

TITLE

TAP TO PROVISION DEVICE BINDING TECHNIQUE

TECHNICAL FIELD

[0001] The following disclosure relates generally to tokenization and, more specifically, to provisioning a token for use in a digital wallet of a user device.

SUMMARY

[0002] In part, in one aspect, the present disclosure provides a computer-implemented method for provisioning a token for use in a digital wallet of a user device, the computer-implemented method including retrieving, by a user device via communication between the user device and a payment card associated with a payment account, a payment card identity and a cryptogram of the payment card; sending, by the user device, a token provisioning request including the payment card identity, the cryptogram, and a device identity of the user device to a service provider; and receiving, by the user device, a token provisioning response including a provisioned token from the service provider, the token provisioning response is based on the payment card identity and the cryptogram, and the token provisioning response is cryptographically bound to the user device based on the device identity.

[0003] In part, in one aspect, the present disclosure provides a computer-implemented method for provisioning a token for use in a digital wallet of a user device, the computer-implemented method including receiving, by a service provider, a token provisioning request including a payment card identity, a cryptogram, and a device identity from a user device, the payment card identity and the cryptogram relate to a payment card associated with a payment account, and the device identity relates to the user device; sending, by the service provider, the token provisioning request to a token vault; receiving, by the service provider, a token provisioning response including a provisioned token from the token vault, the token provisioning response is based on the payment card identity and the cryptogram, and the token provisioning response is cryptographically bound to the user device based on the device identity; and sending, by the service provider, the token provisioning response to the user device.

[0004] In part, in one aspect, the present disclosure provides a computer-implemented method for provisioning a token for use in a digital wallet of a user device, the computer-implemented method including receiving, by a token vault, a token provisioning request including a payment card identity, a cryptogram, and a device identity, the payment card identity and the cryptogram relate to a payment card associated with a payment account,

and the device identity relates to a user device; generating, by the token vault, a token provisioning response including a provisioned token, the token provisioning response is based on the payment card identity and the cryptogram, and the token provisioning response is cryptographically bound to the user device based on the device identity; and sending, by the token vault, the token provisioning response to the user device.

BRIEF DESCRIPTION OF THE DRAWINGS

[0005] In the description, for purposes of explanation and not limitation, specific details are set forth, such as particular aspects, procedures, techniques, etc., to provide a thorough understanding of the present technology. However, it will be apparent to one skilled in the art that the present technology may be practiced in other aspects that depart from these specific details.

[0006] The accompanying drawings, where like reference numerals refer to identical or functionally similar elements throughout the separate views, together with the detailed description below, are incorporated in and form part of the specification, and serve to further illustrate aspects of concepts that include the claimed disclosure and explain various principles and advantages of those aspects.

[0007] The systems and methods disclosed herein have been represented where appropriate by conventional symbols in the drawings, showing only those specific details that are pertinent to understanding the various aspects of the present disclosure so as not to obscure the disclosure with details that will be readily apparent to those of ordinary skill in the art having the benefit of the description herein.

[0008] FIG. 1 illustrates a system to provision a token for use in a digital wallet of a user device, according to at least one aspect of the present disclosure.

[0009] FIG. 2 illustrates a system to provision a token for use in a digital wallet of a user device, including provisioning fraud, according to at least one aspect of the present disclosure.

[0010] FIG. 3 illustrates a system to provision a token for use in a digital wallet of a user device, including a tap-to-provision device-binding technique, according to at least one aspect of the present disclosure.

[0011] FIG. 4 illustrates a method to provision a token for use in a digital wallet of a user device, according to at least one aspect of the present disclosure.

[0012] FIG. 5 illustrates a method to provision a token for use in a digital wallet of a user

device, according to at least one aspect of the present disclosure.

[0013] FIG. 6 illustrates a method to provision a token for use in a digital wallet of a user device, according to at least one aspect of the present disclosure.

[0014] FIG. 7 is a block diagram of a computer apparatus with data processing subsystems or components, according to at least one aspect of the present disclosure.

[0015] FIG. 8 is a diagrammatic representation of an example system that includes a host machine within which a set of instructions to perform any one or more of the methodologies discussed herein may be executed, according to at least one aspect of the present disclosure.

DESCRIPTION

[0016] The following disclosure may provide exemplary systems, devices, and methods for conducting a financial transaction and related activities. Although reference may be made to such financial transactions in the examples provided below, aspects are not so limited. That is, the systems, methods, and apparatuses may be utilized for any suitable purpose.

[0017] Before discussing specific embodiments, aspects, or examples, some descriptions of terms used herein are provided below.

[0018] “Account credentials” may include any information that identifies an account and allows a payment processor to verify that a device, person, or entity has permission to access the account. For example, account credentials may include an account identifier (e.g., a PAN), a token (e.g., account identifier substitute), an expiration date, a cryptogram, a verification value (e.g., card verification value (CVV)), personal information associated with an account (e.g., address, etc.), an account alias, or any combination thereof. An account credential may be a string of numbers, letters, or any other suitable characters that may serve as confirmation. Account credentials may be static or dynamic such that they change over time. Further, in some embodiments or aspects, the account credentials may include information that is both static and dynamic. For example, an account identifier and expiration date may be static but a cryptogram may be dynamic and change for each transaction. Further, in some embodiments or aspects, some or all of the account credentials may be stored in a secure memory of a user device. The secure memory of the user device may be configured such that the data stored in the secure memory may not be directly accessible by outside applications and a payment application associated with the secure memory may be accessed to obtain the credentials stored on the secure memory. Accordingly, a mobile application may interface with a payment application in order to gain access to payment

credentials stored on the secure memory.

[0019] A “cryptographic algorithm” can be an encryption algorithm that transforms original data into an alternate representation, or a decryption algorithm that transforms encrypted information back to the original data. Examples of cryptographic algorithms may include triple data encryption standard (TDES), data encryption standard (DES), advanced encryption standard (AES), etc. Encryption techniques may include symmetric and asymmetric encryption techniques.

[0020] A “digital wallet” can include an electronic device that allows an individual to conduct electronic commerce transactions. A digital wallet may be designed to streamline the purchase and payment process. A digital wallet may allow the user to load one or more payment cards onto the digital wallet so as to make a payment without having to enter an account number or present a physical card.

[0021] A “digital wallet provider” may include an entity, such as an issuing bank or third party service provider, that issues a digital wallet and/or a digital wallet mobile application to a user that enables the user to conduct financial transactions. A digital wallet provider may provide standalone user-facing software applications that store account numbers, or representations of the account numbers (e.g., payment tokens), on behalf of a cardholder (or other user) to facilitate payments at more than one unrelated merchant, perform person-to-person payments, or load financial value into the digital wallet. A digital wallet provider may enable a user to access its account via a personal computer, mobile device or access device. Additionally, a digital wallet provider may also provide one or more of the following functions: storing multiple payment cards and other payment products on behalf of a user, storing other information including billing address, shipping addresses, and transaction history, initiating a transaction by one or more methods, such as providing a user name and password, NFC or a physical token, and may facilitate pass-through or two-step transactions. Examples of digital wallet providers include, but are not limited to, Google Wallet™, Android Pay®, Apple Pay®, and Samsung Pay®, and/or other like digital payment systems.

[0022] An “issuer” can include a payment account issuer. The payment account (which may be associated with one or more payment devices) may refer to any suitable payment account (e.g., credit card account, a checking account, a savings account, a merchant account assigned to a consumer, or a prepaid account), an employment account, an identification account, an enrollment account (e.g., a student account), etc.

[0023] As used herein, a “payment account” (which may be associated with one or more payment devices) may refer to any suitable payment account including a credit card account, a checking account, or a prepaid account.

[0024] A “payment network” may refer to an electronic payment system used to accept, transmit, or process transactions made by payment devices for money, goods, or services. The payment network may transfer information and funds among issuers, acquirers, merchants, and payment device users. One illustrative non-limiting example of a payment network is VisaNet, which is operated by Visa, Inc.

