

SYSTEMS AND METHODS FOR PROVISIONING FUNDING CARD NUMBERS TO THIRD PARTY WALLETS

BACKGROUND OF THE INVENTION

1. Field of the Invention

[0001] Embodiments generally relate to systems and methods for provisioning funding card numbers to third party wallets.

2. Description of the Related Art

[0002] It is common practice for an issuer to provision a payment token, or device primary account number (“DPAN”), to a merchant. The DPAN allows the merchant to conduct a transaction without having the actual account number (the funding primary account number, or “FPAN”). Because the FPAN is not provided, the DPAN provides additional security.

SUMMARY OF THE INVENTION

[0003] Systems, methods, and devices for provisioning funding card numbers to merchant wallets are disclosed. In one embodiment, in an information processing apparatus comprising at least one computer processor, a method for provisioning funding card numbers to third party wallets may include: (1) authenticating a customer using an electronic device; (2) redirecting the customer to a third-party website; (3) receiving, from the third-party website and via a first API, a request for funding primary account numbers (FPANs) associated with the customer; (4) providing the third-party website with a plurality of FPAN identifiers for FPANs associated with the customer; (5) receiving, from the third-party website and via a second API, a request for a FPAN associated with a selected FPAN identifier; (6) encrypting

the FPAN associated with the selected FPAN identifier; and (7) communicating the encrypted FPAN to the third-party website.

[0004] In one embodiment, the method may further include providing the third-party website with an authentication token and a session key during the redirect.

[0005] In one embodiment, the FPAN identifiers may each include fewer than all digits of the FPAN.

[0006] In one embodiment, the FPAN identifiers may be encrypted

[0007] In one embodiment, the step of encrypting the FPAN associated with the selected FPAN identifier may include encrypting FPAN data associated with the selected FPAN identifier, wherein the FPAN data comprises the FPAN and at least one of an expiration date and a billing zip code.

[0008] In one embodiment, the third party may decrypt the encrypted FPAN and may store the FPAN.

[0009] According to another embodiment, in an issuer backend comprising at least one computer processor, a method for provisioning funding card numbers to third party wallets may include: (1) authenticating a customer using an electronic device accessing the issuer backend using a computer program; (2) receiving, from the customer, a request to provision a FPAN to a third party; (3) launching a frame in the computer program with a website for the third party, wherein the customer logs in to the website for the third party using the frame and the third-party website generates a session identifier for a session with the customer; (4) receiving, from the third-party website, the session identifier; (5) encrypting the FPAN; and (6) communicating the encrypted FPAN to the third-party website.

[0010] In one embodiment, the computer program may include a computer application or a website.

[0011] In one embodiment, the frame may include a lightbox.

[0012] In one embodiment, the method may further include validating the session identifier.

[0013] In one embodiment, the validation may include OAUTH or SiteMinder validation.

[0014] In one embodiment, the step of encrypting the FPAN may include encrypting FPAN data associated with the FPAN, wherein the FPAN data comprises the FPAN and at least one of an expiration date and a billing zip code.

[0015] In one embodiment, the third party may decrypt the encrypted FPAN and may store the FPAN.

[0016] According to another embodiment, in an information processing apparatus comprising at least one computer processor, a A method for provisioning funding card numbers to third party wallets may include: (1) receiving, from a third-party website and on behalf of a customer, an authentication request for the customer; (2) generating an access token; (3) generating a symmetric key using the access token; (4) receiving, from the third-party website and via a first API, a request for funding primary account numbers (FPANs) associated with the customer and an authentication token; (5) providing the third-party website with a plurality of FPAN identifiers for FPANs associated with the customer; (6) receiving, from the third-party website and via a second API, a request for a FPAN associated with a selected FPAN identifier and the authentication token; (7) encrypting the FPAN associated with

the selected FPAN identifier with the symmetric key; and (8) communicating the encrypted FPAN to the third-party website.

[0017] In one embodiment, the FPAN identifiers each may include fewer than all digits of the FPAN.

[0018] In one embodiment, the FPAN identifiers may be encrypted

[0019] In one embodiment, the step of encrypting the FPAN associated with the selected FPAN identifier may include encrypting FPAN data associated with the selected FPAN identifier, wherein the FPAN data comprises the FPAN and at least one of an expiration date and a billing zip code.

[0020] In one embodiment, the third party may decrypt the encrypted FPAN using the symmetric key and may store the FPAN.

