November 2022

BUMP TO INITIATE AUTHENTICATION BASED TOKEN ON A MOVING DEVICE

Wilson Thampi
Visa

Tony Kollamparambil
Visa

BUMP TO INITIATE AUTHENTICATION BASED TOKEN ON A MOVING DEVICE

VISA

Inventors:

Wilson Thampi

Tony Kollamparambil

TECHNICAL FIELD

[001] The present disclosure relates generally for token-based authentication, and more particularly discloses bump to initiate authentication-based token on a moving device.

BACKGROUND

[002] Authentication is helpful in a variety of situations, such as e-commerce transactions, secure system access, etc. In general, authentication technologies are used to confirm a user's identity before granting them access to functions, such as viewing confidential data or carrying out approved transactions.

[003] Identity theft crimes, like credit card fraud, are on the rise because of the increased usage of credit and debit cards. To provide sufficient authentication, a user may be required to provide additional information during the card approval process, such as specific numbers printed on the back of the card, the postal code for the billing address associated with the card, a primary account number (PAN), or a personal identification number (PIN) associated with the card. Such information may be ineffective because it is stagnant. Using token-based authentication could help to solve these issues. However, there aren't any systems or methods for starting token on mobile device while making drive-through payments.

[004] There is a need of systems and methods for initiating the token on credit on a mobile device by bumping on a moving vehicle dashboard without disclosing PAN.

[005] The information disclosed in this background of the disclosure section is only for enhancement of understanding of the general background of the invention and should not be

taken as an acknowledgement or any form of suggestion that this information forms the prior art already known to a person skilled in the art.

SUMMARY

[006] The objective of the present invention is to employ the second device for propagating to the loyalty model to allow a user to access a temporary card token without disclosing primary account number (PAN) information. When used by other members of the cardholder's family, a first device is pre-registered with the software development kit (SDK) of the user's payment network provider for authorization tokens without disclosing card information. In addition, if a token is bumped on the dashboard of the first device, a token of low value might be sent to the second device based on the consolidated loyalty score of the devices. A silent push message sent by the payment network provider is forwarded by the issuer to the second device. An instant token of the specified amount is generated on the second device after it has verified the push message's authenticity. Utilizing the identity data from the second device, the issuer will bill the customer for the transaction. By using the second device, a cardholder can access a temporary card token without sharing their PAN.

[007] The foregoing summary is illustrative only and is not intended to be in any way limiting. In addition to the illustrative aspects, embodiments, and features described above, further aspects, embodiments, and features will become apparent by reference to the drawings and the following detailed description.

BRIEF DESCRIPTION OF THE DRAWINGS

[0010] The example embodiment(s) of the present invention are illustrated by way of example, and not in way by limitation, in the figures of the accompanying drawings and in which like reference numerals refer to similar elements and in which:

[008] Figures 1 depicts environmental diagram for authenticating devices initiated by bump, in accordance with an embodiment of the present disclosure;

[009] Figure 2 illustrates a flow diagram for authenticating devices initiated by bump, in accordance with an embodiment of the present disclosure;

[0010] Figure 3 illustrates an exemplary block diagram of a computer apparatus in accordance with an embodiment;

[0011] It should be appreciated by those skilled in the art that any block diagrams herein represent conceptual views of illustrative systems embodying the principles of the present subject matter. Similarly, it will be appreciated that any flow charts, flow diagrams, state transition diagrams, pseudo code, and the like represent various processes which may be substantially represented in computer readable medium and executed by a computer or processor, whether or not such computer or processor is explicitly shown. While each of the figures illustrates a particular embodiment for purposes of illustrating a clear example, other embodiments may omit, add to, reorder, and/or modify any of the elements shown in the figures.

DETAILED DESCRIPTION

[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 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 system or apparatus proceeded by “comprises… a” does not, without more constraints, preclude the existence of other elements or additional elements in the system or apparatus.

[0015] Embodiments of the present disclosure relates to tokenisation. In the current domains and/or payment environments, automatic generation of payment tokens is used. Examples include solely for e-commerce, only for a particular merchant or merchants, etc. As a result, tokenized payments are operations in which a token is utilized to carry out a payment transaction rather than the PAN. Because the primary account number (PAN) is not sent during the transaction, tokenized payments are more secure.