[0025] A “primary account number (PAN)” may be a variable length, (e.g., 13 to 19-digit) industry standard-compliant account number that is generated within account ranges associated with a BIN by an issuer.

[0026] “Provisioning” may include a process of providing data for use. For example, provisioning may include providing, delivering, or enabling a token on a device. Provisioning may be completed by any entity within or external to the transaction processing system. For example, in some embodiments or aspects, tokens may be provisioned by an issuer or a payment processing network onto a mobile device of a consumer (e.g., account holder). The provisioned tokens may have corresponding token data stored and maintained in the token vault or token registry. In some embodiments or aspects, a token vault or token registry may generate a token that may then be provisioned or delivered to a device. In some embodiments or aspects, an issuer may specify a token range from which token generation and provisioning can occur. Further, in some embodiments or aspects, an issuer may generate and notify a token vault of a token value and provide the token record information (e.g., token attributes) for storage in the token vault.

[0027] As used herein, the term “system” may refer to one or more computing devices or combinations of computing devices (e.g., processors, servers, client devices, software applications, components of such, and/or the like).

[0028] A “token” or “payment token” may include an identifier for a payment account that is a substitute for an account identifier, such as a primary account number (PAN). For example, a token may include a series of numeric and/or alphanumeric characters that may be used as a substitute for an original account identifier. For example, a token “4900 0000 0000 0001” may be used in place of a PAN “4147 0900 0000 1234.” In some embodiments or aspects, a token may be “format preserving” and may have a numeric format that conforms to the account identifiers used in existing payment processing networks (e.g., ISO

8583 financial transaction message format). In some embodiments or aspects, a token may be used in place of a PAN to initiate, authorize, settle or resolve a payment transaction or represent the original credential in other systems where the original credential would typically be provided. In some embodiments or aspects, a token value may be generated such that the recovery of the original PAN or other account identifier from the token value may not be computationally derived. For example, a token may have a random association with a particular real PAN so that the real PAN is not computationally derivable from the token. A lookup table may be used to associate a real PAN and a corresponding random token. Further, in some embodiments or aspects, the token format may be configured to allow the entity receiving the token to identify it as a token and recognize the entity that issued the token.

[0029] A “token requestor” may refer to a requestor that requests generation of a new token or requesting a new use of an existing token from a network token system. In some embodiments or aspects, a token requestor can request tokens for multiple domains and/or channels. Some non-limiting examples of token requestors may include, for example, card-on-file merchants, acquirers, acquirer processors, and payment gateways acting on behalf of merchants, payment enablers (e.g., original equipment manufacturers, mobile network operators, etc.), digital wallet providers, issuers, third party wallet providers, and/or payment processing networks. A token requestor may refer to an entity that is seeking to implement tokenization according to embodiments or aspects of the present disclosure. The token requestor may initiate a request that a primary account number (PAN) be tokenized by submitting a token request message to the token service provider. According to various embodiments or aspects discussed herein, a token requestor may no longer need to store a PAN associated with a token once the requestor have received the token in response to a token request message. A token requestor may be registered and identified uniquely by the token service provider within the tokenization ecosystem. During token requestor registration, the token service provider may formally process token requestor's application to participate in the token service system. The token service provider may collect information pertaining to the nature of the requestor and relevant use of tokens to validate and formally approve the token requestor and establish appropriate domain restriction controls. Successfully registered token requestors may be assigned a token requestor identifier that may also be entered and maintained within the token vault. Token requestors may be revoked or assigned new token requestor identifiers. This information may be subject to reporting and audit by the token service provider. As used in the specification and the claims, a “service provider” may perform substantially the same functions as a “token requestor,” as described above. In other words, as used in the claims, a “service provider”

may refer to a requestor that requests generation of a new token or requesting a new use of an existing token from a network token system.

[0030] A “token service system” refers to a system that facilitates requesting, generating and/or issuing tokens, as well as maintaining an established mapping of tokens to primary account numbers (PANs) in a repository (e.g., token vault). In some embodiments or aspects, the token service system may establish a token assurance level for a given token to indicate the confidence level of the token to PAN binding. The token service system may support token processing of payment transactions submitted using tokens by de-tokenizing the token to obtain the actual PAN. In various embodiments or aspects, the token service system may include a token requestor and a token service provider interacting with the token requestor. In some embodiments or aspects, a token service system may include a tokenization computer alone, or in combination with other computers such as a transaction processing network computer.

[0031] A “token vault” may refer to a repository that maintains established token-to-PAN mappings. According to various embodiments or aspects, the token vault may also maintain other attributes of the token requestor that may be determined at the time of registration and that may be used by the token service provider to apply domain restrictions or other controls during transaction processing. For example, the token vault may maintain one-to-one mapping between a token and an account identifying number represented by the token. The token vault may be a part of the token service system. In some embodiments or aspects, the token vault may be provided as a part of the token service provider. Alternatively, the token vault may be a remote repository accessible by the token service provider. Token vaults, due to the sensitive nature of the data mappings that are stored and managed in them, may be protected by strong underlying physical and logical security.

[0032] A “user” may include an individual. In some embodiments or aspects, a user may be associated with one or more personal accounts and/or mobile devices. The user may also be referred to as a cardholder, account holder, or consumer.

[0033] A “user device” is an electronic device that may be transported and/or operated by a user. A user device may provide remote communication capabilities to a network. The user device may be configured to transmit and receive data or communications to and from other devices. In some embodiments or aspects, the user device may be portable. Examples of user devices may include mobile phones (e.g., smart phones, cellular phones, etc.), PDAs, portable media players, wearable electronic devices (e.g., smart watches, fitness bands, ankle bracelets, rings, earrings, etc.), electronic reader devices, and portable

computing devices (e.g., laptops, netbooks, ultrabooks, etc.). Examples of user devices may also include automobiles with remote communication capabilities.

[0034] The use of digital wallets and tokenization is becoming increasingly popular due to the simplicity, ease-of-use, and added security benefits that they offer to their users. In a general sense, a user may add a payment card, such as a credit card, a debit card, or the like, to a digital wallet of a user device via a tokenization technique. As such, the user's digital wallet may include a payment token relating to their payment card for use in purchases. In one aspect, a purchase may be made via communication, such as near-field communication (NFC), between the user device including the payment token and a point-of-sale (POS) device. In another aspect, a purchase may be made online via a POS selectable-button, a POS selectable-widget, or the like on a merchant's website, application, or the like, using the payment token stored in the user's digital wallet.

[0035] As a result of the use of digital wallets and tokenization, a user may solely rely on the digital wallet of their user device and leave behind their physical payment card(s). This provides simplicity and ease-of-use while reducing the risk of theft and loss of any payment card that the user may typically carry around in their physical wallet. Even if a user continues to carry their physical payment card(s), the user may choose to utilize their digital wallet and a stored payment token for a purchase at a POS device such that a primary account number (PAN), a card verification value (CVV), and/or an expiry date printed on one of their payment cards is not visible to other members of the public while making purchases. Similarly, a user may decide to use their digital wallet and a stored payment token for a purchase on a merchant's website, application, or the like, such that they are not required to manually enter a PAN, a CVV, and/or an expiry date associated with one of their payment cards, which could pose a serious security threat in the event that a malicious software is able to read their inputs (e.g., keyboard inputs).

[0036] Despite the current benefits that digital wallets and tokenization techniques, there are still associated security risks. One of the largest risks includes provisioning fraud, where a fraudster may manually enter stolen account credentials associated with a user's payment card (e.g., a PAN, a CVV, an expiry date, and/or the like), which may be obtained via a database of leaked account credentials, into a digital wallet to provision a payment token for use to commit fraudulent transactions, which may occur at a POS device, at a retail store, or via a POS selectable input on a merchant's website, application, or the like.