[0021] In one embodiment, the authentication token may include an OAUTH token.

BRIEF DESCRIPTION OF THE DRAWINGS

[0022] In order to facilitate a fuller understanding of the present invention, reference is now made to the attached drawings in which:

[0023] Figure 1 discloses system provisioning funding card numbers to merchant wallets according to one embodiment;

[0024] Figure 2 discloses a method for provisioning funding card numbers to merchant wallets according to one embodiment;

[0025] Figure 3 discloses a method for provisioning funding card numbers to merchant wallets according to one embodiment; and

[0026] Figure 4 discloses a method for provisioning funding card numbers to merchant wallets according to one embodiment.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

[0027] Embodiments are directed to systems and methods for provisioning funding card numbers to merchant wallets.

[0028] Embodiments may use an API to provision funding card numbers with field level encryption using Public Key Infrastructure (PKI) to securely transport Funding Card Number between business entities (e.g., issuers, merchants, etc.). The issuer may be any issuer of the funding card (e.g., banks), and the merchant may be any ecommerce merchant.

[0029] In embodiments, third parties (e.g., FinTechs, merchants, wallet providers, etc.) may have access to the issuer's public API to present a lightbox or similar for authenticating customers and retrieving FPAN credentials.

[0030] In other embodiments, the customer may push FPAN credentials to third parties after they are authenticated by the issuer by authenticating to the merchant.

[0031] Underlying product services may be used to retrieve account information from the issuer's systems of record based on accounts associated with the customer's profile.

[0032] In embodiments, the APIs may be stateless and may be for onetime use. Thus, no life cycle or linkages are managed, and every time the customer wants to checkout or store the FPAN (e.g., card on file), the APIs may need to be invoked.

[0033] Referring to Figure 1, a system for provisioning funding card numbers to merchant wallets is disclosed according to an embodiment. System

100 may include third party 110, which may be any suitable e-commerce merchant, FinTech, e-wallet provider, aggregator, etc. A user or customer may interact with third party 110 using electronic device 115. The user may also interact with third party 110 using electronic device 115 via external API gateway 120.

[0034] Electronic device 115 may be any suitable electronic device, including smartphones, smart watches, desktop computers, notebook computers, laptop computers, workstations, kiosks, Internet of Things (IoT) appliances, etc.

[0035] API gateway 132 may receive FPAN provisioning requests from third party 110 and /or electronic device 115, and may route the requests to FPAN Services 134 within issuing financial institution 130.

[0036] In one embodiment, API 132 gateway may authenticate the user by calling authentication services 136.

[0037] FPAN service 134 may manage the merchant-specific controls, PKI encryption/decryption, and the gathering of data through internal services, such as encryption services 138, decryption services 140, etc.

[0038] Issuing financial institution 130 may further include rewards engine 142 that may provide an interface for the user/customer to pay for goods or services using rewards points.

[0039] Referring to Figure 2, a method for provisioning funding card numbers to merchant wallets is disclosed according to an embodiment. In one embodiment, the method described with reference to this figure may be directed to the issuer pushing a FPAN to a third party at the request of the user or customer.

[0040] In step 205, a customer may authenticate with a financial institution (e.g., using the financial institution's mobile application, website, etc.). The user may be responding to an offer, may be accessing the financial institution's reward website, etc.

[0041] In step 210, the authenticated customer may be redirect to a website for the third party. In one embodiment, a session key that may be passed with the redirect. The session key and/or index data may be used for subsequent API calls (e.g., SAML, OAUTH, etc.).

[0042] In one embodiment, the financial institution may also send the user authentication parameters, such as an authentication token, to the third party when they are invoked. This may be transparent to user.

[0043] In step 215, at checkout, the third party may retrieve a list of FPANs for the customer and may present the list to the customer. In one embodiment, the third party may invoke an API to retrieve the list. The third party may also provide the authentication parameters received in step 210 with the API.

[0044] In one embodiment, the financial institution may return less than the entire FPAN (e.g., it may only return the last four digits of the card, card art, etc.), and may only present that information to the customer. In one embodiment, this may be encrypted.

[0045] In step 220, the customer may select one of the FPANs for provisioning to the third party, and, in step 225, the merchant may request the FPAN for the selected FPAN.

