November 2021

SYSTEM AND METHOD FOR AUTHENTICATION USING MOBILE DEVICE

CHRISTIAN AABYE
Visa

MARK RIGBY
Visa

TITLE: “SYSTEM AND METHOD FOR AUTHENTICATION USING MOBILE DEVICE”

VISA

CHRISTIAN AABYE

MARK RIGBY

TECHNICAL FIELD

[0001] This disclosure relates generally to the field Data Security. More particularly, the present disclosure relates to a system and method for authentication using a mobile device.

BACKGROUND

[0002] With increase in technology, many people use mobile wallets for several purposes such as make-in-store payments, online purchases, pay for digital content and so on. The mobile wallet is a virtual wallet that stores the payment card information on mobile devices of the user. The mobile wallets are a convenient way for the users make in-store payments and can be used at merchants listed with the mobile wallet service provider. Before using the mobile wallets, the user has to initially add the card details in the application to perform further financial transactions. The user may add the card details manually by typing

[0003] the various details such as Personal Account Number (PAN) and the expiry date, also the user may take photo from the camera of the mobile device to enter the card details. These techniques of adding the card details can lead to higher level of frauds, where the fraudsters may download the provisioned credentials and provision these details to the digital wallets. Also, these techniques of entering the card details are clunky process for the consumers to manually enter the details or taking a photo. Thus, there is a need for an efficient and a secure way of provisioning the card details of the user in the mobile wallets. Also, there is need for the efficient and secure way for storing the credentials in the mobile wallets.

SUMMARY

[0004] According to some non-limiting embodiments, the present disclosure relates to a system and method for authentication using mobile device. The method of the present disclosure includes, initially when a user wants to load the credentials of a user device into the mobile application, the mobile application on a mobile device provides an interaction data to the user device. In some embodiments, the mobile device may be a mobile phone, tablet phone and the

like, and the user device may be a payment card. Further the user device generates a cryptogram using a cryptographic key, the interaction data and the credentials stored on the user device. Upon generating the cryptogram, the user device sends the cryptogram to the mobile device. The mobile device upon receiving the cryptogram, transmits a provisioning request message to a server computer over a wireless communication network. The server computer communicates with the token service computer for the validation of the cryptogram. The token service computer transmits the authentication request which includes cryptogram to an authentication server computer. The authentication server computer authenticates the cryptogram and sends the authentication response to the token service computer which in-turn provides a payment token to the mobile device.

[0005] The present research work provides an advantage of a simpler way of entering the details of the user device by just tapping the user device (card of the user) over the mobile device. Also, in the present disclosure a cryptogram is generated by the user device that is used to authenticate the card or the user device and maintaining the credentials details in a secure way without disclosing the credentials explicitly. The card data is tokenized and secured which can be used for further transactions. The present disclosure provides revenue generating and value-added services

[0006] These and other features and characteristics of the present invention, as well as the methods of operation and functions of the related elements of structures and the combination of parts and economies of manufacture, will become more apparent upon consideration of the following description and the appended claims with reference to the accompanying drawings, all of which form a part of this specification, wherein like reference numerals designate corresponding parts in the various figures. It is to be expressly understood, however, that the drawings are for the purpose of illustration and description only and are not intended as a definition of the limits of the invention. As used in the specification and the claims, the singular form of “a,” “an,” and “the” include plural referents unless the context clearly dictates otherwise.

BRIEF DESCRIPTION OF THE DRAWINGS AND APPENDICES

[0007] Additional advantages and details of non-limiting embodiments are explained in greater detail below with reference to the exemplary embodiments that are illustrated in the accompanying schematic figures, in which:

[0008] FIG. 1 discloses a schematic diagram of a system and overlying process flow, in accordance with some embodiments of the present disclosure.

[0009] FIG. 2 discloses an additional embodiment of the system and overlying process flow, in accordance with some embodiments of the present disclosure.

[0010] FIG. 3 is a block diagram of an exemplary computer system for implementing embodiments consistent with the present disclosure.

DESCRIPTION OF THE DISCLOSURE

[0011] In the present document, the word "exemplary" is used herein to mean "serving as an example, instance, or illustration." Any embodiment or implementation of the present subject matter described herein as "exemplary" is not necessarily to be construed as preferred or advantageous over other embodiments.

[0012] While the disclosure is susceptible to various modifications and alternative forms, specific embodiment thereof has been shown by way of example in the drawings and will be described in detail below. It should be understood, however that it is not intended to limit the disclosure to the particular forms disclosed, but on the contrary, the disclosure is to cover all modifications, equivalents, and alternative falling within the spirit and the scope of the disclosure.

[0013] The terms “comprises”, “comprising”, or any other variations thereof, are intended to cover a non-exclusive inclusion, such that a setup, device or method that comprises a list of components or steps does not include only those components or steps but may include other components or steps not expressly listed or inherent to such setup or device or method. In other words, one or more elements in a device or system or apparatus proceeded by “comprises… a”

does not, without more constraints, preclude the existence of other elements or additional elements in the device or system or apparatus.

[0014] The terms "an embodiment", "embodiment", "embodiments", "the embodiment", "the embodiments", "one or more embodiments", "some embodiments", and "one embodiment" mean "one or more (but not all) embodiments of the invention(s)" unless expressly specified otherwise.

[0015] The terms "including", "comprising", “having” and variations thereof mean "including but not limited to", unless expressly specified otherwise.

[0016] As used herein, the terms “communication” and “communicate” may refer to the reception, receipt, transmission, transfer, provision, and/or the like of information (e.g., data, signals, messages, instructions, commands, and/or the like). For one unit (e.g., a device, a system, a component of a device or system, combinations thereof, and/or the like) to be in communication with another unit means that the one unit is able to directly or indirectly receive information from and/or transmit information to the other unit. This may refer to a direct or indirect connection (e.g., a direct communication connection, an indirect communication connection, and/or the like) that is wired and/or wireless in nature. Additionally, two units may be in communication with each other even though the information transmitted may be modified, processed, relayed, and/or routed between the first and second unit. For example, a first unit may be in communication with a second unit even though the first unit passively receives information and does not actively transmit information to the second unit. As another example, a first unit may be in communication with a second unit if at least one intermediary unit (e.g., a third unit located between the first unit and the second unit) processes information received from the first unit and communicates the processed information to the second unit. In some non-limiting embodiments, a message may refer to a network packet (e.g., a data packet and/or the like) that includes data. It will be appreciated that numerous other arrangements are possible.

