(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
13 July 2017 (13.07.2017)

WIPO | PCT

(10) International Publication Number
WO 2017/118923 A1

(51) International Patent Classification:
G06Q 20/00 (2012.01) *G06F 17/30* (2006.01)
G06Q 20/32 (2012.01) *H04L 9/00* (2006.01)

(21) International Application Number:
PCT/IB2017/050016

(22) International Filing Date:
4 January 2017 (04.01.2017)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
201611000234 4 January 2016 (04.01.2016) IN

(71) Applicant: **COMVIVA TECHNOLOGIES LIMITED** [IN/IN]; A-26, Info City, Sector 34, Gurgaon, Haryana 122001 (IN).

(72) Inventors: **JAIN, Manish Kumar**; 43, Vasudha Enclave, Pitampura, Delhi 110034 (IN). **GOYAL, Gaurav**; 1251P, First Floor, Sector-15, Part-2, Gurgaon, Haryana 122001 (IN).

(74) Agent: **SINGH, Manisha**; LEXORBIS, 709/710, Tolstoy House, 15 – 17, Tolstoy Marg, New Delhi 110 001 (IN).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK,

[Continued on next page]

(54) Title: METHODS AND DEVICES FOR AUTHENTICATION OF AN ELECTRONIC PAYMENT CARD USING ELECTRONIC TOKENS

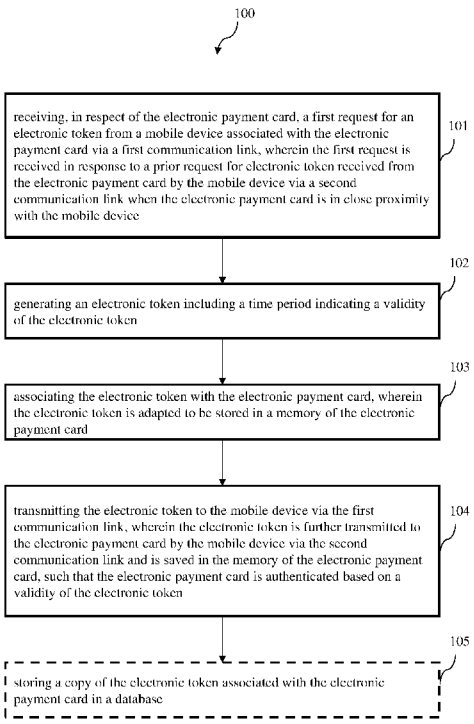

FIGURE 1a

(57) Abstract: The invention relates to method and system for authentication of an electronic payment card using electronic tokens in a payment network. A mobile device associated with the electronic payment card receives a request for electronic token when the electronic payment card is in proximity with the mobile device. In one embodiment, the mobile device transmits the request to a server for generating the electronic token. Upon generating the electronic token, the server transmits the electronic token to the mobile device. In another embodiment, the mobile device generates the electronic token. The mobile device then transmits the electronic token to the electronic payment card for storing in a memory of the electronic payment card such that electronic payment card is authenticated based on a validity of the electronic token.

WO 2017/118923 A1

SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*

— *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))*

Published:

— *with international search report (Art. 21(3))*

METHODS AND DEVICES FOR AUTHENTICATION OF AN ELECTRONIC PAYMENT CARD USING ELECTRONIC TOKENS

DESCRIPTION

TECHNICAL FIELD

The invention generally relates to financial transaction authentication. More particularly, the invention relates to authentication of a contactless card.

BACKGROUND

With advent of technology, proximity based payment or contactless payment has gained wide popularity in addition to Europay, MasterCard, and Visa (EMV) based payments. Example of such contactless payment includes near filed communication (NFC) based payments and radio frequency identification (RFID) based payments. In EMV based payments, cards such as credit card or debit card have secure elements or chips and are dipped into a reading device. For authenticating a transaction, authentication information such PIN is provided onto the card-reading device. On the other hand, in contactless payment, a reader device reads information from the card having the secure element when the card is in close proximity with the reader device over short-range wireless communication. As the cards can be read without a physical contact between the reader device and the contactless card, sharing of confidential authentication information such PIN and CVV number is not required during a transaction.

However, the information from card having the secure element (hereinafter referred to as electronic payment card) can be stolen using a malicious hardware/software component in the reader device. To overcome such security risk, in one technique, the reader device is authenticated prior to reading information from the electronic payment card. However, such authentication fails to prevent unauthorized transactions if the electronic payment card is stolen or lost. Generally, such unauthorized transactions are identified after the unauthorized transactions are processed completely and successfully. Consequently, a user of the electronic payment card is left with very few options such as hot-listing the card and destroying the electronic payment card. However, both the options permanently block the electronic payment cards from usage and require the user to opt for a new electronic payment card that is a time consuming and lengthy process.

In another technique, a one-time password (OTP) is generated during the transaction and sent to a mobile device associated with the electronic payment card. Upon receiving the OTP, the OTP is provided to the reader device. The transaction is completed only if the OTP sent to the mobile device matches with the OTP provided to the reader device. However, this technique fails when the mobile phone is cloned.

Various techniques are available for preventing unauthorized transactions and overcoming above deficiencies. In one technique, a set of OTPs are generated by a server and transmitted to the electronic payment card via the mobile device associated with the electronic payment card. The set of OTPs are then stored in the electronic payment card and used during authentication process. However, the set of OTPs fail to prevent unauthorized transactions if the electronic payment card is stolen. In another technique, token in form of a QR code is generated by a server and transmitted to the mobile device prior to transaction. During transaction, the token is transmitted to a merchant reader device and the transaction is completed if the token matches with the generated token. However, such technique fails if the mobile phone is cloned. In one another technique, a server maintains a mapping of the electronic payment card and dynamic security code, and sends a first security code to the mobile device. For authenticating a transaction made using the electronic payment card, the first security code present in the mobile device is provided. Upon successful authentication, the first security code is replaced with a second security code. The second security code is then sent to the mobile device for authenticating subsequent transaction. The second security code is sent when the mobile device is within a predefined range with the electronic payment card. In one embodiment, the server continually attempts to send the second security code until the second security code is successfully sent. In another embodiment, the server attempts to send the second security code only once. However, in this technique, such security code is visible and the chances of stealing the security code is high.

Thus, there exists a need to provide a better technique for preventing such unauthorized transactions using the electronic payment cards.

SUMMARY OF THE INVENTION

In accordance with the purposes of the invention, the present invention as embodied and broadly described herein, provides for enhancing security of electronic payment card in a payment network.

Accordingly, electronic payment card requests for an electronic token or e-token from a mobile device via a first communication link. The electronic payment card can be chip card or smart card having a secure element or chip. The first communication link is a proximity based communication link available between the mobile device and the electronic payment card. The request can be provided via various methods such as tapping the electronic payment card on the mobile device, touching the electronic payment card on the mobile device, and sweeping the electronic payment card over the mobile device.