[0016] Figure 1 depicts environmental diagram environmental diagram for authenticating devices initiated by bump, in accordance with an embodiment of the present disclosure. The

environment (100) comprises a first device (101), a second device (102). The first device (101) includes a dashboard that is integrated with a user's payment network company's software development kit (SDK). The first device (101) could be a car or another type of vehicle. The user's payment network provider's SDK is likewise included in the second device (102). The second device could be a mobile phone or another form of communication. The first device dashboard bumps the second device (102) for initiating a token. The token is a distinct string of numbers which is a secure identifier created using a the PAN. When it bumps into the first device's dashboard, a token of low value might be sent to the second device (102) based on the first device's (101) consolidated loyalty score (101).

[0017] Additionally, the second device (102) obtains the geolocation via open application programming interfaces (APIs) and transmits device data to the first device (101). REST APIs and SOAP APIs are two examples of Open APIs. The phone numbers of the first device (101) and the second device (102) may be shared using near field communication (NFC) technology to begin the generation of tokens. The second device receives the device ID and phone number from the first device's mobile (101) device (102). An issuer token service verifies the first device (101) for device ID and active range. The financial institution that issues the cardholder's payment cards is known as the Issuer. In addition to calling the issuer SDK included inside the issuer application of the second device (102) and sending information pertinent to cryptogram as well as a shared key for authentication, the first device (101) also sends a device ID request. By ensuring the security and validity of the card, the cryptogram may be used to validate the transaction for the bank. Visa loyalty creates a temporary ID and produces a new risk score based on Device ID, Device Model, and geolocation. A Temporary ID is given to the issuer token services to create a 3D secure Authentication URL for previously registered issuers for the location. A silent push message sent by the payment network provider is forwarded by the

issuer to the second device (102). An instant token of the specified amount is generated on the second device (102) after it has verified the push message's authenticity. Utilizing the identity data from the second device, the issuer will bill the customer for the transaction (102). Therefore, according to the present invention, a user can utilise another device to access a temporary card token without revealing their PAN.

[0018] Reference is now made to Figure 2. The following method describes the steps performed by the first device (101) and the second device (102). Figure 2 illustrates a flow diagram for authenticating devices initiated by bump, in accordance with an embodiment of the present disclosure.

[0019] As illustrated in Figure 2, the method (200) may comprise one or more steps. The method (200) may be described in the general context of computer executable instructions. Generally, computer executable instructions can include routines, programs, objects, components, data structures, procedures, modules, and functions, which perform functions or implement particular abstract data types.

[0020] The order in which the method (200) is described is not intended to be construed as a limitation, and any number of the described method blocks can be combined in any order to implement the method. Additionally, individual blocks may be deleted from the methods without departing from the scope of the subject matter described herein. Furthermore, the method can be implemented in any suitable hardware, software, firmware, or combination thereof.

[0021] The following steps are performed by the first device (101) and the second device (102) to initiate authentication-based token by bumping the second device (102) on the first device (101) dashboard.

[0022] At step 201, the first device (101) dashboard is integrated with SDK for loyalty authentication. Herein, the first device may be the user's car or any other vehicle. The SDK may be of the user's payment network company. The SDK enables the cardholders to easily supply cards to mobile wallets and online retailers through their mobile banking application. Companies reward users with points or rewards through a loyalty program. In exchange, users can use their points to get deals, freebies, incentives, or access to exclusive benefits. In the present disclosure, for example, the automated car with "A" bank is integrated with the SDK of Visa payment network company. The dashboard is connected to a mobile device of the user wherein the device is registered on the issuer application. Further, the device is added to the Visa token services. Firstly, the issuer connects with Visa mobile service to send consolidated loyalty score. For example, the default loyalty score of registered device is maybe 500 points.

[0023] At step 202, the second device (102) is bumped on the first device (101) which is also integrated to SDK of the user's payment network company. Herein, the second device (102) maybe the mobile phone of the user's spouse or child or any other communication means. For example, the user's spouse thinks to order food on a drive through. Then the user's spouse bumps her mobile device on the car dashboard with user's registered device. Furthermore, the issuer application checks whether the second device (102) is bumped for the purpose of token authentication. The user confirms for initiating a token. Furthermore, the registered device of the car fetches the geolocation of the user's spouse mobile and shares the information to the car. Furthermore, the issuer application verifies the geolocation of the car and the user's spouse

mobile are matching. Table 1 illustrates comparing the geolocation of the car and the user's spouse mobile.