[0017] As used herein, the term “computing device” may refer to one or more electronic devices that are configured to directly or indirectly communicate with or over one or more networks. A computing device may be a mobile or portable computing device, a desktop computer, a server, and/or the like. Furthermore, the term “computer” may refer to any computing device that

includes the necessary components to receive, process, and output data, and normally includes a display, a processor, a memory, an input device, and a network interface. A “computing system” may include one or more computing devices or computers. An “application” or “Application Program Interface” (API) refers to computer code or other data sorted on a computer-readable medium that may be executed by a processor to facilitate the interaction between software components, such as a client-side front-end and/or server-side back-end for receiving data from the client. An “interface” refers to a generated display, such as one or more graphical user interfaces (GUIs) with which a user may interact, either directly or indirectly (e.g., through a keyboard, mouse, touchscreen, etc.). Further, multiple computers, e.g., servers, or other computerized devices, such as an autonomous vehicle including a vehicle computing system, directly or indirectly communicating in the network environment may constitute a “system” or a “computing system”.

[0018] As used herein, the term "mobile device" may refer to any electronic device that may be transported and operated by a user, which may also provide remote communication capabilities to a network. Examples of remote communication capabilities include using a mobile phone (wireless) network, wireless data network (e.g., 3G, 4G or similar networks), Wi-Fi, Wi-Max, or any other communication medium that may provide access to a network such as the Internet or a private network. Examples of mobile devices include mobile phones (e.g., cellular phones), PDAs, tablet computers, net books, laptop computers, personal music players, hand-held specialized readers, wearable devices (e.g., watches), vehicles (e.g., cars), etc. A mobile device may comprise any suitable hardware and software for performing such functions, and may also include multiple devices or components (e.g., when a device has remote access to a network by tethering to another device - i.e., using the other device as a relay - both devices taken together may be considered a single mobile device).

[0019] As used herein, the term "Authentication data" may refer to any data suitable for authenticating a user or mobile device. Authentication data may be obtained from a user or a device that is operated by the user. Examples of authentication data obtained from a user may include PINs (personal identification numbers), passwords, etc. Examples of authentication data that may be obtained from a device may include device serial 15 numbers, hardware secure element identifiers, device fingerprints, phone numbers, IMEI numbers, etc.

[0020] As used herein, the term "provisioning server computer" may refer to any suitable computer that can provision data such as one or more access credentials to a device. In some embodiments of the invention, a provisioning server computer may be an access credential provisioning server computer, which may provision access credentials to a mobile device such as a mobile phone, over the air. An access provisioning server computer may store or generate access credentials. In some embodiments, an access provisioning server computer may include a token vault.

[0021] As used herein, the term "user device" may refer to a device that is operated by a user. An example of a "user device" may be a "payment device.",

[0022] As used herein, the term "payment device" may refer to any suitable device that may be used to conduct a financial transaction, such as to provide payment credentials to a merchant. The payment device may be a software object, a hardware object, or a physical object. As examples of physical objects, the payment device may comprise a substrate such as a paper or plastic card, and information that is printed, embossed, encoded, or otherwise included at or near a surface of an object. A hardware object can relate to circuitry (e.g., permanent voltage values), and a software object can relate to nonpermanent data stored on a device. A payment device may be associated with a value such as a monetary value, a discount, or store credit, and a payment device may be associated with an entity such as a bank, a merchant, a payment processing network, or a person. A payment device may be used to make a payment transaction. Suitable payment devices can be hand-held and compact so that they can fit into a user's wallet and/or pocket (e.g., pocket-sized). Example payment devices may include smart cards, magnetic stripe cards, keychain devices (such as the Speedpass ^{TM} commercially available from Exxon-Mobil Corp.), etc. Other examples of mobile devices include pagers, payment cards, security cards, access cards, smart media, transponders, and the like. If the payment device is in the form of a debit, credit, or smartcard, the payment device may also optionally have features such as magnetic stripes. Such devices can operate in either a contact or contactless mode. In some embodiments, a mobile device can function as a payment device (e.g., a mobile device can store and be able to transmit payment credentials for a transaction).

[0023] As used herein, the term "credential" may refer to any suitable information that serves as reliable evidence of worth, ownership, identity, or authority. An "access credential" may be a credential that may be used to gain access to a particular resource (e.g., a good, service, location, etc.). A credential may be a string of numbers, letters, or any other suitable characters, or any object or document that can serve as confirmation. Examples of credentials include identification cards, certified documents, access cards, passcodes and other login information, payment account numbers, access badge numbers, payment tokens, etc.

[0024] As used herein, the term "Payment credentials" may refer to any suitable information associated with an account (e.g. a payment account and/or payment device associated with the account). Such information may be directly related to the account or may be derived from information related to the account. Examples of account information may include a PAN (primary account number or "account number"), user name, expiration date, CVV (card verification value), dCVV (dynamic card verification value), CVV2 (card verification value 2), CVC3 card verification values, etc. Payment credentials may be any information that identifies or is associated with a payment account. Payment credentials may be provided in order to make a payment from a payment account. Payment credentials can also include a user name, an expiration date, a gift card number or code, and any other suitable information.

[0025] As used herein, the term "application" may refer to a computer code or other data stored on a computer readable medium (e.g. memory element or secure element) that may be executable by a processor to complete a task.

[0026] As used herein, the term "digital wallet" may refer to an electronic device that allows an individual to conduct electronic commerce transactions. A digital wallet may store user profile information, payment credentials, bank account information, one or more digital wallet identifiers and/or the like and can be used in a variety of transactions, such as but not limited to eCommerce, social networks, money transfer/ personal payments, mobile commerce, proximity payments, gaming, and/or the like for retail purchases, digital goods purchases, utility payments, purchasing games or gaming credits from gaming websites, transferring funds between users, and/or the like.

[0027] As used herein, the term "digital wallet provider" may refer to an entity, such as an issuing bank or third-party service provider, that issues a digital wallet 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.

[0028] As used herein, the term "token" may refer to a substitute value for a real credential. A token may be a type of credential, and may be a string of numbers, letters, or any other suitable characters. Examples of tokens include payment tokens, personal identification tokens, etc.