In one embodiment, upon receiving the request, the mobile device transmits the request to a server via a second communication link. The second communication link is one of a data communication link and a non-data communication link available between the mobile device and the server. Upon receiving the request, the server generates an electronic token including time period indicating validity of the electronic token and transmits to the mobile device via the second communication link. In addition, the server saves a copy of the electronic token including the time period in a database. The mobile device then further transmits the electronic token to the electronic payment card via the second communication link such that the electronic payment card is authenticated based on a validity of the electronic token.

In another embodiment, upon receiving the request, the mobile device generates an electronic token including time period indicating validity of the electronic token. The mobile device then transmits the electronic token including the time period to the electronic payment card via the first communication link. In addition, the mobile device saves a copy of the electronic token including the time period in a memory. In yet another embodiment, the mobile device transmits a copy of the electronic token including the time period to the server via the second communication link. The server then stores the copy of the electronic token including the time period in the database.

Further, during a transaction using the electronic payment card, the server receives the stored electronic token from the electronic payment card. The server authenticates the electronic payment card by comparing with a copy of the electronic token associated with the electronic payment card. In one embodiment, the server obtains the copy of the electronic token corresponding to the electronic payment card from a database. In another embodiment, the server obtains the copy of the electronic token corresponding to the electronic payment card from the mobile device associated with the electronic payment card.

Upon obtaining the copy of the electronic token, the server authenticates the electronic payment card based on at least one of: validity of the copy of electronic token; comparison of the electronic token in the second request with the copy of electronic token; and time period indicated in the copy of electronic token.

The advantages of the invention include, but not limited to, enhanced security of the electronic payment cards by saving an electronic token, which is valid for a limited period, in the electronic payment card. By saving a limited validity electronic token in the electronic payment card, the security of the electronic payment card is greatly increased. This eliminates the chances of unauthorized transactions with the electronic payment card since an invalid token will prevent the completion of the transaction. Further, the electronic token is transmitted only upon receiving the request from the electronic payment card when the electronic payment card is in close proximity with the mobile device. The request can be received via various methods such as by way of tapping the electronic payment card on the mobile device, touching the electronic payment card on the mobile device and sweeping the electronic payment card over the mobile device. This further eliminates the chances of stealing the electronic token using a malicious device or software as the electronic payment card has to be in close proximity with the mobile device for receiving the electronic token.

Further, two-step security verification is provided during a transaction. Accordingly, in the first step verification, a determination is made if an electronic token is received from the electronic payment card. The transaction is prevented if the electronic token is not received. However, if the electronic token is received, second step verification is performed. In second step verification, a copy of electronic token associated with the electronic payment card is obtained. The transaction is allowed if the copy of electronic token is valid or time period indicated in the copy of electronic token is current with respect to the electronic token or the received electronic token matches with the copy of electronic token. As such, the security of the electronic payment card is greatly enhanced.

These and other aspects as well as advantages will be more clearly understood from the following detailed description taken in conjunction with the accompanying drawings and claims.

BRIEF DESCRIPTION OF THE ACCOMPANYING DRAWINGS:

To further clarify advantages and aspects of the invention, a more particular description of the invention will be rendered by reference to specific embodiments thereof, which is illustrated in the appended drawings. It is appreciated that these drawings depict only typical embodiments of the invention and are therefore not to be considered limiting of its scope. The invention will be described and explained with additional specificity and detail with the accompanying drawings, which are listed below for quick reference.

Figures 1a & 1b illustrate an exemplary method implemented by a server for communicating electronic token to an electronic payment card, in accordance with an embodiment of present invention.

Figure 2 illustrates an exemplary method implemented by a mobile device for communicating electronic token to an electronic payment card, in accordance with an embodiment of present invention.

Figures 3a & 3b illustrate an exemplary method implemented by a mobile device for communicating electronic token to an electronic payment card, in accordance with another embodiment of present invention.

Figure 4 illustrates an exemplary server communicating electronic token to an electronic payment card, in accordance with an embodiment of present invention.

Figure 5 illustrates an exemplary mobile device communicating electronic token to an electronic payment card, in accordance with an embodiment of present invention.

Figure 6 schematically illustrates an exemplary payment networked environment that implements a mobile device and a server for communicating electronic token to an electronic payment card, in accordance with an embodiment of the present invention.

Figure 7 illustrates a flow diagram for communicating electronic token to an electronic payment card by a server, in accordance with an embodiment of present invention.

Figure 8 illustrates a flow diagram for communicating electronic token to an electronic payment card by a mobile device, in accordance with an embodiment of present invention.

Figure 9 illustrates a flow diagram for authentication of an electronic payment card in respect of a transaction, in accordance with an embodiment of present invention.

It may be noted that to the extent possible, like reference numerals have been used to represent like elements in the drawings. Further, those of ordinary skill in the art will appreciate that elements in the drawings are illustrated for simplicity and may not have been necessarily drawn to scale. For example, the dimensions of some of the elements in the drawings may be exaggerated relative to other elements to help to improve understanding of aspects of the invention. Furthermore, the one or more elements may have been represented in the drawings by conventional symbols, and the drawings may show only those specific details that are pertinent to understanding the embodiments of the invention so as not to obscure the drawings with details that will be readily apparent to those of ordinary skill in the art having benefit of the description herein.

DETAILED DESCRIPTION

It should be understood at the outset that although illustrative implementations of the embodiments of the present disclosure are illustrated below, the present invention may be implemented using any number of techniques, whether currently known or in existence. The present disclosure should in no way be limited to the illustrative implementations, drawings, and techniques illustrated below, including the exemplary design and implementation illustrated and described herein, but may be modified within the scope of the appended claims along with their full scope of equivalents.

The term "some" as used herein is defined as "none, or one, or more than one, or all." Accordingly, the terms "none," "one," "more than one," "more than one, but not all" or "all" would all fall under the definition of "some." The term "some embodiments" may refer to no embodiments or to one embodiment or to several embodiments or to all embodiments. Accordingly, the term "some embodiments" is defined as meaning "no embodiment, or one embodiment, or more than one embodiment, or all embodiments."

The terminology and structure employed herein is for describing, teaching and illuminating some embodiments and their specific features and elements and does not limit, restrict or reduce the spirit and scope of the claims or their equivalents.

More specifically, any terms used herein such as but not limited to "includes," "comprises," "has," "consists," and grammatical variants thereof do NOT specify an exact

limitation or restriction and certainly do NOT exclude the possible addition of one or more features or elements, unless otherwise stated, and furthermore must NOT be taken to exclude the possible removal of one or more of the listed features and elements, unless otherwise stated with the limiting language "MUST comprise" or "NEEDS TO include."