[0037] As a result, the present disclosure provides a tap-to-provision solution, which requires a user to tap a physical payment card, such as a credit card, a debit card, or the

like, to a user device to capture account credentials, such as a PAN and an EMV (Europay, Mastercard, or Visa) cryptogram, associated with the physical payment card via communication, such as NFC. Based on a successful verification of the account credentials by a network and/or an issuer, a token may be provisioned for use in the user's digital wallet. This tap-to-provision solution provides additional security to prevent provisioning fraud as a fraudster would no longer be able to manually enter stolen account credentials. Rather, a fraudster would have to possess the physical payment card for which they are attempting to fraudulently provision. Furthermore, to prevent the risk of fraudsters attempting to capture account credentials of nearby user's in a queue, or the like, the present disclosure provides an authentication step requiring that a user who attempts to tap-to-provision further provide at least one of a card verification value (CVV) or an expiration date associated and/or printed on the physical payment card, or a one-time passcode sent to a contact (e.g., a phone number or an e-mail address) associated with the physical payment card. As a result, if a fraudster is able to read a nearby user's payment card's account credentials via communication, such as NFC, they will be unable to provision the physical payment card to their digital wallet as they will not have access to any one of the card verification value (CVV), the expiration date, or the one-time passcode sent to a contact associated with the physical payment card.

[0038] In addition to the tap-to-provision solution disclosed herein, the present disclosure, in some aspects, further provides a tap-to-provision device-binding solution, which includes each of the benefits of the aforementioned tap-to-provision solution and further cryptographically binds a token provisioning response to the user's device that initiated the token provisioning request. Thus, in the event that a malicious software is installed on the user's device and reroutes the token provisioning response, including a provisioned token, to a fraudster's user device, the fraudster would be unable to use the provisioned token as it has been cryptographically bound to the user's device.

[0039] Each of the tap-to-provision and tap-to-provision device-binding solutions will now be described in greater detail with respect to each of FIGs. 1-8.

[0040] FIG. 1 illustrates a system 100 to provision a token for use in a digital wallet of a user device, including a tap-to-provision technique, according to at least one aspect of the present disclosure. As shown, the system 100 includes a user device 102, the user device 102 further includes a digital wallet 104, and the digital wallet 104 further includes a kernel software 106 and a payment software 108. The system further includes a card 110, a service provider 112, a token vault 114, a POS 116, a network 118, and an issuer 120. Altogether, the system 100 and each of the aforementioned elements of the system 100 form a basis for

provisioning a token for use in a digital wallet of a user device based on a tap-to-provision technique. In at least one aspect, a user may tap a card 110 to a user device 102 and, as a result, the digital wallet 104 may retrieve account credentials, such as a PAN and an EMV cryptogram, associated with the card 110 via communication, such as NFC, by the kernel software 106. A token provisioning request, including the account credentials, is then generated and sent from the user device 102 via the kernel software 106 to a service provider 112. In at least one aspect, the user may be required to authenticate the token provisioning request. Authenticating the token provisioning request may include providing at least one of a card verification value (CVV) associated with the card 110, an expiration date associated with the card 110, or a one-time passcode sent to a contact (e.g., a phone number or an e-mail address) associated with the card 110. The service provider 112 then verifies the account credentials via the network 118 and the issuer 120. After verifying the account credentials, the token provisioning request is sent to a token vault 114. The token vault 114 then generates a token provisioning response, including a provisioned token, based on the account credentials included in the token provisioning request. The token vault 114 then sends the token provisioning response to the service provider 112, and the service provider 112 further sends the token provisioning response to the digital wallet 104 of the user device 102, which is received by the payment software 108, to provision the token in the digital wallet 104. After provisioning the token in the digital wallet 104, the token may be used for purchases via communication, such as NFC, at a POS 116, or via a POS 116 selectable-button, widget, or the like on a merchant's website, application, or the like. In at least one aspect, a user may tap the user device 102 to a POS 116 and the token will be sent to the POS 116 via communication, such as NFC. In at least one aspect, a user may select to use the token stored in digital wallet 104 for purchases made via a POS 116 selectable-button, widget, or the like on a merchant's website, application, or the like. The POS 116 then sends the token to a processor, an acquirer, and the network 118. After receiving the token at the network 118, the network 118 calls the token vault 114 to detokenize the token. After detokenizing the token, the network 118 verifies the account credentials, and the network 118 further sends an authorization to the issuer 120 to complete the transaction. As described above, FIG. 1 provides a system 100 to provision a token for use in a digital wallet of a user device, including a tap-to-provision technique.

[0041] FIG. 2 illustrates a system 200 to provision a token for use in a digital wallet of a user device, including a tap-to-provision technique and provisioning fraud, according to at least one aspect of the present disclosure. As shown, the system 200 includes user devices 202a-b, the user devices 202a-b further include digital wallets 204a-b, respectively, and digital wallets 204a-b further include a kernel software 206 and a payment software 208,

respectively. The system further includes a card 210, a service provider 212, a token vault 214, a POS 216, a network 218, and an issuer 220. Altogether, the system 200 and each of the aforementioned elements of the system 200 form a basis for provisioning a token for use in a digital wallet of a user device based on a tap-to-provision technique, while illustrating the risk of provisioning fraud. In at least one aspect, a user may tap a card 210 to a user device 202a, and, as a result, the digital wallet 204a may retrieve account credentials, such as a PAN and an EMV cryptogram, associated with the card 210 via communication, such as NFC, by the kernel software 206. A token provisioning request, including the account credentials, is then generated and sent from the user device 202a via the kernel software 206 to a service provider 212. In at least one aspect, the user may be required to authenticate the token provisioning request. Authenticating the token provisioning request may include providing at least one of a card verification value (CVV) associated with the card 210, an expiration date associated with the card 210, or a one-time passcode sent to a contact (e.g., a phone number or an e-mail address) associated with the card 210. The service provider 212 then verifies the account credentials via the network 218 and the issuer 220. After verifying the account credentials, the token provisioning request is sent to a token vault 214. The token vault 214 then generates a token provisioning response, including a provisioned token, based on the account credentials included in the token provisioning request. The token vault 214 then sends the token provisioning response to the service provider 212, and the service provider 212 further attempts to send the token provisioning response to the digital wallet 204a of the user device 202a, to provision the token in the digital wallet 204a. However, due to malicious software, or malware, installed on the user device 202a, the token provisioning response may be rerouted to a fraudster's user device 202b, which receives the token provisioning response in the fraudster's digital wallet 204b by the payment software 208, to provision the token in the digital wallet 204b. After rerouting the token provisioning response, and provisioning the token in the fraudster's digital wallet 204b, the fraudster may use the token for purchases via communication, such as NFC, at a POS 216, or via a POS 216 selectable-button, widget, or the like on a merchant's website, application, or the like. In at least one aspect, the fraudster may tap the fraudster user device 202b to a POS 216 and the token will be sent to the POS 216 via communication, such as NFC. In at least one aspect, the fraudster may select to use the token stored in digital wallet 204b for purchases made via a POS 216 selectable-button, widget, or the like on a merchant's website, application, or the like. The POS 216 then sends the token to a processor, an acquirer, and the network 218. After receiving the token at the network 218, the network 218 calls the token vault 214 to detokenize the token. After detokenizing the token, the network 218 verifies the account credentials, and the network 218 further sends an authorization to the issuer 220 to complete the transaction.