[0029] As used herein, the term "payment token" may refer to 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 alphanumeric characters that may be used as a substitute for an original account identifier. For example, a token "4900 0000 00000001" may be used in place of a PAN "4147 0900 0000 1234." In some embodiments, a token may be "format preserving" and may have a numeric format that conforms to the account identifiers used in existing transaction processing networks (e.g., ISO 8583 financial transaction message format). In some embodiments, 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, 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. Further, in some embodiments, 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.

[0030] As used herein, the term "Tokenization" is a process by which data is replaced with substitute data. For example, a payment account identifier (e.g., a primary account number (PAN)) may be tokenized by replacing the primary account identifier with a substitute number (e.g. a token) that may be associated with the payment account identifier. Further, tokenization may be

applied to any other information that may be replaced with a substitute value (i.e., token). Tokenization may be used to enhance transaction efficiency, improve transaction security, increase service transparency, or to provide a method for third party enablement.

[0031] As used herein, the term "token service provider" or "token service system" can include a system that services tokens. In some embodiments, a token service system can facilitate requesting, determining (e.g., 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, the token service system may establish a token assurance level for a given token to indicate the confidence level of the token to 30PAN binding. The token service system may include or be in communication with a token vault where the generated tokens are stored. The token service system may support token processing of payment transactions submitted using tokens by detokenizing the token to obtain the actual PAN. In some embodiments, a token service system may include a tokenization computer alone, or in combination with other computers such as a transaction processing network computer.

[0032] As used herein, the term "token domain" may refer to an area and/or circumstance in which a token can be used. Examples of the token domain may include, but are not limited to, payment channels (e.g., e-commerce, physical point of sale, etc.), POS entry modes (e.g., contactless, magnetic stripe, etc.), and merchant identifiers to uniquely identify where the token can be used. A set of parameters (i.e. token domain restriction controls) may be established as part of token issuance by the token service provider that may allow for enforcing appropriate usage of the token in payment transactions. For example, the token domain restriction controls may restrict the use of the token with particular presentment modes, such as contactless or e-commerce presentment modes. In some embodiments, the token domain restriction controls may restrict the use of the token at a particular merchant that can be uniquely identified. Some exemplary token domain restriction controls may require the verification of the presence of a token cryptogram that is unique to a given transaction. In some embodiments, a token domain can be associated with a token requestor.

[0033] As used herein, the term "Token expiry date" may refer to the expiration date/time of the token. The token expiry date may be passed among the entities of the tokenization ecosystem

during transaction processing to ensure interoperability. The token expiration date may be a numeric value (e.g. a 4-digit numeric value). In some embodiments, the token expiry date can be expressed as a time duration as measured from the time of issuance.

[0034] As used herein, the term "token request message" may be an electronic message for requesting a token. A token request message may include information usable for identifying a payment account or digital wallet, and/or information for generating a payment token. For example, a token request message may include payment credentials, mobile device identification information (e.g. a phone number or MSISDN), a digital wallet identifier, information identifying a tokenization service provider, a merchant identifier, a cryptogram, and/or any other suitable information. Information included in a token request message can be encrypted (e.g., with an issuer-specific key).

[0035] As used herein, the term "token response message" may be a message that responds to a token request. A token response message may include an indication that a token request was approved or denied. A token response message may also include a payment token, mobile device identification information (e.g. a phone number or MSISDN), a digital wallet identifier, information identifying a tokenization service provider, a merchant identifier, a cryptogram, and/or any other suitable information. Information included in a 10token response message can be encrypted (e.g., with an issuer-specific key).

[0036] As used herein, the term "user" may include an individual. In some embodiments, 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.

[0037] As used herein, the term "resource provider" may be an entity that can provide a resource such as goods, services, information, and/or access. Examples of resource providers include merchants, access devices, secure data access points, etc. A "merchant" may typically be an entity that engages in transactions and can sell goods or services, or provide access to goods or services.

[0038] As used herein, the term "acquirer" may typically be a business entity (e.g., a commercial bank) that has a business relationship with a particular merchant or other entity. Some entities can perform both issuer and acquirer functions. Some embodiments may encompass such single entity

issuer-acquirers. An acquirer may operate an acquirer computer, which can also be generically referred to as a "transport computer".

[0039] As used herein, the term "authorizing entity" may be an entity that authorizes a request. Examples of an authorizing entity may be an issuer, a governmental agency, a document repository, an access administrator, etc. An "issuer" may typically refer to a business entity (e.g., a bank) that maintains an account for a user. An issuer may also issue payment credentials stored on a user device, such as a cellular telephone, smart card, tablet, or laptop to the consumer. An authorizing entity may operate an authorizing computer.

[0040] As used herein, the term "access device" may be any suitable device that provides access to a remote system. An access device may also be used for communicating with a merchant computer, a transaction processing computer, an authentication computer, or any other suitable system. An access device may generally be located in any suitable location, such as at the location of a merchant. An access device may be in any suitable form. Some examples of access devices include POS or point of sale devices (e.g., POS terminals), cellular phones, PDAs, personal computers (PCs), tablet PCs, hand-held specialized readers, set-top boxes, electronic cash registers (ECRs), automated teller machines (ATMs), virtual cash registers (VCRs), kiosks, security systems, access systems, and the like. An access device may use any suitable contact or contactless mode of operation to send or receive data from, or associated with, a user mobile device. In some embodiments, where an access device may comprise a POS terminal, any suitable POS terminal may be used and may include a reader, a processor, and a computer-readable medium. A reader may include any suitable contact or contactless mode of operation. For example, exemplary card readers can include radio frequency (RF) antennas, optical scanners, bar code readers, or magnetic stripe readers to interact with a payment device and/or mobile device. In some embodiments, a cellular phone, tablet, or other dedicated wireless device used as a POS terminal may be referred to as a mobile point of sale or an "mPOS" terminal.

[0041] As used herein, the term "authorization request message" may be an electronic message that is sent to request authorization for a transaction. In some embodiments, an authorization request message may be an electronic message that is sent to a payment processing network and/or an issuer of a payment card to request authorization for a transaction. An authorization request

message according to some embodiments may comply with ISO 8583, which is a standard for systems that exchange electronic transaction information associated with a payment made by a consumer using a payment device or payment account. The authorization request message may include an issuer account identifier that may be associated with a payment device or payment account. An authorization request message may also comprise additional data elements corresponding to "identification information" including, by way of example only: a service code, a CVV (card verification value), a dCVV (dynamic card verification value), an expiration date, etc. An authorization request message may also comprise "transaction information," such as any information associated with a current transaction, such as the transaction amount, merchant identifier, merchant location, etc., as well as any other information that may be utilized in determining whether to identify and/or authorize a transaction.