Whether or not a certain feature or element was limited to being used only once, either way it may still be referred to as "one or more features" or "one or more elements" or "at least one feature" or "at least one element." Furthermore, the use of the terms "one or more" or "at least one" feature or element do NOT preclude there being none of that feature or element, unless otherwise specified by limiting language such as "there NEEDS to be one or more . . . " or "one or more element is REQUIRED."

Unless otherwise defined, all terms, and especially any technical and/or scientific terms, used herein may be taken to have the same meaning as commonly understood by one having an ordinary skill in the art.

Reference is made herein to some "embodiments." It should be understood that an embodiment is an example of a possible implementation of any features and/or elements presented in the attached claims. Some embodiments have been described for the purpose of illuminating one or more of the potential ways in which the specific features and/or elements of the attached claims fulfil the requirements of uniqueness, utility and non-obviousness.

Use of the phrases and/or terms such as but not limited to "a first embodiment," "a further embodiment," "an alternate embodiment," "one embodiment," "an embodiment," "multiple embodiments," "some embodiments," "other embodiments," "further embodiment", "furthermore embodiment", "additional embodiment" or variants thereof do NOT necessarily refer to the same embodiments. Unless otherwise specified, one or more particular features and/or elements described in connection with one or more embodiments may be found in one embodiment, or may be found in more than one embodiment, or may be found in all embodiments, or may be found in no embodiments. Although one or more features and/or elements may be described herein in the context of only a single embodiment, or alternatively in the context of more than one embodiment, or further alternatively in the context of all embodiments, the features and/or elements may instead be provided separately or in any appropriate combination or not at all. Conversely, any features

and/or elements described in the context of separate embodiments may alternatively be realized as existing together in the context of a single embodiment.

Any particular and all details set forth herein are used in the context of some embodiments and therefore should NOT be necessarily taken as limiting factors to the attached claims. The attached claims and their legal equivalents can be realized in the context of embodiments other than the ones used as illustrative examples in the description below.

Figures 1a & 1b illustrate an exemplary method (100) implemented by a server for communicating electronic token to an electronic payment card, in accordance with an embodiment of present invention. In said embodiment, referring to **Figure 1a**, at step (101), a first request for an electronic token is received from a mobile device associated with the electronic payment card via a first communication link. The first request is received in response to a prior request for electronic token received from the electronic payment card by the mobile device via a second communication link when the electronic payment card is in close proximity with the mobile device.

At step (102), an electronic token including a time period indicating a validity of the electronic token is generated.

At step (103), the electronic token is associated with the electronic payment card, wherein the electronic token is adapted to be stored in a memory of the electronic payment card.

At step (104), the electronic token is transmitted to the mobile device via the first communication. The electronic token is further transmitted to the electronic payment card by the mobile device via the second communication link and is saved in the memory of the electronic payment card, such that the electronic payment card is authenticated based on a validity of the electronic token.

Further, the electronic payment card is one of: a credit card, a debit card, an automated teller machine (ATM) card, a fleet card, stored-value card, prepaid card, and a gift card.

Further, the first communication link is independent of the second communication link, the first communication link being one of a data communication link and a non-data

communication link available between the mobile device and the server, and the second communication link being a proximity based communication link available between the mobile device and the electronic payment card.

Further, the first request is received via an application available in a memory of the mobile device over the first communication link.

Further, the prior request for electronic token is received from the electronic payment card by the application via the second communication link.

Further, the electronic token is an encrypted key of configurable length.

In addition, at step (105), a copy of the electronic token associated with the electronic payment card is stored in a database.

Referring to **Figure 1b**, at step (106), a second request to authenticate the electronic payment card in respect of a transaction initiated using the electronic payment card is received from a designated intermediary device.

At step (107), availability of an electronic token in the second request is determined. The electronic token is being sent by the electronic payment card to the designated intermediary device.

At step (108), upon determination, a copy of an electronic token associated with the electronic payment card is obtained.

At step (109), a response to the mobile device associated with the electronic payment card and the designated intermediary device is transmitted based on at least one of: validity of the copy of electronic token; comparison of the electronic token in the second request with the copy of electronic token; and time period indicated in the copy of electronic token.

Further, the copy of the electronic token associated with the electronic payment card is obtained from a database, the database being adapted to store the copy of the electronic token.

In addition, at step (110), the copy of electronic token is set as invalid for further request to authenticate the electronic payment card in respect of one or more further transactions initiated using the electronic payment card.

Figure 2 illustrates an exemplary method (200) implemented by a mobile device for communicating electronic token to an electronic payment card, in accordance with an embodiment of present invention. In said embodiment, referring to **Figure 2**, at step (201), a first request for an electronic token from an electronic payment card associated with the mobile device is received via a first communication link. The first request is received in when the electronic payment card is in close proximity with the mobile device.

At step (202), an electronic token including a time period indicating a validity of the electronic token is generated.

At step (203), the electronic token is associated with the electronic payment card, wherein the electronic token is adapted to be stored in a memory of the electronic payment card.

At step (204), the electronic token is transmitted to the electronic payment card via the first communication link such that electronic token is stored in the memory of the electronic payment card.

At step (205), a copy of the electronic token is transmitted to a server via a second communication link, such that the server based on a validity of the electronic token authenticates the electronic payment card.

Further, the electronic payment card is one of: a credit card, a debit card, an automated teller machine (ATM) card, a fleet card, stored-value card, prepaid card, and a gift card.

Further, the first request is received through an application available in the memory of the mobile device via the first communication link.

Further, the first communication link is independent of the second communication link, the first communication link being a proximity based communication link available between the mobile device and the electronic payment card, and the second communication link being one of a data communication link and a non-data communication link available between the mobile device and the server.

Further, the electronic token is a encrypted key of configurable length.

In addition, at step (206), response from the server is received through the application via the second communication link based on at least one of: validity of the copy of electronic token; comparison of an electronic token received in the second request with the copy of electronic token, the electronic token being sent by the electronic payment card to the server; and time period indicated in the copy of electronic token.

Figures 3a & 3b illustrate an exemplary method (300) implemented by a mobile device for communicating electronic token to an electronic payment card, in accordance with another embodiment of present invention. In said embodiment, referring to **Figure 3a**, at step (301) a first request for an electronic token is received from the electronic payment card associated with the mobile device via a first communication link. The first request is received in when the electronic payment card is in close proximity with the mobile device.

At step (302), the electronic token including a time period indicating a validity of the electronic token is generated.

At step (303), the electronic token is associated with the electronic payment card, wherein the electronic token is adapted to be stored in a memory of the electronic payment card.

At step (304), a copy of the electronic token associated with the electronic payment card is stored in a memory.

At step (305), the electronic token is transmitted to the electronic payment card via the first communication link such that electronic token is stored in the memory of the electronic payment card, wherein the electronic payment card is authenticated based on a validity of the electronic token.

Further, the first request is received through an application available in the memory of the mobile device via the first communication link.