Car Data	Mobile
Issuer ID	Android
Timestamp	Samsung X
Location attributes	Location Attributes
Datetime	Datetime

Table 1: Compare Geolocation of the first device and the second device

[0024] At step 203, phone numbers of first device and second device are exchanged for initiating a token using near field communication (NFC) Technology. Table 2 depicts exchanging phone numbers by the devices.

Car Data	Mobile
Issuer ID	Android
Timestamp	Samsung X
Location attributes	Location Attributes
Datetime	Datetime
Mobile number	Mobile number

Table 2: Exchange of Phone numbers of first device and second device

[0025] At step 204, loyalty score of the second device (device ID, Issuer ID) is requested by the first device (101) by calling issuer app integrated SDK. The first device (101) is validated for device ID and active range by an issuer token service. The issuer is the financial institution that issues the payment cards to the cardholder. The first device (101) sends a device ID request, calls the issuer SDK incorporated inside the issuer application of the second device (102), and sends information relevant to cryptogram and a shared key for authentication. The first device (101) and the second device are preconfigured for SDK of the user’s payment network

company. The first device (101) sends a device ID request, calls the issuer SDK incorporated inside the issuer application of the second device (102), and sends information relevant to cryptogram and a shared key for authentication. Table 3 depicts authentication of device by requesting device ID and issuer ID.

Car Data	Validated at Visa
Issuer ID	
Timestamp	Samsung X
Location attributes	Location Attributes
Datetime	Datetime
Mobile Number	Mobile number

Table 3: Authentication of Device

[0026] At step 205, the issuer sends silent push message to the second device (102). The issuer sends the second device (102) a silent push message sent by the payment network company.

[0027] At step 206, the second device authenticates the push message, and an instant token is created on the second device. The second device verifies the push message sent by the issuer. After verifying the push message, the instant token is created. For instance, $20 is created on the user's spouse to make the payment for the drive through purchase.

[0028] At step 207, the user's spouse is billed for the payment using the device identity by the issuer. In this way the customer is billed for the payment while drive through purchase using the device identity. A user can access a temporary card token without disclosing PAN information by utilizing the second device.

[0029] Figure 3 illustrates a block diagram of an exemplary computer system (300) for implementing embodiments consistent with the present disclosure. In an embodiment, the computer system (300) is used to implement the method for authorising transactions in the platform (300). The computer system (300) may comprise a central processing unit ("CPU" or "processor") (302). The processor (302) may comprise at least one data processor for executing program components for dynamic resource allocation at run time. 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.

[0030] The processor (302) may be disposed in communication with one or more input/output (I/O) devices (not shown) via I/O interface (301). The I/O interface (301) may employ communication protocols/methods such as, without limitation, audio, analog, digital, monoaural, RCA, stereo, IEEE-1394, serial bus, universal serial bus (USB), infrared, PS/2, BNC, coaxial, component, composite, digital visual interface (DVI), high-definition multimedia interface (HDMI), RF antennas, S-Video, VGA, IEEE 802.n /b/g/n/x, Bluetooth, cellular (e.g., code-division multiple access (CDMA), high-speed packet access (HSPA+), global system for mobile communications (GSM), long-term evolution (LTE), WiMax, or the like), etc.

[0031] Using the I/O interface (301), the computer system (300) may communicate with one or more I/O devices. For example, the input device (310) may be an antenna, keyboard, mouse, joystick, (infrared) remote control, camera, card reader, fax machine, dongle, biometric reader, microphone, touch screen, touchpad, trackball, stylus, scanner, storage device, transceiver, video device/source, etc. The output device (311) 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.

[0032] In some embodiments, the computer system (300) is connected to the service operator through a communication network (309). The processor (302) may be disposed in communication with the 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, e-commerce network, a peer to peer (P2P) network, local area network (LAN), wide area network (WAN), wireless network (e.g., using Wireless Application Protocol), the Internet, Wi-Fi, etc. Using the network interface (303) and the communication network (309), the computer system 400 may communicate with the one or more service operators.

[0033] In some embodiments, the processor (302) may be disposed in communication with a memory (305) (e.g., RAM, ROM, etc) 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), 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.

[0034] The memory (305) may store a collection of program or database components, including, without limitation, user interface (306), an operating system (307), web server (308) etc. In some embodiments, computer system (300) may store user/application data (306), 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.

[0035] The operating system (307) may facilitate resource management and operation of the computer 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, 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, Blackberry OS, or the like.

[0036] In some embodiments, the computer system (300) may implement a web browser (308) stored program component. The 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, 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 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.