[0042] FIG. 3 illustrates a system 300 to provision a token for use in a digital wallet of a user device, including a tap-to-provision device-binding technique, according to at least one aspect of the present disclosure. As shown, the system 300 includes a user device 302, the user device 302 further includes a digital wallet 304, and the digital wallet 304 further includes a kernel software 306 and a payment software 308. The system further includes a card 310, a service provider 312, a token vault 314, a POS 316, a network 318, and an issuer 320. Altogether, the system 300 and each of the aforementioned elements of the system 300 form a basis for provisioning a token for use in a digital wallet of a user device based on a tap-to-provision device-binding technique. In at least one aspect, a user may tap a card 310 to a user device 302, and, as a result, the digital wallet 304 may retrieve account credentials, such as a PAN and an EMV cryptogram, associated with the card 310 via communication, such as NFC, by the kernel software 306. Additionally, the kernel software 306 may retrieve a device identity, such as a serial number, a universally unique identifier (UUID), a certificate, a public key, or a nonce, associated with the user device 302 from the payment software 308. Alternatively, according to at least one aspect of the present disclosure, the kernel software 306 may retrieve the device identity from an operating system of the user device 302. A token provisioning request, including the account credentials and the device identity, is then generated and sent from the user device 302 via the kernel software 306 to a service provider 312. In at least one aspect, the user may be required to authenticate the token provisioning request. Authenticating the token provisioning request may include providing at least one of a card verification value (CVV) associated with the card 310, an expiration date associated with the card 310, or a one-time passcode sent to a contact (e.g., a phone number or an e-mail address) associated with the card 310. The service provider 312 then verifies the account credentials via the network 318 and the issuer 320. After verifying the account credentials, the token provisioning request is sent to a token vault 314. The token vault 314 then generates a token provisioning response, including a provisioned token, based on the account credentials included in the token provisioning request, and the token vault 314 further cryptographically binds the token provisioning response to the user device 302 based on the device identity. In at least one aspect, the token vault 314 may cryptographically bind the token provisioning response to the user device 302 using a cryptographic encryption algorithm such as triple data encryption standard (TDES), advanced encryption standard (AES), or the like to encrypt the token provisioning response using the public key of the user device 302. The token vault 314 then sends the token provisioning response to the service provider 312, and the service provider 312 further sends the token provisioning response to the digital wallet 304 of the user device 302, which is received by the payment software 308, to provision the token in the digital wallet 304. In at least one aspect, the user device 302 may decrypt the token provisioning

response using a cryptographic decryption algorithm such as TDES, AES, or the like to decrypt the token provisioning response using a private key of the user device 302. After provisioning the token in the digital wallet 304, the token may be used for purchases via communication, such as NFC, at a POS 316, or via a POS 316 selectable-button, widget, or the like on a merchant's website, application, or the like. In at least one aspect, a user may tap the user device 302 to a POS 316 and the token will be sent to the POS 316 via communication, such as NFC. In at least one aspect, a user may select to use the token stored in digital wallet 304 for purchases made via a POS 316 selectable-button, widget, or the like on a merchant's website, application, or the like. The POS 316 then sends the token to a processor, an acquirer, and the network 318. After receiving the token at the network 318, the network 318 calls the token vault 314 to detokenize the token. After detokenizing the token, the network 318 verifies the account credentials, and the network 118 further sends an authorization to the issuer 320 to complete the transaction.

[0043] As a result of the tap-to-provision device-binding technique described above with respect to FIG. 3, a single payment account, or PAN, may have multiple associated tokens. For example, a single payment account, or PAN, may have a different token for each different device that may be used to initiate a transaction associated with the PAN using a specific token. That is, if a user wishes to use a single payment account, or PAN, for purchases made via communication, such as NFC, with a smartphone and a smartwatch, each device will have a separate token associated with the same payment account, or PAN.

[0044] Now, with respect to each of FIGs. 1-3, the user device 102, 202, and/or 302 may be any computing device such as a mobile device, a desktop computer, and/or the like that includes the necessary components to send, receive, process, and/or output data, and normally includes a display device, a processor, a memory, an input device, a network interface, and/or the like. As an example, the user device 102, 202a-b, and/or 302 may be one of a smartphone, a smartwatch, a laptop, a desktop, or the like. The digital wallet 104, 204a-b, and/or 304 may be any digital wallet as provided by a digital wallet provider, such as Google Wallet™, Android Pay®, Apple Pay®, and Samsung Pay®, and/or the like. Although disclosed herein as two separate elements, the service provider 112, 212, and 312, as well as the token vault 114, 214, and 314, may be combined into a single element. As an example, such a single element may be a token service system, which may perform substantially the same function and purpose of a combination of the service provider 112, 212, and 312, as well as the token vault 114, 214, and 314. Finally, the network 118, 218, and 318 may be a payment network, a processing network, and/or a payment processing network.

[0045] Furthermore, as would be appreciated by one having ordinary skill in the art, each of the systems 100, 200, and/or 300 of FIGs. 1-3, respectively, may include additional elements that may not be shown and/or described in the present disclosure. Namely, at least one of a computer apparatus, a computer system, or a computer server may be used in each of the systems 100, 200, and/or 300 to facilitate communication between each of the aforementioned elements of each of the systems 100, 200, and/or 300, respectively.

[0046] FIG. 4 illustrates a method 400 to provision a token for use in a digital wallet of a user device, according to at least one aspect of the present disclosure. According to at least one aspect of the present disclosure, the method 400 shown in FIG. 4 will now be described together with system 300 shown in FIG. 3. Accordingly, with reference now to FIGs. 3 and 4, in at least one aspect, according to the method 400, a user device 302 retrieves 402, via near-field communication between the user device 302 and a card 310 associated with a payment account, a payment card identity and a cryptogram of the card 310. The user device 302 further sends 404 a token provisioning request comprising the payment card identity, the cryptogram, and a device identity of the user device to a service provider 312. Finally, according to the method 400, the user device 302 receives 406 a token provisioning response comprising a provisioned token from the service provider 312, wherein the token provisioning response is based on the payment card identity and the cryptogram, and wherein the token provisioning response is cryptographically bound to the user device 302 based on the device identity. Altogether, each of 402, 404, and 406 provide a method 400 to provision a token for use in a digital wallet of a user device. As would be appreciated by one having ordinary skill in the art, the method 400 may be carried out by any suitable computer apparatus, computer system, or the like. Although each of 402, 404, and 406 have been described herein as being performed by the user device 302, it shall be appreciated that each of 402, 404, and 406 may be carried out by any suitable element to provision a token for use in a digital wallet of a user device.

[0047] FIG. 5 illustrates a method 500 to provision a token for use in a digital wallet of a user device, according to at least one aspect of the present disclosure. According to at least one aspect of the present disclosure, the method 500 shown in FIG. 5 will now be described together with system 300 shown in FIG. 3. Accordingly, with reference now to FIGs. 3 and 5, in at least one aspect, according to the method 500, a service provider 312 receives 502 a token provisioning request comprising a payment card identity, a cryptogram, and a device identity from a user device 302, wherein the payment card identity and the cryptogram relate to a card 310 associated with a payment account, and wherein the device identity relates to the user device 302. The service provider 312 further sends 504 the token provisioning

request to a token vault 314. The service provider 312 further receives 506 a token provisioning response comprising a provisioned token from the token vault 314, wherein the token provisioning response is based on the payment card identity and the cryptogram, and wherein the token provisioning response is cryptographically bound to the user device 302 based on the device identity. Finally, according to the method 500, the service provider 312 sends 508 the token provisioning response to the user device 302. Altogether, each of 502, 504, 506, and 508 provide a method 500 to provision a token for use in a digital wallet of a user device. As would be appreciated by one having ordinary skill in the art, the method 500 may be carried out by any suitable computer apparatus, computer system, or the like. Although each of 502, 504, 506, and 508 have been described herein as being performed by the service provider 312, it shall be appreciated that each of 502, 504, 506, and 508 may be carried out by any suitable element to provision a token for use in a digital wallet of a user device.