[0042] As used herein, the term "authorization response message" may be an electronic message reply to an authorization request message. It may be generated by an issuing financial institution or a payment processing network. The authorization response message may include, by way of example only, one or more of the following status indicators: Approval transaction was approved; Decline transaction was not approved; or Call Center response pending more information, merchant must call the toll-free authorization phone number. The authorization response message may also include an authorization code, which may be a code that a credit card issuing bank returns in response to an authorization request message in an electronic message (either directly or through the payment processing network) to the merchant's access device (e.g. POS equipment) that indicates approval of the transaction. The code may serve as proof of 20 authorization. As noted above, in some embodiments, a payment processing network may generate or forward the authorization response message to the merchant.

[0043] As used herein, the term "server computer" is typically a powerful computer or cluster of computers. For example, the server computer can be a large mainframe, a minicomputer cluster, or a group of servers functioning as a unit. In one example, the server computer may be a database server coupled to a Web server.

[0044] As used herein, the term "processor" may refer to any suitable data computation device or devices. A processor may comprise one or more microprocessors working together to accomplish

a desired function. The processor may include CPU comprises at least one high-speed data processor adequate to execute program components for executing user and/or system-generated requests. The CPU may be a microprocessor such as AMD's Athlon, Duron and/or Opteron; IBM and/or Motorola's PowerPC; IBM's and Sony's Cell processor; Intel's Celeron, Itanium, Pentium, Xeon, and/or XScale; and/or the like processor(s).

[0045] As used herein, the term "memory" may be any suitable device or devices that can store electronic data. A suitable memory may comprise a non-transitory computer readable medium that stores instructions that can be executed by a processor to implement a desired method. Examples of memories may comprise one or more memory chips, disk drives, etc. Such memories may operate using any suitable electrical, optical, and/or magnetic mode of operation.

[0046] It will be apparent that systems and/or methods, described herein, can be implemented in different forms of hardware, software, or a combination of hardware and software. The actual specialized control hardware or software code used to implement these systems and/or methods is not limiting of the implementations. Thus, the operation and behavior of the systems and/or methods are described herein without reference to specific software code, it being understood that software and hardware can be designed to implement the systems and/or methods based on the description herein.

[0047] FIG. 1 discloses a schematic diagram of a system and overlying process flow.

[0048] In FIG. 1, a schematic diagram of a system 100 shows a user device 102, a mobile device 104, a server computer 106, and a token service computer 108 and an authentication server computer 110. The user device 102 may receive client data from one or more data sources (not shown in the FIG.1A) associated with the user device 102. The mobile device 104 may have an application running on it and can communicate with the server computer 106 at the remote location. The server computer 106 may be a wallet operator gateway. Also, the token service computer may be a visa token service and the authentication server computer may be a Visa authenticate system chip. The server computer 106 communicates with the token service computer 108, which in-turn communicates with the authentication server computer 110. The messages are transmitted among the devices over a wireless or a wired communication network using a secure

communications protocol such as, but not limited to, File Transfer Protocol (FTP), Hyper Text Transfer Protocol (HTTP), Secure Hypertext Transfer Protocol (HHTPS), Secure Socket Layer (SSL), ISO and so on.

[0049] In the step 1: Initially, a user requests the mobile device 104 to load the new card credentials of the user device 102. For example, the user may load the new card credentials to fund their prepaid account. The user may click on the icon "load new card" displayed within the mobile application.

[0050] In step 2: The user is prompted to tap their user device 102 over the mobile device 104. In communication between the user device 102 and the mobile device 104, the mobile device 104 acts similar to a POS terminal and may provide interaction data to the user device 102. The interaction data may include data such as mobile device identifier, a transaction amount, an unpredictable number and so on. Since the current interaction does not involve a actual payment transaction, the transaction amount may be zero value or in other words a null value. Once the interaction data is received by the user device 102, the interaction data and a credential (e.g., a primary account number) may be retrieved by the user device 102. The user device 102 generates a cryptogram by encrypting interaction data and the credential using a cryptographic key and sends it to the mobile device 104.

[0051] In step 3: Upon mobile device 104 receiving the cryptogram, the mobile device 104 sends a request to the wallet operator operating at the server computer 106 over a communication network. The request sent by the mobile device 104 includes the credentials and the cryptogram.

[0052] In step 4: The server computer 106 further transmits a token request which includes the credential and the cryptogram to the token service computer 108.

[0053] In step 5: The token service computer 108 transmits an authentication request which includes cryptogram and credential and interaction data to the authentication server computer 110.

[0054] In step 6: The authentication server computer 110 authenticates the cryptogram received from the token service computer 108. The authentication server computer 110 uses a key to generate a Message Authentication Code for the cryptogram that is stored in the user device

102. Further the authentication server computer 110 compares the generated cryptogram with the received cryptogram to validate the received cryptogram. In some embodiments, the cryptographic key may be a symmetric key that is generated using either master derived key or a unique derived key.

[0055] In step 7: The authentication server computer 110 transmits an authentication response with the cryptogram validation result to the token service computer 108. The cryptogram validation result may be successful or not successful. If the cryptogram generated by the authentication server computer 110 matches with the received cryptogram, then the validation is successful. If there is no match found between the cryptogram generated by the authentication server computer 110 and the received cryptogram then the validation is unsuccessful. The result of the validation is included in the authentication response message.

[0056] In step 8: The token service computer 108 then send a payment token to the server computer 106 if the validation result is successful. The token service computer 108 generates a token for the credentials of the user device and further sends the token to the server computer 106. The token service computer 108 directly does not return the original credentials, but does return the payment token to the server computer 106.

[0057] In step 9: The wallet operator operating at the server computer 106 decides whether the user device 102 is accepted for provisioning in the prepaid wallet operated via the mobile device 104. The server computer 106 provides a decision to the application regarding whether the requested token can be provisioned to the prepaid wallet operated via the mobile device104. If the decision is positive, then provisioning process is initiated. The wallet operators operating at the server computer **106** stores the token information which can be used for subsequent transactions.

[0058] In step 10: The mobile device 104 sends a notification to the user about the success or failure of provisioning the card details in the prepaid wallet operated via the mobile device 104.