[0037] In an embodiment, the computer system (300) is a directory server providing services for facilitating transactions between a merchant associated with an acquirer system, and an issuer system. In an embodiment, the computer system (300) is connected to the entities comprising the merchant, acquirer system, issuer system.

[0038] 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.

[0039] The terms "including", "comprising", “having” and variations thereof mean "including but not limited to", unless expressly specified otherwise.

[0040] The enumerated listing of items does not imply that any or all of the items are mutually exclusive, unless expressly specified otherwise. The terms "a", "an" and "the" mean "one or more", unless expressly specified otherwise.

[0041] A description of an embodiment with several components in communication with each other does not imply that all such components are required. On the contrary a variety of optional

components are described to illustrate the wide variety of possible embodiments of the invention.

[0042] When a single device or article is described herein, it will be readily apparent that more than one device/article (whether or not they cooperate) may be used in place of a single device/article. Similarly, where more than one device or article is described herein (whether or not they cooperate), it will be readily apparent that a single device/article may be used in place of the more than one device or article, or a different number of devices/articles may be used instead of the shown number of devices or programs. The functionality and/or the features of a device may be alternatively embodied by one or more other devices which are not explicitly described as having such functionality/features. Thus, other embodiments of the invention need not include the device itself.

[0043] 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. It is therefore intended that the scope of the invention be limited not by this detailed description, but rather by any claims that issue on an application based here on. Accordingly, the disclosure of the embodiments of the invention is intended to be illustrative, but not limiting, of the scope of the invention, which is set forth in the following claims.

[0044] While various aspects and embodiments have been disclosed herein, other aspects and embodiments will be apparent to those skilled in the art. The various aspects and embodiments disclosed herein are for purposes of illustration and are not intended to be limiting, with the true scope being indicated by the following claims.

ABSTRACT

[0045] The present invention aims to employ the second device for propagating to the loyalty model to allow a user to access a temporary card token without disclosing primary account number (PAN) information. A first device (101) is pre-registered with the software development kit (SDK) of the user's payment network provider for authorization tokens without disclosing card information. In addition, if a token is bumped on the dashboard of the first device, a token of low value might be sent to the second device based on the consolidated loyalty score of the devices. A silent push message sent by the payment network provider is forwarded by the Issuer to the second device (102). An Instant Token of the specified amount is generated on the second device after it has verified the push message's authenticity. Utilizing the identity data from the second device, Issuer will bill the customer for the transaction.