Referring to **Figure 3b**, at step (306), a second request for an electronic token associated with the electronic payment card is received from a server through an application via a second communication link. The second request corresponding to authentication of the electronic payment card in respect of a transaction initiated using the electronic payment card.

At step (307), a copy of the electronic token associated with the electronic payment card is fetched from a memory.

At step (308), the copy of the electronic token associated with the electronic payment card is transmitted to the server through the application via the second communication link.

At step (309), a response is received from the server based on at least one of: validity of the copy of electronic token; comparison of an electronic token received in the second request with the copy of electronic token, the electronic token being sent by the electronic payment card to the server; and time period indicated in the copy of electronic token. The response is received through the application via the second communication link.

Further, the first communication link is independent of the second communication link, the first communication link being a proximity based communication link available between the mobile device and the electronic payment card, and the second communication link being one of a data communication link and a non-data communication link available between the mobile device and the server.

Figure 4 illustrates an exemplary server (400) communicating electronic token to an electronic payment card, in accordance with an embodiment of present invention. As would be understood, the server (400) is capable of implementing the methods as described with reference to preceding Figures 1a and 1b.

In said embodiment, the server (400) comprises a first receiving unit (401) adapted to receive, in respect of the electronic payment card, a first request for an electronic token from a mobile device associated with the electronic payment card via a first communication link. The first request is received in response to a prior request for electronic token received from the electronic payment card by the mobile device via a second communication link when the electronic payment card is in close proximity with the mobile device. The first communication link is independent of the second communication link. The first communication link is one of a data communication link and a non-data communication link available between the mobile device and the server. The second communication link being a proximity based communication link available between the mobile device and the electronic payment card.

Further, the electronic payment card is one of: a credit card, a debit card, an automated teller machine (ATM) card, a fleet card, stored-value card, prepaid card, and a gift card.

The server (400) further comprises a processing unit (402) coupled to the first receiving unit (401) and adapted to generate an electronic token including a time period indicating a validity of the electronic token. The electronic token is an encrypted key of configurable length.

The processing unit (402) is further adapted to associate the electronic token with the electronic payment card, wherein the electronic token is adapted to be stored in a memory of the electronic payment card. The processing unit (402) is further adapted to stores a copy of the electronic token associated with the electronic payment card in a database (404) communicatively coupled to the server (400).

The server (400) further comprises a transmitting unit (403) coupled to the processing unit (402). The transmitting unit (403) is adapted to transmit the electronic token to the mobile device via the first communication link. The electronic token is then further transmitted to the electronic payment card by the mobile device via the second communication link and is saved in the memory of the electronic payment card, such that the electronic payment card is authenticated based on a validity of the electronic token.

The server (400) further comprises a second receiving unit (405) coupled to the processing unit (402). The second receiving unit (405) is adapted to receive, from a designated intermediary device, a second request to authenticate the electronic payment card in respect of a transaction initiated using the electronic payment card.

The server (400) further comprises an analysis unit (406) coupled to the second receiving unit (405). The analysis unit (406) is adapted to determine availability of an electronic token in the second request, the electronic token being sent by the electronic payment card to the designated intermediary device. Upon determining, the analysis unit (406) is further adapted to obtain a copy of an electronic token associated with the electronic payment card. The analysis unit (406) obtains a copy of the electronic token associated with the electronic payment card from the database (404), which stores the copy of the electronic token

Thereafter, the analysis unit (406) is further adapted to transmit a response to the mobile device associated with the electronic payment card and the designated intermediary device. The analysis unit (406) provides the response based on at least one of: validity of the copy of electronic token; comparison of the electronic token in the second request with the copy of electronic token; and time period indicated in the copy of electronic token. Accordingly, the server (400) further comprises a message generating unit (407) adapted to generate the response based on the validation.

The analysis unit (406) is further adapted to set the copy of electronic token as invalid for further request to authenticate the electronic payment card in respect of one or more further transactions initiated using the electronic payment card.

Additionally, the server (400) may include a memory (408) adapted to store the outputs of each of the previously mentioned units. In addition, the server (400) may include a bus system (not shown in the figure) for enabling communication between the various units, and communication interface (not shown in the figure) and network interface unit (not shown in the figure) for receiving inputs over one or more different networks. Further, it would be understood that in one embodiment the above-mentioned functions of various units can be performed by a single unit.

It would be understood, that the processing unit (402) may include various hardware modules/units/components or software modules or a combination of hardware and software modules as necessary for implementing the invention. Further, the analysis unit (406) may be implemented using hardware components or software components or combination of both. In one embodiment, the analysis unit (406) and the processing unit (402 may form a single unit/module.

Although specific hardware components have been depicted in reference to the server (400), it is to be understood that the server (400) and the various components therein may include other hardware components and/or software components as known in the art for performing necessary functions.

Figure 5 illustrates an exemplary mobile device (500) communicating electronic token to an electronic payment card, in accordance with an embodiment of present invention. As would be understood, the mobile device (500) is capable of implementing the methods as described with reference to preceding Figures 2, 3a, and 3b

In one embodiment, the mobile device (500) comprises a first receiving unit (501) adapted to receive a first request for an electronic token from an electronic payment card associated with the mobile device (500) via a first communication link. The first request is received when the electronic payment card is in close proximity with the mobile device. The first communication link is a proximity based communication link available between the mobile device and the electronic payment card. Further, the electronic payment card is one of: a credit card, a debit card, an automated teller machine (ATM) card, a fleet card, stored-value card, prepaid card, and a gift card.

The mobile device (500) further comprises a processing unit (502) coupled to the first receiving unit (501). The processing unit (502) is adapted to generate an electronic token including a time period indicating a validity of the electronic token. The processing unit (502) is further adapted to associate the electronic token with the electronic payment card, wherein the electronic token is adapted to be stored in a memory of the electronic payment card. The electronic token is an encrypted key of configurable length.

The mobile device (500) further comprises a transmitting unit (503) coupled to the processing unit (502). The transmitting unit (503) is adapted to transmit the electronic token to the electronic payment card via the first communication link such that electronic token is stored in the memory of the electronic payment card (605). Further, the transmitting unit (503) is adapted to transmit a copy of the electronic token to a server via a second communication link, such that the server based on a validity of the electronic token authenticates the electronic payment card.

Further, the first communication link is independent of the second communication link. The first communication link is a proximity based communication link available between the mobile device and the electronic payment card. The second communication link is one of a data communication link and a non-data communication link available between the mobile device (500) and the server.

The mobile device (500) further includes a memory (504). The memory (504) includes an application (505) adapted to receive the first request from the electronic payment card via the first communication link.