[0059] FIG. 2 discloses an additional embodiment of the system and overlying process. In yet another embodiment, the system 200 shows a user device 102, a prepaid wallet operated via a mobile device 104, a server computer 106, and an authentication server computer 108. In this

embodiment, the steps 1-3 are same as that described under FIG 1. However, the only change in this embodiment is the that the cryptogram from the server computer 106 is directly sent to the authentication server computer 108, without the process of tokenization. However, in this embodiment, in step 4: The server computer 106 further transmits the authentication request which includes the credential and the cryptogram to the authentication server computer 108 without the need for tokenization as in the embodiment explained via FIG.1.

[0060] In Step 5: The authentication server computer 108 authenticates the cryptogram received from the server computer 106. The authentication server computer 108 uses a key to generate a Message Authentication Code for the cryptogram that is stored in the user device 102 Further the authentication server computer 108 compares the generated cryptogram with the received cryptogram to validate the received cryptogram.

[0061] In Step 6: The authentication server computer 108 transmits an authentication response with the cryptogram validation result to the server computer 106. The cryptogram validation result may be successful or not successful. If the cryptogram generated by the authentication server computer 108 matches with the received cryptogram, then the validation is successful. If there is no match found between the cryptogram generated by the authentication server computer 108 and the received cryptogram then the validation is unsuccessful. The result of the validation is included in the authentication response message.

[0062] In step 7: The wallet operator operating at the server computer 106 decides whether the user device 102 is accepted for provisioning in the mobile device of prepaid wallet operated via the mobile device 104. If the decision is positive, then provisioning process is initiated.

[0063] In step 8: The mobile device 104 sends a notification to the user about the success or failure of provisioning the card details in the prepaid wallet operated via the mobile device 104.

[0064] FIG. 3 is a block diagram of an exemplary computer system for implementing embodiments consistent with the present disclosure.

[0065] In some embodiments, FIG. 3 illustrates a block diagram of an exemplary computer system 300 for implementing embodiments consistent with the present disclosure. In some embodiments, the computer system 300 may be a authentication server computer 110 to perform the

authentication of the user device 102 for provisioning of the card details on the mobile device 104 The processor 302 may include at least one data processor for executing program components for executing user or system-generated business processes. A user may include a person, a person using a device such as those included in this disclosure, or such a device itself. The processor 302 may include specialized processing units such as integrated system (bus) controllers, memory management control units, floating point units, graphics processing units, digital signal processing units, etc.

[0066] The processor 302 may be disposed in communication with input devices 311 and output devices 312 via I/O interface 301. The I/O interface 301 may employ communication protocols/methods such as, without limitation, audio, analog, digital, stereo, IEEE-1393, serial bus, Universal Serial Bus (USB), infrared, PS/2, BNC, coaxial, component, composite, Digital Visual Interface (DVI), high-definition multimedia interface (HDMI), Radio Frequency (RF) antennas, S-Video, Video Graphics Array (VGA), IEEE 802.n /b/g/n/x, Bluetooth, cellular (e.g., Code-Division Multiple Access (CDMA), High-Speed Packet Access (HSPA+), Global System For Mobile Communications (GSM), Long-Term Evolution (LTE), WiMax, or the like), etc.

[0067] Using the I/O interface 301, the computer system 300 may communicate with the input devices 311 and the output devices 312.

[0068] In some embodiments, the processor 302 may be disposed in communication with a communication network 309 via a network interface 303. The network interface 303 may communicate with the communication network 309. The network interface 303 may employ connection protocols including, without limitation, direct connect, Ethernet (e.g., twisted pair 10/100/1000 Base T), Transmission Control Protocol/Internet Protocol (TCP/IP), token ring, IEEE 802.11a/b/g/n/x, etc. Using the network interface 303 and the communication network 209, the computer system 300 may communicate with a token service computer 108, which could be for instance, VISA token service. The VISA token service in-turn communicates with the mobile device 104 via the server computer 106, which could be for instance, wallet operator gateway. The communication network 309 can be implemented as one of the different types of networks, such as intranet or Local Area Network (LAN), Closed Area Network (CAN) and such. The communication network 309 may either be a dedicated network or a shared network, which

represents an association of the different types of networks that use a variety of protocols, for example, Hypertext Transfer Protocol (HTTP), CAN Protocol, Transmission Control Protocol/Internet Protocol (TCP/IP), Wireless Application Protocol (WAP), etc., to communicate with each other. Further, the communication network 309 may include a variety of network devices, including routers, bridges, servers, computing devices, storage devices, etc. In some embodiments, the processor 302 may be disposed in communication with a memory 305 (e.g., RAM, ROM, etc. not shown in FIG.3) via a storage interface 303. The storage interface 303 may connect to memory 305 including, without limitation, memory drives, removable disc drives, etc., employing connection protocols such as Serial Advanced Technology Attachment (SATA), Integrated Drive Electronics (IDE), IEEE-1393, Universal Serial Bus (USB), fibre channel, Small Computer Systems Interface (SCSI), etc. The memory drives may further include a drum, magnetic disc drive, magneto-optical drive, optical drive, Redundant Array of Independent Discs (RAID), solid-state memory devices, solid-state drives, etc.

[0069] The memory 305 may store a collection of program or database components, including, without limitation, a user interface 306, an operating system 307, a web browser 308 etc. In some embodiments, the computer system 300 may store user/application data, such as the data, variables, records, etc. as described in this disclosure. Such databases may be implemented as fault-tolerant, relational, scalable, secure databases such as Oracle or Sybase.

[0070] The operating system 307 may facilitate resource management and operation of the computer system 200. Examples of operating systems include, without limitation, APPLE® MACINTOSH® OS X®, UNIX®, UNIX-like system distributions (E.G., BERKELEY SOFTWARE DISTRIBUTION® (BSD), FREEBSD®, NETBSD®, OPENBSD, etc.), LINUX® DISTRIBUTIONS (E.G., RED HAT®, UBUNTU®, KUBUNTU®, etc.), IBM®OS/2®, MICROSOFT® WINDOWS® (XP®, VISTA®/7/8, 10 etc.), APPLE® IOS®, GOOGLE™ ANDROID™, BLACKBERRY® OS, or the like. The User interface 206 may facilitate display, execution, interaction, manipulation, or operation of program components through textual or graphical facilities. For example, user interfaces may provide computer interaction interface elements on a display system operatively connected to the computer system 300, such as cursors, icons, checkboxes, menus, scrollers, windows, widgets, etc. Graphical User Interfaces (GUIs) may

be employed, including, without limitation, Apple® Macintosh® operating systems' Aqua®, IBM® OS/2®, Microsoft® Windows® (e.g., Aero, Metro, etc.), web interface libraries (e.g., ActiveX®, Java®, Javascript®, AJAX, HTML, Adobe® Flash®, etc.), or the like.