[0048] FIG. 6 illustrates a method 600 to provision a token for use in a digital wallet of a user device, according to at least one aspect of the present disclosure. According to at least one aspect of the present disclosure, the method 600 shown in FIG. 6 will now be described together with system 300 shown in FIG. 3. Accordingly, with reference now to FIGs. 3 and 6, in at least one aspect, according to the method 600, a token vault 314 receives 602 a token provisioning request comprising a payment card identity, a cryptogram, and a device identity, wherein the payment card identity and the cryptogram relate to a card 310 associated with a payment account, and wherein the device identity relates to a user device 302. The token vault 314 further generates 604 a token provisioning response comprising a provisioned token, wherein the token provisioning response is based on the payment card identity and the cryptogram, and wherein the token provisioning response is cryptographically bound to the user device 302 based on the device identity. Finally, according to the method 600, the token vault 314 sends 606 the token provisioning response to the user device 302. Altogether, each of 602, 604, and 606 provide a method 600 to provision a token for use in a digital wallet of a user device. As would be appreciated by one having ordinary skill in the art, the method 600 may be carried out by any suitable computer apparatus, computer system, or the like. Although each of 602, 604, and 606 have been described herein as being performed by the token vault 314, it shall be appreciated that each of 602, 604, and 606 may be carried out by any suitable element to provision a token for use in a digital wallet of a user device.

[0049] The aforementioned systems and methods to provision a token for use in a digital wallet of a user device, as described above with respect to each of FIGs. 1-6, may include,

or make use of, a number of computer apparatuses, computer systems, or the like. In other words, in order to utilize the systems and methods disclosed herein, at least one of a computer apparatus, computer system, or the like may be implemented. Each of these computer apparatuses, computer systems, or the like are described in greater detail below with respect to the computer apparatus 3000 shown in FIG. 7 and the example system 4000 shown in FIG. 8, which provides a connection between the solution disclosed herein and how such a solution may be implemented within a business entity, such as a payment network, a processing network, a payment processing network, or the like.

[0050] FIG. 7 is a block diagram of a computer apparatus 3000 with data processing subsystems or components, according to at least one aspect of the present disclosure. The subsystems shown in FIG. 7 are interconnected via a system bus 3010. Additional subsystems such as a printer 3018, keyboard 3026, fixed disk 3028 (or other memory comprising computer-readable media), monitor 3022, which is coupled to a display adapter 3020, and others are shown. Peripherals and input/output (I/O) devices, which couple to an I/O controller 3012 (which can be a processor or other suitable controller), can be connected to the computer system by any number of means known in the art, such as a serial port 3024. For example, the serial port 3024 or external interface 3030 can be used to connect the computer apparatus to a wide area network such as the Internet, a mouse input device, or a scanner. The interconnection via system bus allows the central processor 3016 to communicate with each subsystem and to control the execution of instructions from system memory 3014 or the fixed disk 3028, as well as the exchange of information between subsystems. The system memory 3014 and/or the fixed disk 3028 may embody a computer-readable medium.

[0051] FIG. 8 is a diagrammatic representation of an example system 4000 that includes a host machine 4002 within which a set of instructions to perform any one or more of the methodologies discussed herein may be executed, according to at least one aspect of the present disclosure. In various aspects, the host machine 4002 operates as a standalone device or may be connected (e.g., networked) to other machines. In a networked deployment, the host machine 4002 may operate in the capacity of a server or a client machine in a server-client network environment, or as a peer machine in a peer-to-peer (or distributed) network environment. The host machine 4002 may be a computer or computing device, a personal computer (PC), a tablet PC, a set-top box (STB), a personal digital assistant (PDA), a cellular telephone, a portable music player (e.g., a portable hard drive audio device such as an Moving Picture Experts Group Audio Layer 3 (MP3) player), a web appliance, a network router, switch or bridge, or any machine capable of executing a set of

instructions (sequential or otherwise) that specify actions to be taken by that machine. Further, while only a single machine is illustrated, the term “machine” shall also be taken to include any collection of machines that individually or jointly execute a set (or multiple sets) of instructions to perform any one or more of the methodologies discussed herein.

[0052] The example system 4000 includes the host machine 4002, running a host operating system (OS) 4004 on a processor or multiple processor(s)/processor core(s) 4006 (e.g., a central processing unit (CPU), a graphics processing unit (GPU), or both), and various memory nodes 4008. The host OS 4004 may include a hypervisor 4010 which is able to control the functions and/or communicate with a virtual machine (“VM”) 4012 running on machine readable media. The VM 4012 also may include a virtual CPU or vCPU 4014. The memory nodes 4008 may be linked or pinned to virtual memory nodes or vNodes 4016. When the memory node 4008 is linked or pinned to a corresponding vNode 4016, then data may be mapped directly from the memory nodes 4008 to their corresponding vNodes 4016.

[0053] All the various components shown in host machine 4002 may be connected with and to each other, or communicate to each other via a bus (not shown) or via other coupling or communication channels or mechanisms. The host machine 4002 may further include a video display, audio device or other peripherals 4018 (e.g., a liquid crystal display (LCD), alpha-numeric input device(s) including, e.g., a keyboard, a cursor control device, e.g., a mouse, a voice recognition or biometric verification unit, an external drive, a signal generation device, e.g., a speaker,) a persistent storage device 4020 (also referred to as disk drive unit), and a network interface device 4022. The host machine 4002 may further include a data encryption module (not shown) to encrypt data. The components provided in the host machine 4002 are those typically found in computer systems that may be suitable for use with aspects of the present disclosure and are intended to represent a broad category of such computer components that are known in the art. Thus, the system 4000 can be a server, minicomputer, mainframe computer, or any other computer system. The computer may also include different bus configurations, networked platforms, multi-processor platforms, and the like. Various operating systems may be used including UNIX, LINUX, WINDOWS, QNX ANDROID, IOS, CHROME, TIZEN, and other suitable operating systems.

[0054] The disk drive unit 4024 also may be a Solid-state Drive (SSD), a hard disk drive (HDD) or other includes a computer or machine-readable medium on which is stored one or more sets of instructions and data structures (e.g., data/instructions 4026) embodying or utilizing any one or more of the methodologies or functions described herein. The data/instructions 4026 also may reside, completely or at least partially, within the main memory node 4008 and/or within the processor(s) 4006 during execution thereof by the host

machine 4002. The data/instructions 4026 may further be transmitted or received over a network 4028 via the network interface device 4022 utilizing any one of several well-known transfer protocols (e.g., Hyper Text Transfer Protocol (HTTP)).

[0055] The processor(s) 4006 and memory nodes 4008 also may comprise machine-readable media. The term "computer-readable medium" or "machine-readable medium" should be taken to include a single medium or multiple medium (e.g., a centralized or distributed database and/or associated caches and servers) that store the one or more sets of instructions. The term "computer-readable medium" shall also be taken to include any medium that is capable of storing, encoding, or carrying a set of instructions for execution by the host machine 4002 and that causes the host machine 4002 to perform any one or more of the methodologies of the present application, or that is capable of storing, encoding, or carrying data structures utilized by or associated with such a set of instructions. The term "computer-readable medium" shall accordingly be taken to include, but not be limited to, solid-state memories, optical and magnetic media, and carrier wave signals. Such media may also include, without limitation, hard disks, floppy disks, flash memory cards, digital video disks, random access memory (RAM), read only memory (ROM), and the like. The example aspects described herein may be implemented in an operating environment comprising software installed on a computer, in hardware, or in a combination of software and hardware.

[0056] One skilled in the art will recognize that Internet service may be configured to provide Internet access to one or more computing devices that are coupled to the Internet service, and that the computing devices may include one or more processors, buses, memory devices, display devices, input/output devices, and the like. Furthermore, those skilled in the art may appreciate that the Internet service may be coupled to one or more databases, repositories, servers, and the like, which may be utilized to implement any of the various aspects of the disclosure as described herein.

[0057] The computer program instructions also may be loaded onto a computer, a server, other programmable data processing apparatus, or other devices to cause a series of operational steps to be performed on the computer, other programmable apparatus or other devices to produce a computer implemented process such that the instructions which execute on the computer or other programmable apparatus provide processes for implementing the functions/acts specified in the flowchart and/or block diagram block or blocks.