The mobile device (500) further includes a second receiving unit (506) adapted to receive response from the server. The server provides the response based on at least one of:

validity of the copy of electronic token; comparison of an electronic token received in the second request with the copy of electronic token, the electronic token being sent by the electronic payment card to the server; and time period indicated in the copy of electronic token. The second receiving unit (506) is adapted to receive the response through the application (505) via the second communication link.

In another embodiment, upon generating the electronic token, the processing unit (502) stores a copy of the electronic token (507) in the memory (504). In such embodiment, the transmitting unit (503) excludes transmitting the copy of the electronic token to the server via the second communication link. The transmitting unit (503) only transmits the electronic token to the electronic payment card after the processing unit (502) generates the electronic token.

Further, in such embodiment, the second receiving unit (506) is further adapted to receive, through the application (505) via the second communication link, a second request for an electronic token associated with the electronic payment card from a server. The second request corresponding to authentication of the electronic payment card in respect of a transaction initiated using the electronic payment card. Upon receiving the request, the processing unit (502) fetches a copy of the electronic token (507) associated with the electronic payment card from the memory (504). Accordingly, the transmitting unit (503) is further adapted to transmit, through the application (505) via the second communication link, the copy of the electronic token associated with the electronic payment card to the server. Thereafter, the second receiving unit (506) receives response from the server. The server provides the response based on at least one of: validity of the copy of electronic token; comparison of an electronic token received in the second request with the copy of electronic token, the electronic token being sent by the electronic payment card to the server; and time period indicated in the copy of electronic token. The second receiving unit (506) receives the response through the application (505) via the second communication link.

Figure 6 schematically illustrates an exemplary payment networked environment (600) that implements the mobile device (500) and the server (400) for communicating electronic token to an electronic payment card, in accordance with an embodiment of the present invention.

Accordingly, the payment networked environment (600) includes a plurality of issuer systems (601-1, 601-2, ...601-N), (hereinafter referred to as issuer system (601) indicating one issuer system and issuer systems (601) indicating a plurality of issuer systems) corresponding to plurality of issuers such as banks and merchants. The issuers, among various other services, issue one or more electronic payment cards to a user for conducting financial transactions such as purchase transactions and banking transactions. Examples of the issuer systems (601) include systems employed by banks and merchants. The issuer systems (601) are communicatively coupled with the server (400) over a network (602). In an example, the issuer systems (601) are registered with the server (400). Examples of the network (602) include wireless network, wired network, and cloud based network.

Further, the network environment (600) includes a plurality of point of transaction (POT) systems (603-1, 603-2, ...603-N), (hereinafter referred to as POT system (603) indicating one POT system and POT systems (603) indicating a plurality of POT systems). The POT system (603) enables the user to perform financial transactions using the one or more electronic payment cards issued to the user by the issuers. Examples of the POT system (603) include point of sale (POS) systems and automated teller machines (ATMs), where the user engages in a financial transaction. The POT systems (603) are communicatively coupled with issuer systems (601) over the network (602). Further, the POT systems (603) may be coupled with other systems (not shown in the figure) such as inventory systems, catalogue systems, customer relationship management (CRM) system, and bill processing systems, as well as third party systems over the network (602).

Further, the server (400) is coupled with the mobile device (500) over a first communication link (604). Examples of the first communication link (604) include data communication link and non-data communication link. The server (400) provides various services to users for managing their financial equipment such as electronic payment cards. Examples of the electronic payment cards include a credit card, a debit card, an automated teller machine (ATM) card, a fleet card, stored-value card, prepaid card, and a gift card. One such service includes authentication of electronic payment cards to enhance their security. For accessing the service, a user registers with the server (400) via the application (505) installed in the mobile device (500). In one example, the user downloads the application (505) from the server (400) onto the mobile device (500). In another example, the

application (505) is preinstalled on the mobile device (500) at the time of manufacturing. The registration of the user includes registration of a mobile number or Mobile Station International Subscriber Directory Number (MSISDN) of the mobile device (500) with the server (400) along with details of the user such as name and address. The server (400) stores the details in the database (404).

Additionally, in one aspect, the server (400) may perform validation of the user during registration. The validation may performed using methods known in the art, such as transmitting one-time password (OTP), captcha, and requesting for other user-details. Further, during registration, an encryption technique is agreed between the server (400) and mobile device (500). Accordingly, details of the encryption technique are saved with the application (505).

Upon registering with the server (400), the user registers one or more electronic payment cards (605-1, 605-2, ...605-N) (hereinafter referred to as electronic payment card (605) indicating one electronic payment card and electronic payment cards (605) indicating a plurality of electronic payment cards) with the server (400) via the application (505). It would be understood that the associated electronic payment cards might be issued to the user by one issuer or by multiple issuers. The association of the one or more electronic payment cards (605) may include providing details of the associated electronic payment card (605) and the corresponding issuer issuing the associated electronic payment card (605). Thereafter the association is performed as known in the art. In an example, the association includes mapping the details of the associated electronic payment card (605) with the corresponding issuer and the MSISDN of the mobile device (500). As would be understood, the MSISDN of the mobile device (500) is same as registered with the issuer of the electronic payment card (605).

The server (400) then stores the details of the associated electronic payment cards (605) and the mobile device (500) in the database (404). In an example, a flag is set to indicate the association of the electronic payment cards (605). In addition, the server (400) shares association details with the issuer systems (601) of the corresponding issuers. The association details are indicative that the server (400) will perform authentication of the associated electronic payment cards (605). In the example above, the server (400) shares information regarding the setting of the flag for each of the associated electronic payment cards (605) with the issuer systems (601) of the corresponding issuer of the associated

electronic payment card (605). The issuer systems (601) save the association details in a database (not shown in the figure). In an example, the issuer system (601) saves a list of associated electronic payment cards (605) along with the flag details in the database. Thus, upon receiving information of a transaction using the associated electronic payment card (605), the issuer system (601) sends a validation request to the server (400) based on the association details, as will be described in subsequent Figures and paragraphs.

Furthermore, the electronic payment card (605) includes a secure element (606), such as a chip, embedded within the electronic payment card (605). Thus, the electronic payment card (605) can be a chip card or a smart card. The secure element (606) is adapted to use short range wireless communication for secure data communication. Examples of the short range wireless include, but not limited to, Wireless Fidelity (Wi-Fi), Near Field Communication (NFC), Bluetooth, Bluetooth Low Energy (BLE), Zigbee, Wi-Fi Direct (WFD), and Ultra Wideband (UWB). The secure element (606) includes various components (not shown in the figure) such as a power supply module, short range wireless communication module, memory module, a processing unit, and a communication bus system. The memory module stores details of the electronic payment card (605) such as account number, user identification details, user verification number, account balance information, and transaction record information. In an example, the short range wireless communication module is a NFC sensor, which may further include a transceiver module and an antenna module. The short range wireless communication sensor enables communication of such data when the electronic payment card (605) is in proximity with short range wireless communication enabled devices.