FIGURE 1

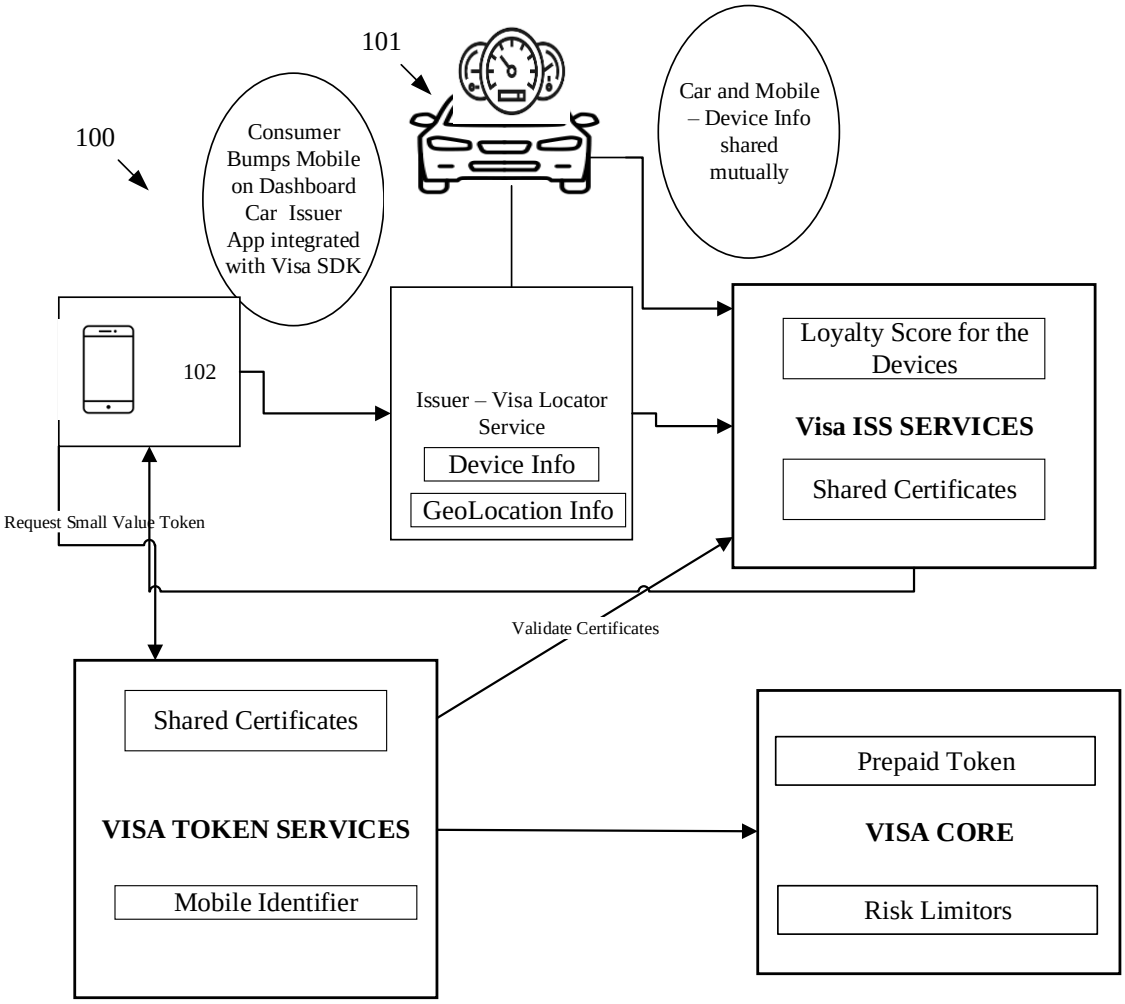
101
100
Consumer Bumps Mobile on Dashboard Car Issuer App integrated with Visa SDK
Car and Mobile – Device Info shared mutually
102
Issuer – Visa Locator Service
Device Info
GeoLocation Info
Loyalty Score for the Devices
Visa ISS SERVICES
Shared Certificates
Request Small Value Token
Validate Certificates
Shared Certificates
VISA TOKEN SERVICES
Mobile Identifier
Prepaid Token
VISA CORE
Risk Limitors

Figure 1

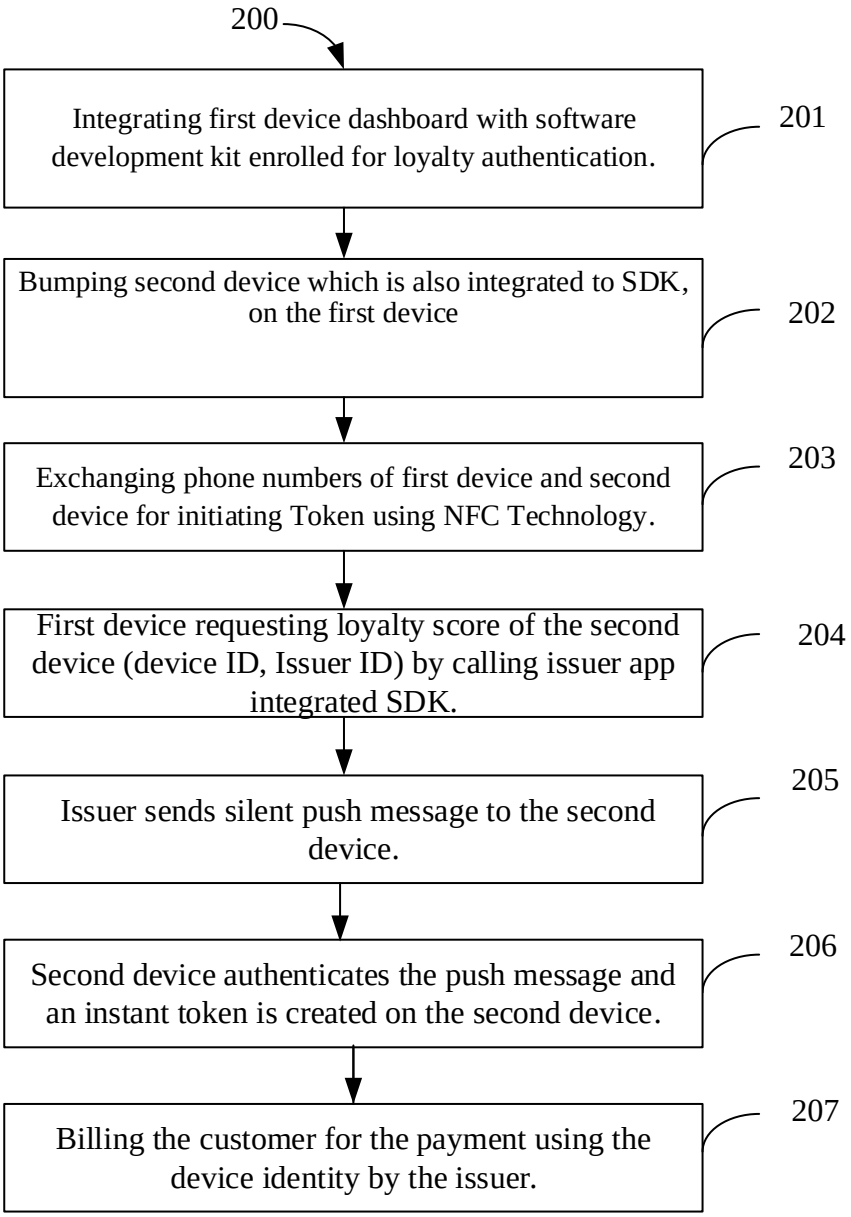
200
Integrating first device dashboard with software development kit enrolled for loyalty authentication.
201
Bumping second device which is also integrated to SDK, on the first device
202
Exchanging phone numbers of first device and second device for initiating Token using NFC Technology.
203
First device requesting loyalty score of the second device (device ID, Issuer ID) by calling issuer app integrated SDK.
204
Issuer sends silent push message to the second device.
205
Second device authenticates the push message and an instant token is created on the second device.
206
Billing the customer for the payment using the device identity by the issuer.
207