[0071] In some embodiments, the computer system 300 may implement the web browser 308 stored program components. The web browser 308 may be a hypertext viewing application, such as MICROSOFT® INTERNET EXPLORER®, GOOGLE™ CHROME™, MOZILLA® FIREFOX®, APPLE® SAFARI®, etc. Secure web browsing may be provided using Secure Hypertext Transport Protocol (HTTPS), Secure Sockets Layer (SSL), Transport Layer Security (TLS), etc. Web browsers 308 may utilize facilities such as AJAX, DHTML, ADOBE® FLASH®, JAVASCRIPT®, JAVA®, Application Programming Interfaces (APIs), etc. In some embodiments, the computer system 300 may implement a mail server stored program component. The mail server may be an Internet mail server such as Microsoft Exchange, or the like. The mail server may utilize facilities such as Active Server Pages (ASP), ACTIVEX®, ANSI® C++/C#, MICROSOFT®, .NET, CGI SCRIPTS, JAVA®, JAVASCRIPT®, PERL®, PHP, PYTHON®, WEBOBJECTS®, etc. The mail server may utilize communication protocols such as Internet Message Access Protocol (IMAP), Messaging Application Programming Interface (MAPI), MICROSOFT® exchange, Post Office Protocol (POP), Simple Mail Transfer Protocol (SMTP), or the like. In some embodiments, the computer system 300 may implement a mail client stored program component. The mail client may be a mail viewing application, such as APPLE® MAIL, MICROSOFT® ENTOURAGE®, MICROSOFT® OUTLOOK®, MOZILLA® THUNDERBIRD®, etc.

[0072] Furthermore, one or more computer-readable storage media may be utilized in implementing embodiments consistent with the present disclosure. A computer-readable storage medium refers to any type of physical memory on which information or data readable by a processor may be stored. Thus, a computer-readable storage medium may store instructions for execution by one or more processors, including instructions for causing the processor(s) to perform steps or stages consistent with the embodiments described herein. The term "computer-readable medium" should be understood to include tangible items and exclude carrier waves and transient signals, i.e., non-transitory. Examples include Random Access Memory (RAM), Read-Only Memory (ROM), volatile memory, non-volatile memory, hard drives, Compact Disc (CD) ROMs, Digital Video Disc (DVDs), flash drives, disks, and any other known physical storage media.

[0073] Finally, the language used in the specification has been principally selected for readability and instructional purposes, and it may not have been selected to delineate or circumscribe the inventive subject matter. Accordingly, the disclosure of the embodiments of the disclosure is intended to be illustrative, but not limiting, of the scope of the disclosure.

[0074] With respect to the use of substantially any plural and/or singular terms herein, those having skill in the art can translate from the plural to the singular and/or from the singular to the plural as is appropriate to the context and/or application. The various singular/plural permutations may be expressly set forth herein for sake of clarity.

[0075] Any of the software components or functions described in this application, may be implemented as software code to be executed by a processor using any suitable computer language such as, for example, Java, C++ or Perl using, for example, conventional or object-oriented techniques. The software code may be stored as a series of instructions, or commands on a computer readable medium, such as a random access memory (RAM), a read only memory (ROM), a magnetic medium such as a hard-drive or a floppy disk, or an optical medium such as a CD-ROM. Any such computer readable medium may reside on or within a single computational apparatus, and may be present on or within different computational apparatuses within a system or network.

[0076] The above description is illustrative and is not restrictive. Many variations of the invention may become apparent to those skilled in the art upon review of the disclosure. The scope of the invention can, therefore, be determined not with reference to the above description, but instead can be determined with reference to the pending claims along with their full scope or equivalents.

[0077] One or more features from any embodiment may be combined with one or more features of any other embodiment without departing from the scope of the invention.

[0078] A recitation of "a", "an" or "the" is intended to mean "one or more" unless specifically indicated to the contrary.

[0079] All patents, patent applications, publications, and descriptions mentioned above are herein incorporated by reference in their entirety for all purposes. None is admitted to be prior art.

[0080] Although the invention has been described in detail for the purpose of illustration based on what is currently considered to be the most practical and preferred embodiments, it is to be understood that such detail is solely for that purpose and that the invention is not limited to the disclosed embodiments, but, on the contrary, is intended to cover modifications and equivalent arrangements that are within the spirit and scope of the appended claims. For example, it is to be understood that the present invention contemplates that, to the extent possible, one or more features of any embodiment can be combined with one or more features of any other embodiment.

SYSTEM AND METHOD FOR AUTHENTICATION USING MOBILE DEVICE

ABSTRACT

[0081] The methods and system disclosed in present disclosure is to perform authentication of a user device before provisioning card details in a digital wallet. In present disclosure, user taps user device on mobile device, upon tapping interaction data is sent to user device. The user device further generates cryptogram using interaction data and credentials of user device. The cryptogram generated is sent to server computer, which verifies whether card details can be provisioned by sending token request to token service computer which further sends authentication request to authentication server system. The authentication server system authenticates received cryptogram and generates validation result either to be successful or to be a failure. The validation result is sent to token service system which in turn sends token response to server computer. Further, server computer decides whether to provision and store the card details and the token received based on token response. Finally, result of provisioning is updated to the user through the mobile device. Hence, the method and the system of the present disclosure eases the provisioning process for cardholders by removing the need to manually enter card details or take a photo of the card and provides assurance that the genuine card is in the possession of individual initiating the provisioning request.