[0058] Suitable networks may include or interface with any one or more of, for instance, a local intranet, a PAN (Personal Area Network), a LAN (Local Area Network), a WAN (Wide

Area Network), a MAN (Metropolitan Area Network), a virtual private network (VPN), a storage area network (SAN), a frame relay connection, an Advanced Intelligent Network (AIN) connection, a synchronous optical network (SONET) connection, a digital T1, T3, E1 or E3 line, Digital Data Service (DDS) connection, DSL (Digital Subscriber Line) connection, an Ethernet connection, an ISDN (Integrated Services Digital Network) line, a dial-up port such as a V.90, V.34 or V.34bis analog modem connection, a cable modem, an ATM (Asynchronous Transfer Mode) connection, or an FDDI (Fiber Distributed Data Interface) or CDDI (Copper Distributed Data Interface) connection. Furthermore, communications may also include links to any of a variety of wireless networks, including WAP (Wireless Application Protocol), GPRS (General Packet Radio Service), GSM (Global System for Mobile Communication), CDMA (Code Division Multiple Access) or TDMA (Time Division Multiple Access), cellular phone networks, GPS (Global Positioning System), CDPD (cellular digital packet data), RIM (Research in Motion, Limited) duplex paging network, Bluetooth radio, or an IEEE 802.11-based radio frequency network. The network 4030 can further include or interface with any one or more of an RS-232 serial connection, an IEEE-1394 (Firewire) connection, a Fiber Channel connection, an IrDA (infrared) port, a SCSI (Small Computer Systems Interface) connection, a USB (Universal Serial Bus) connection or other wired or wireless, digital or analog interface or connection, mesh or Digi® networking.

[0059] In general, a cloud-based computing environment is a resource that typically combines the computational power of a large grouping of processors (such as within web servers) and/or that combines the storage capacity of a large grouping of computer memories or storage devices. Systems that provide cloud-based resources may be utilized exclusively by their owners or such systems may be accessible to outside users who deploy applications within the computing infrastructure to obtain the benefit of large computational or storage resources.

[0060] The cloud is formed, for example, by a network of web servers that comprise a plurality of computing devices, such as the host machine 4002, with each server 4030 (or at least a plurality thereof) providing processor and/or storage resources. These servers manage workloads provided by multiple users (e.g., cloud resource customers or other users). Typically, each user places workload demands upon the cloud that vary in real-time, sometimes dramatically. The nature and extent of these variations typically depends on the type of business associated with the user.

[0061] It is noteworthy that any hardware platform suitable for performing the processing described herein is suitable for use with the technology. The terms “computer-readable storage medium” and “computer-readable storage media” as used herein refer to any medium or media that participate in providing instructions to a CPU for execution. Such

media can take many forms, including, but not limited to, non-volatile media, volatile media, and transmission media. Non-volatile media include, for example, optical or magnetic disks, such as a fixed disk. Volatile media include dynamic memory, such as system RAM. Transmission media include coaxial cables, copper wire and fiber optics, among others, including the wires that comprise one aspect of a bus. Transmission media can also take the form of acoustic or light waves, such as those generated during radio frequency (RF) and infrared (IR) data communications. Common forms of computer-readable media include, for example, a flexible disk, a hard disk, magnetic tape, any other magnetic medium, a CD-ROM disk, digital video disk (DVD), any other optical medium, any other physical medium with patterns of marks or holes, a RAM, a PROM, an EPROM, an EEPROM, a FLASH EPROM, any other memory chip or data exchange adapter, a carrier wave, or any other medium from which a computer can read.

[0062] Various forms of computer-readable media may be involved in carrying one or more sequences of one or more instructions to a CPU for execution. A bus carries the data to system RAM, from which a CPU retrieves and executes the instructions. The instructions received by system RAM can optionally be stored on a fixed disk either before or after execution by a CPU.

[0063] Computer program code for carrying out operations for aspects of the present technology may be written in any combination of one or more programming languages, including an object-oriented programming language such as Java, Smalltalk, C++, or the like and conventional procedural programming languages, such as the "C" programming language, Go, Python, or other programming languages, including assembly languages. The program code may execute entirely on the user's computer, partly on the user's computer, as a stand-alone software package, partly on the user's computer and partly on a remote computer or entirely on the remote computer or server. In the latter scenario, the remote computer may be connected to the user's computer through any type of network, including a local area network (LAN) or a wide area network (WAN), or the connection may be made to an external computer (for example, through the Internet using an Internet Service Provider).

[0064] Examples of the systems and methods according to various aspects of the present disclosure are provided below in the following numbered clauses. Any aspect of a system or method may include any one or more than one, and any combination of, the numbered clauses described below.

[0065] Clause 1: A computer-implemented method for provisioning a token for use in a digital wallet of a user device, the computer-implemented method comprising: retrieving, by a user device via communication between the user device and a payment card

associated with a payment account, a payment card identity and a cryptogram of the payment card; sending, by the user device, to a service provider, a token provisioning request comprising the payment card identity, the cryptogram, and a device identity of the user device; and receiving, by the user device, a token provisioning response comprising a provisioned token from the service provider, wherein the token provisioning response is based on the payment card identity and the cryptogram, and wherein the token provisioning response is cryptographically bound to the user device based on the device identity.

[0066] Clause 2: The computer-implemented method according to Clause 1, wherein the payment card identity comprises a primary account number (PAN) of the payment card.

[0067] Clause 3: The computer-implemented method according to either of Clauses 1 or 2, wherein the cryptogram comprises a Europay, Mastercard, or Visa (EMV) cryptogram.

[0068] Clause 4: The computer-implemented method according to any of Clauses 1-3, wherein the device identity comprises at least one of a serial number, a universally unique identifier (UUID), a certificate, a public key, or a nonce associated with the user device.

[0069] Clause 5: The computer-implemented method according to any of Clauses 1-4, wherein the token provisioning response is encrypted using the public key, and wherein the computer-implemented method further comprises decrypting, by the user device, the token provisioning response using a private key associated with the user device.

[0070] Clause 6: The computer-implemented method according to any of Clauses 1-5, further comprising authenticating, by the user device, the token provisioning request.

[0071] Clause 7: The computer-implemented method according to any of Clauses 1-6, wherein authenticating the token provisioning request comprises providing at least one of a card verification value (CVV2) associated with the payment card, an expiration date associated with the payment card, or a one-time passcode sent to a contact associated with the payment card.

[0072] Clause 8: A computer-implemented method for provisioning a token for use in a digital wallet of a user device, the computer-implemented method comprising: receiving, by a service provider, a token provisioning request comprising a payment card identity, a cryptogram, and a device identity from a user device, wherein the payment card identity and the cryptogram relate to a payment card associated with a payment account; sending, by the service provider, the token provisioning request to a token vault; receiving, by the service

provider, a token provisioning response comprising a provisioned token from the token vault, wherein the token provisioning response is based on the payment card identity and the cryptogram, and wherein the token provisioning response is cryptographically bound to the user device based on the device identity; and sending, by the service provider, the token provisioning response to the user device.

[0073] Clause 9: The computer-implemented method according to Clause 8, wherein the payment card identity comprises a primary account number (PAN) of the payment card.

[0074] Clause 10: The computer-implemented method according to either of Clauses 8 or 9, wherein the cryptogram comprises a Europay, Mastercard, or Visa (EMV) cryptogram.

[0075] Clause 11: The computer-implemented method according to any of Clauses 8-10, wherein the device identity comprises at least one of a serial number, a universally unique identifier (UUID), a certificate, a public key, or a nonce associated with the user device.

[0076] Clause 12: The computer-implemented method according to any of Clauses 8-11, wherein the token provisioning response is encrypted using the public key, and wherein the token provisioning response is to be decrypted using a private key associated with the user device.

[0077] Clause 13: The computer-implemented method according to any of Clauses 8-12, further comprising requesting, by the service provider, authentication of the token provisioning request from the user device.

[0078] Clause 14: The computer-implemented method according to any of Clauses 8-13, wherein requesting authentication comprises requesting at least one of a card verification value (CVV2) associated with the payment card, an expiration date associated with the payment card, or a one-time passcode sent to a contact associated with the payment card.