Figure 2

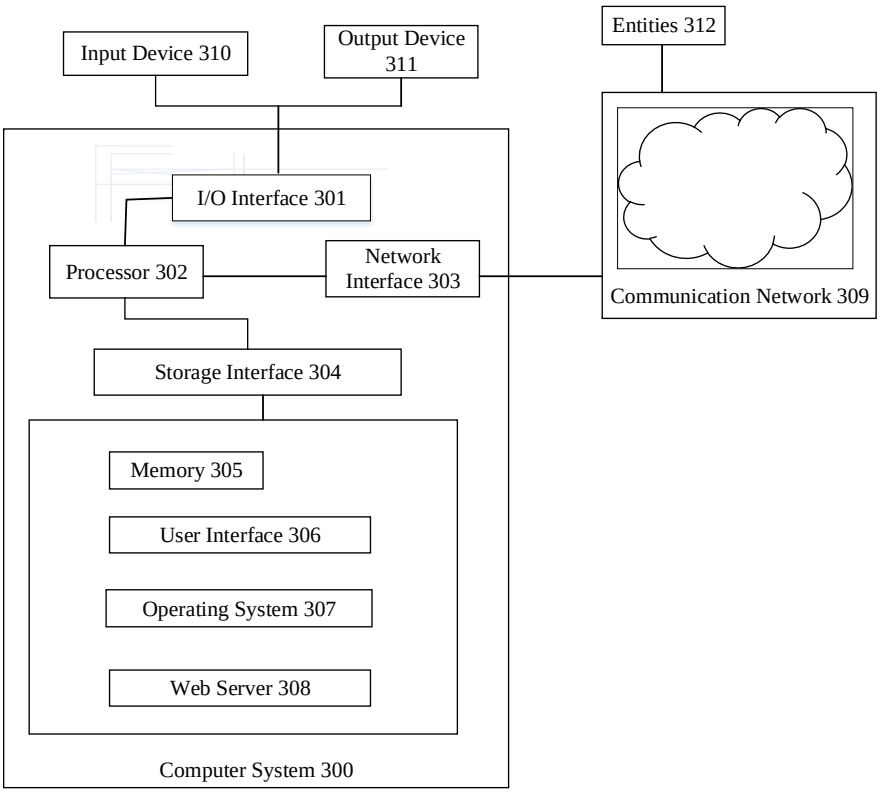
Input Device 310
Output Device 311
Entities 312
I/O Interface 301
Processor 302
Network Interface 303
Communication Network 309
Storage Interface 304
Memory 305
User Interface 306
Operating System 307
Web Server 308
Computer System 300

Figure 3