[0046] In step 230, the financial institution may encrypt the financial instrument data (e.g., card number, expiration date, billing address, etc.) for the

FPAN and may provide the encrypted financial instrument data to the third party. In embodiments, at a minimum, the billing zip code may be provided.

[0047] In step 235, the third party may receive the encrypted financial instrument data and may decrypt it using PKI.

[0048] In step 240 the FPAN may be stored by the third party (e.g., for card on file transactions), or may be used for a pending transaction.

[0049] Referring to Figure 3, a method for provisioning funding card numbers to merchant wallets is disclosed according to an embodiment. In one embodiment, the method described with reference to this figure may be directed to the use of a redirect to a third party during checkout.

[0050] In step 305, a customer may authenticate with a financial institution (e.g., using the financial institution's mobile application, website, etc.). In one embodiment, the customer may be authenticated using OAuth. Additional information (e.g., a SiteMinder ID, a hashed SiteMinder ID, etc.) may be used for additional security as is necessary and/or desired.

[0051] In step 310, the authenticated customer may select to adding a FPAN to a third party, such as a third-party payment application, a merchant, etc.

[0052] In step 315, the financial institution's mobile application or website may open a frame or lightbox with the third party's web client.

[0053] In step 320, the customer may log in to the third party using the customer's credentials with the third party.

[0054] In step 325, the third-party web client may create a session with the issuer mobile application.

[0055] In step 330, the third-party web client may provide the session identifier to the financial institution (e.g., the financial institution's backend).

[0056] In step 335, the financial institution's backend may validate the session id and may initiate push provisioning of the FPAN to the third party. In one embodiment, the validation may include OAuth and/or SiteMinder validation

[0057] In step 340, the financial institution's backend may encrypt the financial instrument data (e.g., card number, expiration date, billing address, etc.) for the FPAN, and may send the encrypted financial instrument data to the third-party backend.

[0058] In step 345, the third-party backend may decrypt the financial instrument data using PKI. The third-party backend may store the decrypted financial instrument data.

[0059] Different encryption methods may be used based on the level of third party integration. For example, PGP may be used for encryption.

[0060] In step 350, the third-party web client may notify the customer that the financial instrument has been added for card on file payments.

[0061] Referring to Figure 4, a method for provisioning funding card numbers to merchant wallets is disclosed according to an embodiment. In one embodiment, the method described with reference to this figure may be directed to a third party pulling the FPAN from the issuer.

[0062] In step 405, a customer may log in to an account with a third party using the customer's credentials.

[0063] In step 410, the customer may select an option to add a financial instrument from the financial institution to the third party.

[0064] In step 415, the third party may initiate OAUTH login and access token creation with the financial institution.

[0065] In one embodiment, the issuer may generate an access token. An example of such is disclosed in U.S. Patent Application Ser. Nos. 16/697,780 and 62/773,860 are hereby incorporated by reference in their entireties.

[0066] In step 420, the financial institution may generate a symmetric key using the access token. In one embodiment, the symmetric key may be generated using, for example, Hardware Security Module, Java Keystore, Key Management Service for additional security, in addition to the OAUTH token.

[0067] In step 425, the third party may request a list of FPANs available for provisioning. In one embodiment, the third party may use an API to retrieve the list. In one embodiment, the OAUTH, SessionID, SiteMinder ID, or similar token will identify the customer.

[0068] This may be similar to step 215, above.

[0069] In step 430, the third party may receive the list of FPANs and may present the list to the customer. The customer may then select one of the FPANs for provisioning.

[0070] In step 435, the financial institution may receive a request for the selected FPAN. In one embodiment, the request may include the profile ID for the user and the symmetric key. In another embodiment, the request may include the OAUTH, SessionID, and/or SiteMinderID token, from which the customer profile id is determined.

[0071] In step 440, the financial institution may encrypt the financial instrument data (e.g., card number, expiration date, billing address, etc.) for the

FPAN using the symmetric key, and may send the encrypted financial instrument data to the third-party backend.

[0072] In step 445, the financial institution may provide the encrypted financial instrument data to the third-party backend.

[0073] In step 450, the third-party backend may decrypt the financial instrument data using the symmetric key. The third-party backend may store the decrypted financial instrument data.

[0074] In step 455, the third-party web client may notify the customer that the financial instrument has been added for card on file payments.

[0075] Hereinafter, general aspects of implementation of the systems and methods of embodiments will be described.