FIG .1

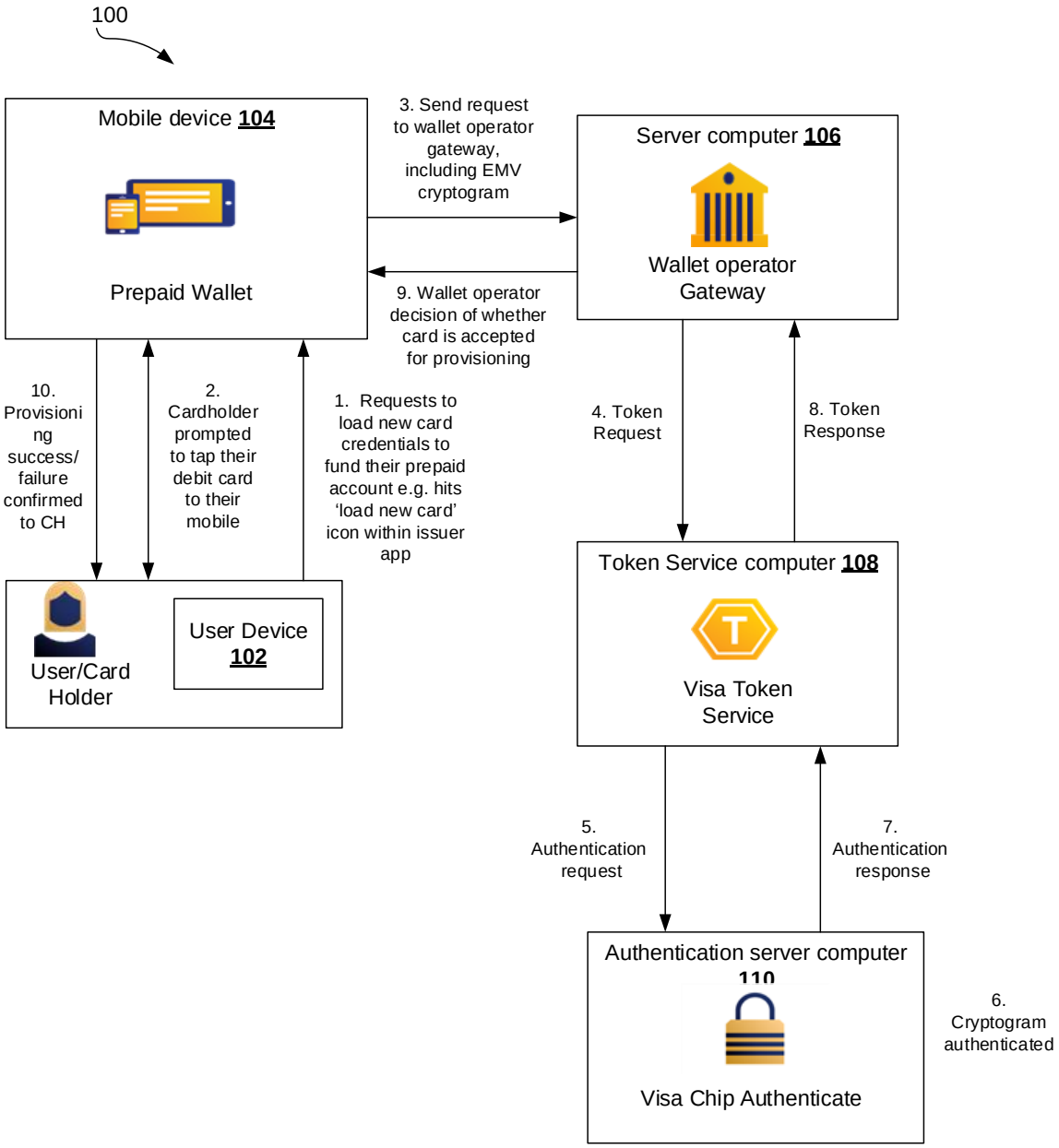
100
Mobile device 104
Prepaid Wallet
3. Send request to wallet operator gateway, including EMV cryptogram
9. Wallet operator decision of whether card is accepted for provisioning
Server computer 106
Wallet operator Gateway
10. Provisioning success/ failure confirmed to CH
2. Cardholder prompted to tap their debit card to their mobile
1. Requests to load new card credentials to fund their prepaid account e.g. hits 'load new card' icon within issuer app
4. Token Request
8. Token Response
User/Card Holder
User Device 102
Token Service computer 108
Visa Token Service
5. Authentication request
7. Authentication response
Authentication server computer 110
Visa Chip Authenticate
6. Cryptogram authenticated

FIG. 1

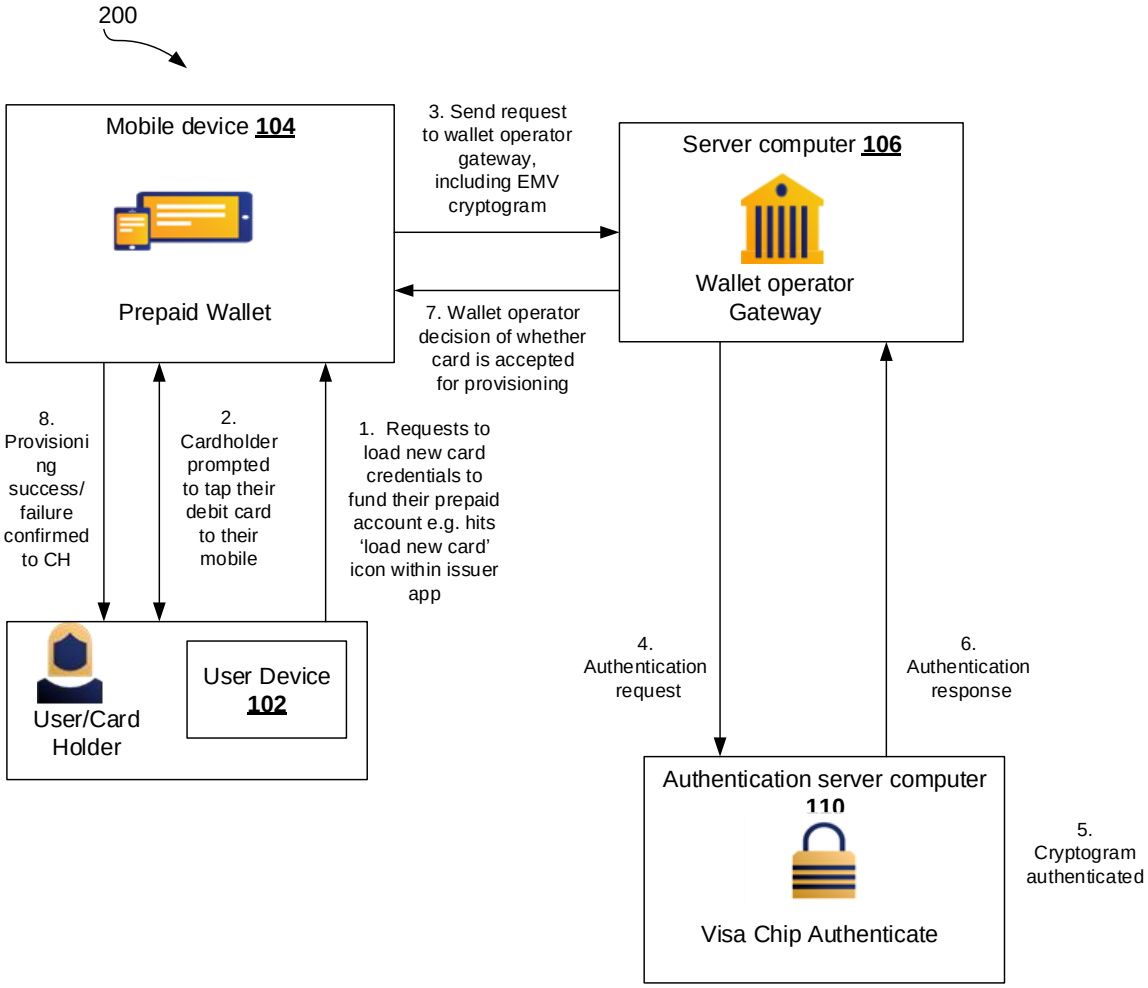
200
Mobile device 104
Prepaid Wallet
3. Send request to wallet operator gateway, including EMV cryptogram
Server computer 106
Wallet operator Gateway
7. Wallet operator decision of whether card is accepted for provisioning
8. Provisioning success/ failure confirmed to CH
2. Cardholder prompted to tap their debit card to their mobile
1. Requests to load new card credentials to fund their prepaid account e.g. hits 'load new card' icon within issuer app
User/Card Holder
User Device 102
4. Authentication request
6. Authentication response
Authentication server computer 110
Visa Chip Authenticate
5. Cryptogram authenticated