In said embodiment, the mobile device (500) and the electronic payment card (605) are communicatively coupled with each other via a second communication link (607). The second communication link (606) is a proximity based communication link, and therefore is independent of the first communication link (604) available between the mobile deice (500) and the server (400). Examples of the proximity based communication link include, but not limited to, Wireless Fidelity (Wi-Fi), Near Field Communication (NFC), Bluetooth, Bluetooth Low Energy (BLE), Zigbee, Wi-Fi Direct (WFD), and Ultra Wideband (UWB). Accordingly, the mobile device (500) includes an electronic payment module (not shown in the figure), which is adapted to use proximity based communication protocols for secure data communication. The electronic payment module is pre-installed in the mobile device

(500) by a manufacturer of the mobile device (500). The electronic payment module is adapted to communicate with the secure element (606) of the electronic payment card (605) via the second communication link (607) when the electronic payment card (605) is in close proximity to the mobile device (400). The communication with the secure element (606) is enabled when the electronic payment card (605) and the mobile device (500) are within a predefined range. In the present embodiment, the electronic payment module can be implemented with the first receiving unit (501) for receiving input and can also be implemented with the transmitting unit (503) for transmitting output via the a second communication link (607).

Furthermore, the electronic payment card (605) interacts with the POT system (603) when a financial transaction is initiated using the electronic payment card (605) by the user. Examples of the transaction include banking transaction at ATM and purchase transaction at POS system. In one aspect, the electronic payment card (605) interacts with the POT system (603) via the second communication link (607). Accordingly, the secure element (606) transmits details of the electronic payment card (605) such as card number, card validity period, and issuer name, to the POT system (603) via the second communication link (607). In another aspect, the electronic payment card (605) interacts with the POT system (603) by way of physical contact such as inserting or dipping the electronic payment card (605) interacts in the POT system (603).

Figure 7 illustrates the operations (700) performed by the server (400) to transmit an electronic token to the electronic payment card (605), in accordance with an embodiment of present invention.

Referring to **Figures 4, 5, and 6 along with Figure 7**, at step 701 the user sends a request for an electronic token to the mobile device (500). The user sends the request through the electronic payment card (605) via the second communication link (607) when the electronic payment card (605) is in close proximity to the mobile device. In an example, the user can tap the electronic payment card (605) on the mobile device (500). In another example, the user can sweep the electronic payment card (605) on the mobile device (500). In yet another example, the user can touch the electronic payment card (605) on the mobile device (500). Consequently, when the electronic payment card (605) is in close proximity to the mobile device, the secure element (606) of the electronic payment card (605) communicates with the first receiving unit (501) over the second communication link (607)

and transmits the request via to electronic payment module. The request includes an identifier indicating generation of electronic token and details of the electronic payment card (605) such as card number. As would be understood, at a given time, one electronic payment card can be used to send the request for the electronic token. Upon receiving the request, the electronic payment module forwards the request to the application (505) based on the identifier.

At step 702, the second receiving unit (506) sends the request to the server (400) through the application (505) via the first communication link (604). The request includes details of the electronic payment card (605) such as card number and mobile number.

At step 703, the first receiving unit (401) of the server (400) receives the request. Upon receiving the request, the processing unit (402) generates an electronic token. The electronic token is generated using techniques known in the art. The electronic token is an encrypted key of configurable length. In one aspect, the length is changed periodically to enhance the security. Further, the key includes alphanumerical characters and is generated using methods known in the art. The key is encrypted using the encryption technique pre-agreed with the mobile device (500).

Further, the electronic token includes a time period indicating a validity of the electronic token. The time period is predetermined and is of very short duration comprising of few seconds. In an example, the predetermined duration is 20 seconds. The time period is determined from the time of generation of the electronic token. Thus, the electronic token gets invalidated upon expiry of the time period.

Upon generating the electronic token, the processing unit (402) associates the electronic token with the electronic payment card (605). In an example, the processing unit (402) associates the electronic token by mapping the electronic token with the card number as received in the request from the application (505).

At step 704, the processing unit (402) saves a copy of the electronic token in the database (404) along with the association details.

At step 705, the transmitting unit (403) transmits the generated electronic token including the time period to the mobile device (500) via the first communication link (604).

At step 706, upon receiving the generated electronic token including the time period, the application (505) transmits the generated electronic token to the electronic payment card (605). As described earlier, the second receiving unit (506) receives the generated electronic token through the application (505) via the first communication link (604). Upon receiving, the application (505) transmits the generated electronic token to the contactless module. The transmitting unit (503) then transmits the generated electronic token including the time period to the electronic payment card (605) via the second communication link (607). Upon receiving the generated electronic token including the time period, the secure element (606) stores the generated electronic token including the time period in the memory.

Figure 8 illustrates the operations (800) performed by the mobile device (500) to transmit an electronic token to the electronic payment card (605), in accordance with another embodiment of present invention.

Referring to **Figures 4, 5, and 6 along with Figure 8**, at step 801 the user sends a request for an electronic token to the mobile device (500). The user sends the request through the electronic payment card (605) via the second communication link (607) when the electronic payment card (605) is in close proximity to the mobile device. In an example, the user can tap the electronic payment card (605) on the mobile device (500). In another example, the user can sweep the electronic payment card (605) on the mobile device (500). In yet another example, the user can touch the electronic payment card (605) on the mobile device (500). Consequently, when the electronic payment card (605) is in close proximity to the mobile device, the secure element (606) of the electronic payment card (605) communicates with the first receiving unit (501) over the second communication link (607) and transmits the request to the electronic payment module. The request includes an identifier indicating generation of electronic token and details of the electronic payment card (605) such as card number. As would be understood, at a given time, one electronic payment card can be used to send the request for the electronic token. Upon receiving the request, the electronic payment module (608) forwards the request to the application (505) based on the identifier.

At step 802, the processing unit (502) generates an electronic token via the application (505). The electronic token is generated using techniques known in the art. The electronic token is an encrypted key of configurable length. The length is pre-stored in the application (505) during the registration process of the mobile device (500) with the server

(400). In one aspect, the length is changed periodically to enhance the security. In such aspect, the server (400) periodically transmits the length to the mobile device (500) periodically. Further, the key includes alphanumerical characters and is generated using methods known in the art. The key is encrypted using the encryption technique pre-agreed with the mobile device (500).

Further, the electronic token includes a time period indicating a validity of the electronic token. The time period is predetermined and is of very short duration comprising of few seconds. In an example, the predetermined duration is 20 seconds. The time period is determined from the time of generation of the electronic token. Thus, the electronic token gets invalidated upon expiry of the time period.

Upon generating the electronic token, the processing unit (502) associates the electronic token with the electronic payment card (605). In an example, the processing unit (502) associates the electronic token by mapping the electronic token with the card number as received in the request.