[0076] Embodiments of the system or portions of the system may be in the form of a “processing machine,” such as a general-purpose computer, for example. As used herein, the term “processing machine” is to be understood to include at least one processor that uses at least one memory. The at least one memory stores a set of instructions. The instructions may be either permanently or temporarily stored in the memory or memories of the processing machine. The processor executes the instructions that are stored in the memory or memories in order to process data. The set of instructions may include various instructions that perform a particular task or tasks, such as those tasks described above. Such a set of instructions for performing a particular task may be characterized as a program, software program, or simply software.

[0077] In one embodiment, the processing machine may be a specialized processor.

[0078] As noted above, the processing machine executes the instructions that are stored in the memory or memories to process data. This processing of data may be in response to commands by a user or users of the processing machine, in response to previous processing, in response to a request by another processing machine and/or any other input, for example.

[0079] As noted above, the processing machine used to implement embodiments may be a general-purpose computer. However, the processing machine described above may also utilize any of a wide variety of other technologies including a special purpose computer, a computer system including, for example, a microcomputer, mini-computer or mainframe, a programmed microprocessor, a micro-controller, a peripheral integrated circuit element, a CSIC (Customer Specific Integrated Circuit) or ASIC (Application Specific Integrated Circuit) or other integrated circuit, a logic circuit, a digital signal processor, a programmable logic device such as a FPGA, PLD, PLA or PAL, or any other device or arrangement of devices that is capable of implementing the steps of the processes disclosed herein.

[0080] The processing machine used to implement embodiments may utilize a suitable operating system. Thus, embodiments may include a processing machine running the iOS operating system, the OS X operating system, the Android operating system, the Microsoft Windows™ operating systems, the Unix operating system, the Linux operating system, the Xenix operating system, the IBM AIX™ operating system, the Hewlett-Packard UX™ operating system, the Novell Netware™ operating system, the Sun Microsystems Solaris™ operating system, the OS/2™ operating system, the BeOS™ operating system, the Macintosh operating system, the Apache operating system, an OpenStep™ operating system or another operating system or platform.

[0081] It is appreciated that in order to practice the method of the embodiments as described above, it is not necessary that the processors and/or the memories of the processing machine be physically located in the same geographical place. That is, each of the processors and the memories used by the processing machine may be located in geographically distinct locations and connected so as to communicate in any suitable manner. Additionally, it is appreciated that each of the processor and/or the memory may be composed of different physical pieces of equipment. Accordingly, it is not necessary that the processor be one single piece of equipment in one location and that the memory be another single piece of equipment in another location. That is, it is contemplated that the processor may be two pieces of equipment in two different physical locations. The two distinct pieces of equipment may be connected in any suitable manner. Additionally, the memory may include two or more portions of memory in two or more physical locations.

[0082] To explain further, processing, as described above, is performed by various components and various memories. However, it is appreciated that the processing performed by two distinct components as described above, in accordance with a further embodiment, may be performed by a single component. Further, the processing performed by one distinct component as described above may be performed by two distinct components.

[0083] In a similar manner, the memory storage performed by two distinct memory portions as described above, in accordance with a further embodiment, may be performed by a single memory portion. Further, the memory storage performed by one distinct memory portion as described above may be performed by two memory portions.

[0084] Further, various technologies may be used to provide communication between the various processors and/or memories, as well as to

allow the processors and/or the memories to communicate with any other entity; i.e., so as to obtain further instructions or to access and use remote memory stores, for example. Such technologies used to provide such communication might include a network, the Internet, Intranet, Extranet, LAN, an Ethernet, wireless communication via cell tower or satellite, or any client server system that provides communication, for example. Such communications technologies may use any suitable protocol such as TCP/IP, UDP, or OSI, for example.

[0085] As described above, a set of instructions may be used in the processing of embodiments. The set of instructions may be in the form of a program or software. The software may be in the form of system software or application software, for example. The software might also be in the form of a collection of separate programs, a program module within a larger program, or a portion of a program module, for example. The software used might also include modular programming in the form of object oriented programming. The software tells the processing machine what to do with the data being processed.

[0086] Further, it is appreciated that the instructions or set of instructions used in the implementation and operation of embodiments may be in a suitable form such that the processing machine may read the instructions. For example, the instructions that form a program may be in the form of a suitable programming language, which is converted to machine language or object code to allow the processor or processors to read the instructions. That is, written lines of programming code or source code, in a particular programming language, are converted to machine language using a compiler, assembler or interpreter. The machine language is binary coded machine instructions that are specific to a particular type of processing machine, i.e., to a particular type of computer, for example. The computer understands the machine language.