[0079] Clause 15: A computer-implemented method for provisioning a token for use in a digital wallet of a user device, the computer-implemented method comprising: receiving, by a token vault, a token provisioning request comprising a payment card identity, a cryptogram, and a device identity, wherein the payment card identity and the cryptogram relate to a payment card associated with a payment account, and wherein the device identity relates to a user device; generating, by the token vault, a token provisioning response comprising a provisioned token, wherein the token provisioning response is based on the

payment card identity and the cryptogram, and wherein the token provisioning response is cryptographically bound to the user device based on the device identity; and sending, by the token vault, the token provisioning response to the user device.

[0080] Clause 16: The computer-implemented method according to Clause 15, wherein the payment card identity comprises a primary account number (PAN) of the payment card.

[0081] Clause 17: The computer-implemented method according to either of Clauses 15 or 16, wherein the cryptogram comprises a Europay, Mastercard, or Visa (EMV) cryptogram.

[0082] Clause 18: The computer-implemented method according to any of Clauses 15-17, wherein the device identity comprises at least one of a serial number, a universally unique identifier (UUID), a certificate, a public key, or a nonce associated with the user device.

[0083] Clause 19: The computer-implemented method according to any of Clauses 15-18, further comprising encrypting, by the token vault, the token provisioning response using the public key, wherein the token provisioning response is to be decrypted using a private key associated with the user device.

[0084] Clause 20: The computer-implemented method according to any of Clauses 15-19, wherein the token provisioning response is generated based on the payment card identity and the cryptogram being verified.

[0085] The foregoing detailed description has set forth various forms of the systems and/or processes via the use of block diagrams, flowcharts, and/or examples. Insofar as such block diagrams, flowcharts, and/or examples contain one or more functions and/or operations, it will be understood by those within the art that each function and/or operation within such block diagrams, flowcharts, and/or examples can be implemented, individually and/or collectively, by a wide range of hardware, software, firmware, or virtually any combination thereof. Those skilled in the art will recognize that some aspects of the forms disclosed herein, in whole or in part, can be equivalently implemented in integrated circuits, as one or more computer programs running on one or more computers (e.g., as one or more programs running on one or more computer systems), as one or more programs running on one or more processors (e.g., as one or more programs running on one or more microprocessors), as firmware, or as virtually any combination thereof, and that designing the circuitry and/or writing the code for the software and or firmware would be well within the

skill of one of skill in the art in light of this disclosure. In addition, those skilled in the art will appreciate that the mechanisms of the subject matter described herein are capable of being distributed as one or more program products in a variety of forms, and that an illustrative form of the subject matter described herein applies regardless of the particular type of signal bearing medium used to actually carry out the distribution.

[0086] Instructions used to program logic to perform various disclosed aspects can be stored within a memory in the system, such as dynamic random access memory (DRAM), cache, flash memory, or other storage. Furthermore, the instructions can be distributed via a network or by way of other computer-readable media. Thus a machine-readable medium may include any mechanism for storing or transmitting information in a form readable by a machine (e.g., a computer), but is not limited to, floppy diskettes, optical disks, compact disc, read-only memory (CD-ROMs), and magneto-optical disks, read-only memory (ROMs), random access memory (RAM), erasable programmable read-only memory (EPROM), electrically erasable programmable read-only memory (EEPROM), magnetic or optical cards, flash memory, or a tangible, machine-readable storage used in the transmission of information over the Internet via electrical, optical, acoustical or other forms of propagated signals (e.g., carrier waves, infrared signals, digital signals, etc.). Accordingly, the non-transitory computer-readable medium includes any type of tangible machine-readable medium suitable for storing or transmitting electronic instructions or information in a form readable by a machine (e.g., a computer).

[0087] 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, Python, 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 RAM, 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.

[0088] As used in any aspect herein, the term “logic” may refer to an app, software, firmware and/or circuitry configured to perform any of the aforementioned operations. Software may be embodied as a software package, code, instructions, instruction sets and/or data recorded on non-transitory computer-readable storage medium. Firmware may be embodied as code, instructions or instruction sets and/or data that are hard-coded (e.g., nonvolatile) in memory devices.

[0089] As used in any aspect herein, the terms “component,” “system,” “module” and the like can refer to a computer-related entity, either hardware, a combination of hardware and software, software, or software in execution.

[0090] As used in any aspect herein, an “algorithm” refers to a self-consistent sequence of steps leading to a desired result, where a “step” refers to a manipulation of physical quantities and/or logic states which may, though need not necessarily, take the form of electrical or magnetic signals capable of being stored, transferred, combined, compared, and otherwise manipulated. It is common usage to refer to these signals as bits, values, elements, symbols, characters, terms, numbers, or the like. These and similar terms may be associated with the appropriate physical quantities and are merely convenient labels applied to these quantities and/or states.

[0091] A network may include a packet switched network. The communication devices may be capable of communicating with each other using a selected packet switched network communications protocol. One example communications protocol may include an Ethernet communications protocol which may be capable of permitting communication using a Transmission Control Protocol/Internet Protocol (TCP/IP). The Ethernet protocol may comply or be compatible with the Ethernet standard published by the Institute of Electrical and Electronics Engineers (IEEE) titled “IEEE 802.3 Standard”, published in December, 2008 and/or later versions of this standard. Alternatively or additionally, the communication devices may be capable of communicating with each other using an X.25 communications protocol. The X.25 communications protocol may comply or be compatible with a standard promulgated by the International Telecommunication Union-Telecommunication Standardization Sector (ITU-T). Alternatively or additionally, the communication devices may be capable of communicating with each other using a frame relay communications protocol. The frame relay communications protocol may comply or be compatible with a standard promulgated by Consultative Committee for International Telegraph and Telephone (CCITT) and/or the American National Standards Institute (ANSI). Alternatively or additionally, the transceivers may be capable of communicating with each other using an Asynchronous Transfer Mode (ATM) communications protocol. The ATM communications protocol may comply or be compatible with an ATM standard published by the ATM Forum titled “ATM-MPLS Network Interworking 2.0” published August 2001, and/or later versions of this standard. Of course, different and/or after-developed connection-oriented network communication protocols are equally contemplated herein.

[0092] Unless specifically stated otherwise as apparent from the foregoing disclosure, it is appreciated that, throughout the present disclosure, discussions using terms such as

“processing,” “computing,” “calculating,” “determining,” “displaying,” or the like, refer to the action and processes of a computer system, or similar electronic computing device, that manipulates and transforms data represented as physical (electronic) quantities within the computer system's registers and memories into other data similarly represented as physical quantities within the computer system memories or registers or other such information storage, transmission or display devices.

[0093] One or more components may be referred to herein as “configured to,” “configurable to,” “operable/operative to,” “adapted/adaptable,” “able to,” “conformable/conformed to,” etc. Those skilled in the art will recognize that “configured to” can generally encompass active-state components and/or inactive-state components and/or standby-state components, unless context requires otherwise.

[0094] Those skilled in the art will recognize that, in general, terms used herein, and especially in the appended claims (e.g., bodies of the appended claims) are generally intended as “open” terms (e.g., the term “including” should be interpreted as “including but not limited to,” the term “having” should be interpreted as “having at least,” the term “includes” should be interpreted as “includes but is not limited to,” etc.). It will be further understood by those within the art that if a specific number of an introduced claim recitation is intended, such an intent will be explicitly recited in the claim, and in the absence of such recitation no such intent is present. For example, as an aid to understanding, the following appended claims may contain usage of the introductory phrases “at least one” and “one or more” to introduce claim recitations. However, the use of such phrases should not be construed to imply that the introduction of a claim recitation by the indefinite articles “a” or “an” limits any particular claim containing such introduced claim recitation to claims containing only one such recitation, even when the same claim includes the introductory phrases “one or more” or “at least one” and indefinite articles such as “a” or “an” (e.g., “a” and/or “an” should typically be interpreted to mean “at least one” or “one or more”); the same holds true for the use of definite articles used to introduce claim recitations.