At step 803, the application (505) transmits the generated electronic token to the electronic payment module for transmitting to the electronic payment card (605). As such, the transmitting unit (503) transmits the generated electronic token including the time period to the electronic payment card (605) via the second communication link (607). Upon receiving the generated electronic token including the time period, the secure element (606) stores the generated electronic token including the time period in the memory.

In one embodiment, at step 804, the transmitting unit (503) further transmits a copy of the electronic token to the server (400) through the application (505) via the first communication link (604). The transmitting unit (503) also transmits the association details along with the copy of the electronic token. Further, at step 805, the server (400) saves the copy of the electronic token in the database (404) along with the association details.

In another embodiment, upon generating the electronic token, the processing unit (502) stores a copy of the electronic token (507) in the memory (504). In such embodiment, the transmitting unit (503) excludes transmitting the copy of the electronic token to the server (400) via the first communication link (604).

Thus, by saving an electronic token, which is valid for limited time period, in the electronic payment card (605), the security of the electronic payment card (605) is greatly

increased. This eliminates the chances of unauthorized transactions with the electronic payment card (605) since an invalid token will prevent the completion of the transaction. Further, the electronic token is transmitted only upon receiving the request from the electronic payment card when the electronic payment card is in close proximity with the by the mobile device. This further eliminates the chances of stealing the electronic token using a malicious device or software.

Figure 9 illustrates the operations performed by the server (400) during a transaction initiated by an electronic payment card, in accordance with an embodiment of present invention.

Referring to **Figures 4, 5, and 6 along with Figure 9a**, at step 901, the secure element (606) of the electronic payment card (605) transmits details of the electronic payment card (605) to the POT system (603) when a financial transaction is initiated using the electronic payment card (605) by the user. In one aspect of the invention, the secure element (606) transmits the details via the second communication link (607). In another aspect of the invention, the electronic payment card (605) interacts with the POT system (603) by way of physical contact such as inserting or dipping the electronic payment card (605) interacts in the POT system (603). Examples of the transaction include banking transaction at ATM and purchase transaction at POS system. Further, if an electronic token is saved in the memory of the electronic payment card (605), the secure element transmits the electronic token along with the details of the electronic payment card (605).

At step 902, the POT system (603) transmits a validation request to the issuer system (601). The validation request includes authentication credentials of the POT system (603), transaction information, and card identifier data indicating details about the electronic payment card (605). In addition to the validation request, the POT system (603) may also transmit authentication credentials such as PIN and Password associated with the electronic payment card and known only to the user. Further, if the electronic token is received from the electronic payment card (605), the validation request includes the received electronic token.

At step 903, upon receiving the validation request, the issuer system (601) determines if the electronic payment card (605) is one of the associated electronic payment cards (605). In an example, the issuer system (601) retrieves the list of associated electronic payment cards (605) along with flag details from a database and determines if the electronic

payment card is one of the associated electronic payment cards (605) based on the flag details. If the flag is set, the electronic payment card (605) is determined as the associated electronic payment card for which the server (400) performs the authentication. Thereafter, the issuer system (601), acting as a designated intermediary device, forwards the validation request to the server (400).

On the contrary, if the flag is not set, the electronic payment card (605) is determined as not being one of the associated electronic payment cards. Consequently, the issuer system (601) will not send the validation request to the server (400). Thereafter, the issuer system (601) performs validation of the electronic payment card (605) in a manner as known in the art. In an example, the issuer system (601) validates the authentication credentials received along with the validation request.

At step 904, upon receiving the validation request, the analysis unit (406) determines availability of an electronic token in the validation request. If the electronic token is not available in the validation request, the analysis unit (406) prevents the completion of the transaction. Accordingly, the message generating unit (407) generates a failure message indicative of the invalid authentication of the electronic payment card (605) in respect of the transaction. In addition to the failure message, the message generating unit (407) generates an alert message for the user. The alert message indicates details about the transaction and invalid authentication of the electronic payment card (605) in respect of the transaction.

At step 905, the transmitting unit (403) of the server (400) transmits the failure message to the designated intermediary device, i.e., issuer system (601) over the network (602). Upon receiving the failure message, the issuer system (601) prevents the processing of the transaction as known in the art. In examples, the banking transaction at ATM and purchase transaction at POS system are prevented from completion.

At step 906, upon preventing the transaction, the issuer system (601) transmits a transaction unsuccessful message to the POT system (603). Upon receiving the transaction unsuccessful message, the POT system (603) may display an appropriate message on a display unit (not shown in the figure) of the POT system (603). In addition, the issuer system (601) transmits a transaction unsuccessful message to the user as known in the art. In an example, the issuer system (601) transmits the transaction unsuccessful message to the mobile device (500).

At step 907, the transmitting unit (403) of the server (400) transmits the alert message to the mobile device (500) via the first communication link (604). Accordingly, the second receiving unit (506) receives the alert message through the application (505) and displays on a display unit (not shown in the figure) of the mobile device (500). Examples of the alert message include SMS message, USSD message, and a flash message.

However, if at step 904, the availability of the electronic token is determined in the validation request, then the process flows to step 908 in Figure 9b.

Referring to **Figures 4, 5, and 6 along with Figure 9b**, at step 908, upon receiving the validation request, the analysis unit (406) obtains a copy of electronic token associated with the electronic payment card (605). Accordingly, in one embodiment, at step 908-1, the analysis unit (406) may obtain the copy of electronic token from the database (404) based on the details of the electronic payment card (605).

In another embodiment, the analysis unit (406) may obtain the copy of electronic token from the mobile device (500) associated with the electronic payment card (605) at the time of transaction. In such embodiment, the copy of electronic token is unavailable in the database (404). As such, the analysis unit (406) may transmit a request to the application (505) via the first communication link (604) for the copy of electronic token associated with the electronic payment card (605). The request includes details of the electronic payment card (605) such as card number.

Upon receiving the request for copy of electronic token from the server (400), the processing unit (502) fetches the copy of electronic token from the memory (504) based on the details of the electronic payment card (605) received in the request. Upon fetching, the processing unit (502) transmits the copy of electronic token through the application (505) via the first communication link (604).

At step 909, the analysis unit (406) authenticates the electronic payment card (605) based on various criteria, as described below. The various criteria includes, but not limited to, validity of the copy of electronic token, comparison of the electronic token in the second request with the copy of electronic token, and time period indicated in the copy of electronic token. The analysis unit (406) may authenticate either on one of the criteria or on all of the criteria.

Accordingly, the analysis unit (406) determines the validity of the copy of the electronic token. The copy of electronic token is marked as invalid by the analysis unit (406) if a validation request has been received previously or time period indicated in the copy of electronic token is expired. In other words, the analysis unit (406) sets the copy of electronic token as invalid for further request to authenticate the electronic payment card (605) in respect of one or more further transactions initiated using the electronic payment card (605). On the contrary, the copy of electronic token is marked as valid by the analysis unit (406) if a validation request has not been received previously or time period indicated in the copy of electronic token is current. If the copy of electronic token is invalid, the analysis unit (406) prevents the completion of the transaction. If the copy of electronic token is valid, the analysis unit (406) allows the completion of the transaction.