[0087] Any suitable programming language may be used in accordance with the various embodiments. Illustratively, the programming language used may include assembly language, Ada, APL, Basic, C, C++, COBOL, dBase, Forth, Fortran, Java, Modula-2, Pascal, Prolog, REXX, Visual Basic, and/or JavaScript, for example. Further, it is not necessary that a single type of instruction or single programming language be utilized in conjunction with the operation of the system and method. Rather, any number of different programming languages may be utilized as is necessary and/or desired.

[0088] Also, the instructions and/or data used in the practice of embodiments may utilize any compression or encryption technique or algorithm, as may be desired. An encryption module might be used to encrypt data. Further, files or other data may be decrypted using a suitable decryption module, for example.

[0089] As described above, the embodiments may illustratively be embodied in the form of a processing machine, including a computer or computer system, for example, that includes at least one memory. It is to be appreciated that the set of instructions, i.e., the software for example, that enables the computer operating system to perform the operations described above may be contained on any of a wide variety of media or medium, as desired. Further, the data that is processed by the set of instructions might also be contained on any of a wide variety of media or medium. That is, the particular medium, i.e., the memory in the processing machine, utilized to hold the set of instructions and/or the data used in embodiments may take on any of a variety of physical forms or transmissions, for example. Illustratively, the medium may be in the form of paper, paper transparencies, a compact disk, a DVD, an integrated circuit, a hard disk, a floppy disk, an optical disk, a magnetic tape, a RAM, a ROM, a PROM, an EPROM, a wire, a cable, a fiber, a communications channel, a satellite transmission, a memory card, a SIM card,

or other remote transmission, as well as any other medium or source of data that may be read by the processors.

[0090] Further, the memory or memories used in the processing machine that implements embodiments may be in any of a wide variety of forms to allow the memory to hold instructions, data, or other information, as is desired. Thus, the memory might be in the form of a database to hold data. The database might use any desired arrangement of files such as a flat file arrangement or a relational database arrangement, for example.

[0091] In the systems and methods, a variety of “user interfaces” may be utilized to allow a user to interface with the processing machine or machines that are used to implement embodiments. As used herein, a user interface includes any hardware, software, or combination of hardware and software used by the processing machine that allows a user to interact with the processing machine. A user interface may be in the form of a dialogue screen for example. A user interface may also include any of a mouse, touch screen, keyboard, keypad, voice reader, voice recognizer, dialogue screen, menu box, list, checkbox, toggle switch, a pushbutton or any other device that allows a user to receive information regarding the operation of the processing machine as it processes a set of instructions and/or provides the processing machine with information. Accordingly, the user interface is any device that provides communication between a user and a processing machine. The information provided by the user to the processing machine through the user interface may be in the form of a command, a selection of data, or some other input, for example.

[0092] As discussed above, a user interface is utilized by the processing machine that performs a set of instructions such that the processing machine processes data for a user. The user interface is typically used by the processing

machine for interacting with a user either to convey information or receive information from the user. However, it should be appreciated that in accordance with some embodiments of the system and method, it is not necessary that a human user actually interact with a user interface used by the processing machine. Rather, it is also contemplated that the user interface might interact, i.e., convey and receive information, with another processing machine, rather than a human user. Accordingly, the other processing machine might be characterized as a user. Further, it is contemplated that a user interface utilized in the system and method may interact partially with another processing machine or processing machines, while also interacting partially with a human user.

[0093] It will be readily understood by those persons skilled in the art that embodiments are susceptible to broad utility and application. Many embodiments and adaptations of the present invention other than those herein described, as well as many variations, modifications and equivalent arrangements, will be apparent from or reasonably suggested by the foregoing description thereof, without departing from the substance or scope.

[0094] Accordingly, while embodiments present invention has been described here in detail in relation to its exemplary embodiments, it is to be understood that this disclosure is only illustrative and exemplary of the present invention and is made to provide an enabling disclosure of the invention. Accordingly, the foregoing disclosure is not intended to be construed or to limit the present invention or otherwise to exclude any other such embodiments, adaptations, variations, modifications or equivalent arrangements.