FIG. 2

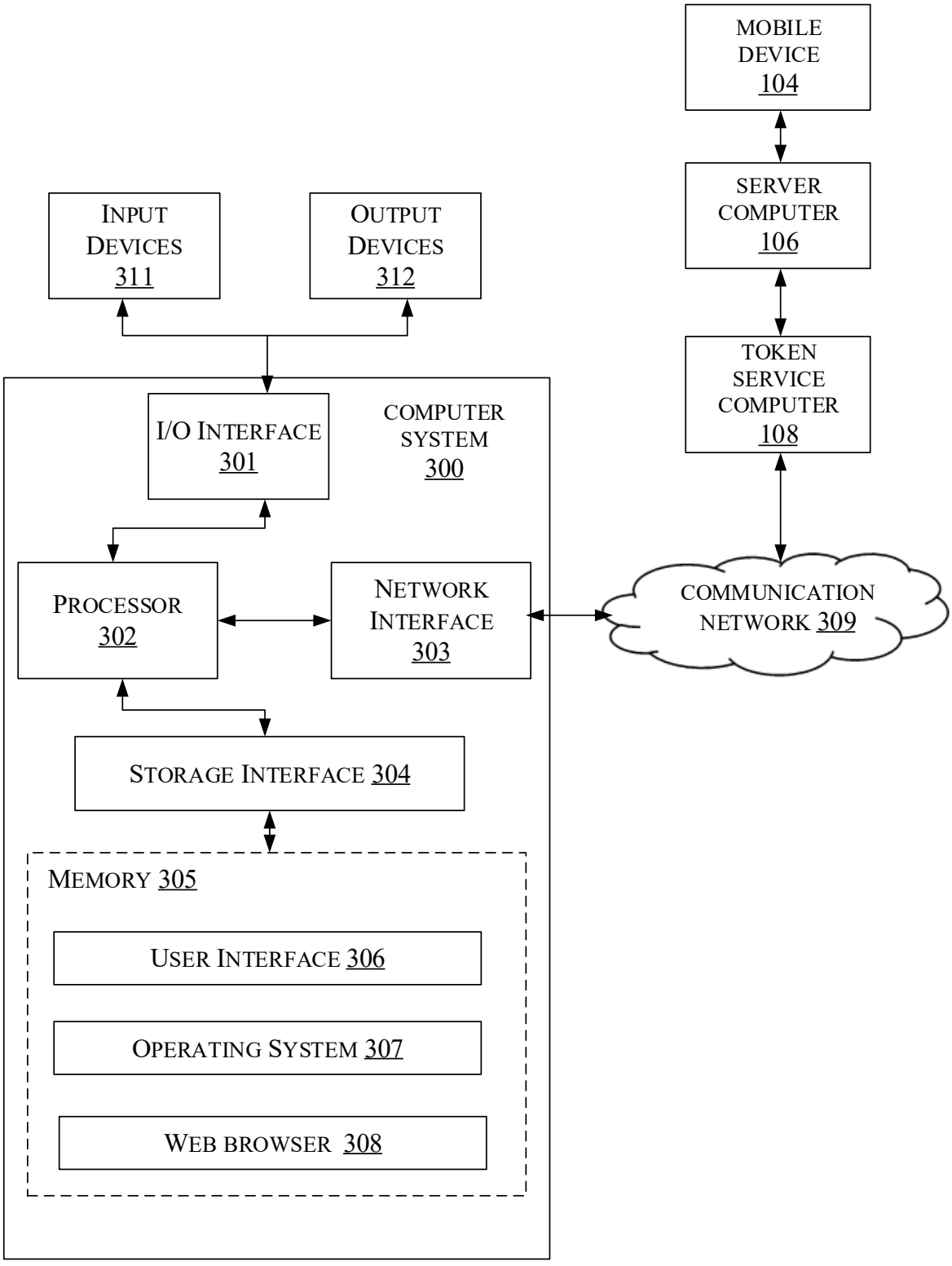
MOBILE DEVICE 104
SERVER COMPUTER 106
TOKEN SERVICE COMPUTER 108
INPUT DEVICES 311
OUTPUT DEVICES 312
COMPUTER SYSTEM 300
I/O INTERFACE 301
PROCESSOR 302
NETWORK INTERFACE 303
COMMUNICATION NETWORK 309
STORAGE INTERFACE 304
MEMORY 305
USER INTERFACE 306
OPERATING SYSTEM 307
WEB BROWSER 308

FIG. 3