[0095] In addition, even if a specific number of an introduced claim recitation is explicitly recited, those skilled in the art will recognize that such recitation should typically be interpreted to mean at least the recited number (e.g., the bare recitation of “two recitations,” without other modifiers, typically means at least two recitations, or two or more recitations). Furthermore, in those instances where a convention analogous to “at least one of A, B, and C, etc.” is used, in general such a construction is intended in the sense one having skill in the art would understand the convention (e.g., “a system having at least one of A, B, and C” would include but not be limited to systems that have A alone, B alone, C alone, A and B

together, A and C together, B and C together, and/or A, B, and C together, etc.). In those instances where a convention analogous to “at least one of A, B, or C, etc.” is used, in general such a construction is intended in the sense one having skill in the art would understand the convention (e.g., “a system having at least one of A, B, or C” would include but not be limited to systems that have A alone, B alone, C alone, A and B together, A and C together, B and C together, and/or A, B, and C together, etc.). It will be further understood by those within the art that typically a disjunctive word and/or phrase presenting two or more alternative terms, whether in the description, claims, or drawings, should be understood to contemplate the possibilities of including one of the terms, either of the terms, or both terms unless context dictates otherwise. For example, the phrase “A or B” will be typically understood to include the possibilities of “A” or “B” or “A and B.”

[0096] With respect to the appended claims, those skilled in the art will appreciate that recited operations therein may generally be performed in any order. Also, although various operational flow diagrams are presented in a sequence(s), it should be understood that the various operations may be performed in other orders than those which are illustrated, or may be performed concurrently. Examples of such alternate orderings may include overlapping, interleaved, interrupted, reordered, incremental, preparatory, supplemental, simultaneous, reverse, or other variant orderings, unless context dictates otherwise. Furthermore, terms like “responsive to,” “related to,” or other past-tense adjectives are generally not intended to exclude such variants, unless context dictates otherwise.

[0097] It is worthy to note that any reference to “one aspect,” “an aspect,” “an exemplification,” “one exemplification,” and the like means that a particular feature, structure, or characteristic described in connection with the aspect is included in at least one aspect. Thus, appearances of the phrases “in one aspect,” “in an aspect,” “in an exemplification,” and “in one exemplification” in various places throughout the specification are not necessarily all referring to the same aspect. Furthermore, the particular features, structures or characteristics may be combined in any suitable manner in one or more aspects.

[0098] As used herein, the singular form of “a,” “an,” and “the” include the plural references unless the context clearly dictates otherwise.

[0099] Any patent application, patent, non-patent publication, or other disclosure material referred to in this specification and/or listed in any Application Data Sheet is incorporated by reference herein, to the extent that the incorporated materials is not inconsistent herewith. As such, and to the extent necessary, the disclosure as explicitly set forth herein supersedes any conflicting material incorporated herein by reference. Any

material, or portion thereof, that is said to be incorporated by reference herein, but which conflicts with existing definitions, statements, or other disclosure material set forth herein will only be incorporated to the extent that no conflict arises between that incorporated material and the existing disclosure material. None is admitted to be prior art.

[0100] In summary, numerous benefits have been described which result from employing the concepts described herein. The foregoing description of the one or more forms has been presented for purposes of illustration and description. It is not intended to be exhaustive or limiting to the precise form disclosed. Modifications or variations are possible in light of the above teachings. The one or more forms were chosen and described in order to illustrate principles and practical application to thereby enable one of ordinary skill in the art to utilize the various forms and with various modifications as are suited to the particular use contemplated. It is intended that the claims submitted herewith define the overall scope.

CLAIMS

What is claimed is:

1. A computer-implemented method for provisioning a token for use in a digital wallet of a user device, the computer-implemented method comprising:
 - retrieving, by a user device via communication between the user device and a payment card associated with a payment account, a payment card identity and a cryptogram of the payment card;
 - sending, by the user device, to a service provider, a token provisioning request comprising the payment card identity, the cryptogram, and a device identity of the user device; and
 - receiving, by the user device, a token provisioning response comprising a provisioned token from the service provider, wherein the token provisioning response is based on the payment card identity and the cryptogram, and wherein the token provisioning response is cryptographically bound to the user device based on the device identity.
2. The computer-implemented method of Claim 1, wherein the payment card identity comprises a primary account number (PAN) of the payment card.
3. The computer-implemented method of Claim 1, wherein the cryptogram comprises a Europay, Mastercard, or Visa (EMV) cryptogram.
4. The computer-implemented method of Claim 1, wherein the device identity comprises at least one of a serial number, a universally unique identifier (UUID), a certificate, a public key, or a nonce associated with the user device.
5. The computer-implemented method of Claim 4, wherein the token provisioning response is encrypted using the public key, and wherein the computer-implemented method further comprises decrypting, by the user device, the token provisioning response using a private key associated with the user device.
6. The computer-implemented method of Claim 1, further comprising authenticating, by the user device, the token provisioning request.

7. The computer-implemented method of Claim 6, wherein authenticating the token provisioning request comprises providing at least one of a card verification value (CVV2) associated with the payment card, an expiration date associated with the payment card, or a one-time passcode sent to a contact associated with the payment card.
8. A computer-implemented method for provisioning a token for use in a digital wallet of a user device, the computer-implemented method comprising:
- receiving, by a service provider, a token provisioning request comprising a payment card identity, a cryptogram, and a device identity from a user device, wherein the payment card identity and the cryptogram relate to a payment card associated with a payment account;
 - sending, by the service provider, the token provisioning request to a token vault;
 - receiving, by the service provider, a token provisioning response comprising a provisioned token from the token vault, wherein the token provisioning response is based on the payment card identity and the cryptogram, and wherein the token provisioning response is cryptographically bound to the user device based on the device identity; and
 - sending, by the service provider, the token provisioning response to the user device.
9. The computer-implemented method of Claim 8, wherein the payment card identity comprises a primary account number (PAN) of the payment card.
10. The computer-implemented method of Claim 8, wherein the cryptogram comprises a Europay, Mastercard, or Visa (EMV) cryptogram.
11. The computer-implemented method of Claim 8, wherein the device identity comprises at least one of a serial number, a universally unique identifier (UUID), a certificate, a public key, or a nonce associated with the user device.
12. The computer-implemented method of Claim 11, wherein the token provisioning response is encrypted using the public key, and wherein the token provisioning response is to be decrypted using a private key associated with the user device.
13. The computer-implemented method of Claim 8, further comprising requesting, by the service provider, authentication of the token provisioning request from the user device.
14. The computer-implemented method of Claim 13, wherein requesting authentication comprises requesting at least one of a card verification value (CVV2) associated with the

payment card, an expiration date associated with the payment card, or a one-time passcode sent to a contact associated with the payment card.

15. A computer-implemented method for provisioning a token for use in a digital wallet of a user device, the computer-implemented method comprising:

receiving, by a token vault, a token provisioning request comprising a payment card identity, a cryptogram, and a device identity, wherein the payment card identity and the cryptogram relate to a payment card associated with a payment account, and wherein the device identity relates to a user device;

generating, by the token vault, a token provisioning response comprising a provisioned token, wherein the token provisioning response is based on the payment card identity and the cryptogram, and wherein the token provisioning response is cryptographically bound to the user device based on the device identity; and

sending, by the token vault, the token provisioning response to the user device.

16. The computer-implemented method of Claim 15, wherein the payment card identity comprises a primary account number (PAN) of the payment card.

17. The computer-implemented method of Claim 15, wherein the cryptogram comprises a Europay, Mastercard, or Visa (EMV) cryptogram.

18. The computer-implemented method of Claim 15, wherein the device identity comprises at least one of a serial number, a universally unique identifier (UUID), a certificate, a public key, or a nonce associated with the user device.

19. The computer-implemented method of Claim 18, further comprising encrypting, by the token vault, the token provisioning response using the public key, wherein the token provisioning response is to be decrypted using a private key associated with the user device.

20. The computer-implemented method of Claim 15, wherein the token provisioning response is generated based on the payment card identity and the cryptogram being verified.