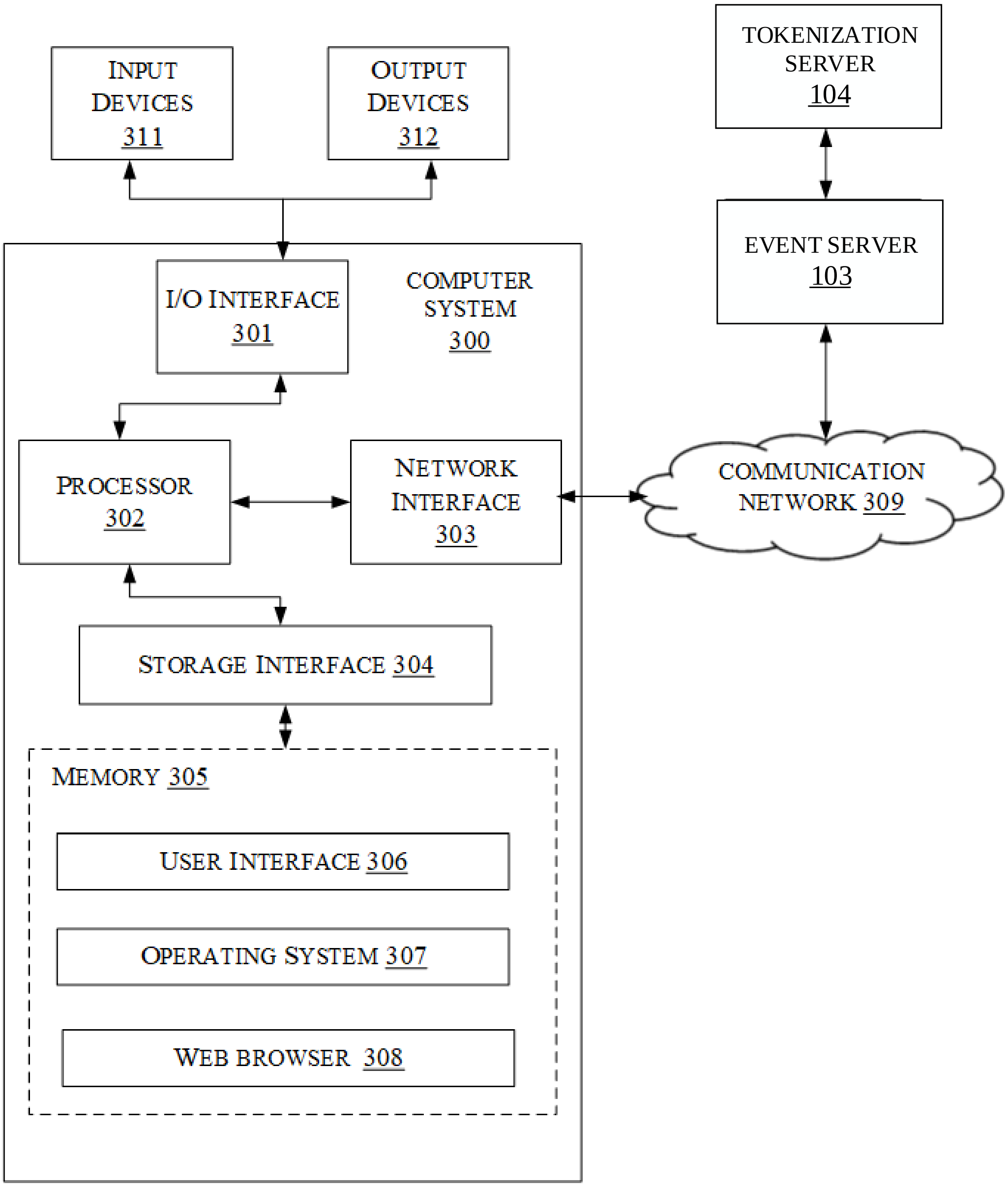
INPUT DEVICES 311
OUTPUT DEVICES 312
TOKENIZATION SERVER 104
EVENT SERVER 103
I/O INTERFACE 301
COMPUTER SYSTEM 300
PROCESSOR 302
NETWORK INTERFACE 303
COMMUNICATION NETWORK 309
STORAGE INTERFACE 304
MEMORY 305
USER INTERFACE 306
OPERATING SYSTEM 307
WEB BROWSER 308

Fig. 3