Further, the analysis unit (406) compares the electronic token received in the validation request with the copy of electronic token. If the received electronic token does not match with the copy of electronic token, the analysis unit (406) prevents the completion of the transaction. If the received electronic token matches the copy of electronic token, the analysis unit (406) allows the completion of the transaction.

Furthermore, the analysis unit (406) determines if the time period indicated in the received electronic token is expired from the time of generating the electronic token. If the time period has expired with respect to the time of generating the electronic token, the analysis unit (406) prevents the completion of the transaction. If the time period is current with respect to the time of generating the electronic token, the analysis unit (406) allows the completion of the transaction.

At step 910, upon authenticating the electronic payment card (605) based on the various criteria, the transmitting unit (403) transmits a success message to the designated intermediary device, i.e., issuer system (601). Accordingly, the message generating unit (407) generates a success message indicative of authentication of the electronic payment card and the transmitting unit (403) transmits the success message to the issuer system (601) over the network (602).

At step 911, upon receiving the success message, the issuer system (601) successfully processes and completes the transaction. In examples, the banking transaction at ATM and purchase transaction at POS system are successfully completed.

However, the completion of the transaction is further based on transaction value. In one embodiment, the issuer system (601) completes the transaction based on the transaction value message received from the server (400). In an example, if the transaction value message indicates that the value of the transaction is below the specified cash limit value/credit limit value, the transaction is completed. In an example, if the transaction value message indicates that the value of the transaction is above the specified cash limit value/credit limit value, the transaction is not completed. In another embodiment, the issuer system (400) completes the transaction based on the cash limit value/credit limit value specified by the user.

Further, upon completing the transaction, the issuer system (601) transmits a transaction successful message POT system (603), as known in the art. Upon receiving the transaction successful message, the POT system (603) may generate a paper bill having transaction information and payment information.

Furthermore, the issuer system (601) transmits a transaction successful message to the user as known in the art. In an example, the issuer system (601) transmits the transaction successful message to the mobile device (500).

At step 912, the transmitting unit (403) of the server (400) transmits a success message to the mobile device (500) via the first communication link (604). Accordingly, the second receiving unit (506) receives the success message through the application (505) and displays on a display unit (not shown in the figure) of the mobile device (500). Examples of the alert message include SMS message, USSD message, and a flash message.

However, if at step 909, the analysis unit (406) does not authenticate the electronic payment card (605), then the process flows to step 913.

At step 913, the transmitting unit (403) of the server (400) transmits a failure message to the designated intermediary device, i.e., issuer system (601) over the network (602). Accordingly, the message generating unit (407) generates the failure message indicative of the invalid authentication of the electronic payment card in respect of the transaction. Upon receiving the failure message, the issuer system (601) prevents the processing of the transaction as known in the art. In examples, the banking transaction at ATM and purchase transaction at POS system are prevented from completion.

At step 914, upon preventing the transaction, the issuer system (601) transmits a transaction unsuccessful message to the POT system (603). Upon receiving the transaction unsuccessful message, the POT system (603) may display an appropriate message on a display unit (not shown in the figure) of the POT system (603). In addition, the issuer system (601) transmits a transaction unsuccessful message to the user as known in the art. In an example, the issuer system (601) transmits the transaction unsuccessful message to the mobile device (500).

At step 915, the transmitting unit (403) of the server (400) transmits an alert message to the mobile device (500) via the first communication link (604). Accordingly, the message generating unit (407) generates the alert message indicating details about the transaction and invalid authentication of the electronic payment card (605) in respect of the transaction.

Accordingly, the second receiving unit (506) of the mobile device (500) receives the alert message through the application (505) and displays on a display unit of the mobile device (500). Examples of the alert message include SMS message, USSD message, and a flash message.

Thus, the transaction is allowed only if the electronic payment card (605) transmits a valid electronic token. This eliminates the chances of unauthorized transactions with the electronic payment card (605) since an invalid token will prevent the completion of the transaction. Further, the electronic token is generated for each transaction and is valid for a limited time period. This eliminates use of same electronic token for subsequent transactions. As such, the security of the electronic payment card is greatly enhanced as two-step security verification is provided.

While certain present preferred embodiments of the invention have been illustrated and described herein, it is to be understood that the invention is not limited thereto. Clearly, the invention may be otherwise variously embodied, and practiced within the scope of the following claims.

WE CLAIM:

1. A method implemented by a server for communicating electronic token to a electronic payment card, the method comprising:
   - receiving, in respect of the electronic payment card, a first request for an electronic token from a mobile device associated with the electronic payment card via a first communication link, wherein the first request is received in response to a prior request for electronic token received from the electronic payment card by the mobile device via a second communication link when the electronic payment card is in close proximity to the mobile device;
   - generating an electronic token including a time period indicating a validity of the electronic token;
   - associating the electronic token with the electronic payment card, wherein the electronic token is adapted to be stored in a memory of the electronic payment card; and
   - transmitting the electronic token to the mobile device via the first communication link, wherein the electronic token is further transmitted to the electronic payment card by the mobile device via the second communication link and is saved in the memory of the electronic payment card, such that the electronic payment card is authenticated based on a validity of the electronic token.

2. The method as claimed in claim 1, wherein the electronic payment card is one of: a credit card, a debit card, an automated teller machine (ATM) card, a fleet card, stored-value card, prepaid card, and a gift card.

3. The method as claimed in claim 1, wherein the first communication link is independent of the second communication link, the first communication link being one of a data communication link and a non-data communication link available between the mobile device and the server, and the second communication link being a proximity based communication link available between the mobile device and the electronic payment card.

4. The method as claimed in claim 1, wherein the first request is received via an application available in a memory of the mobile device over the first communication link.

5. The method as claimed in claim 4, wherein the prior request for electronic token is received from the electronic payment card by the application via the second communication link.

6. The method as claimed in claim 1, wherein the electronic token is an encrypted key of configurable length.

7. The method as claimed in claim 1 further comprises:

- storing a copy of the electronic token associated with the electronic payment card in a database.

8. The method as claimed in claim 1 further comprises:

- receiving, from a designated intermediary device, a second request to authenticate the electronic payment card in respect of a transaction initiated using the electronic payment card;
- determining availability of an electronic token in the second request, the electronic token being sent by the electronic payment card to the designated intermediary device;
- upon determination, obtaining a copy of an electronic token associated with the electronic payment card; and
- transmitting a response to the mobile device associated with the electronic payment card and the designated intermediary device based on at least one of:
  - validity of the copy of electronic token;
  - comparison of the electronic token in the second request with the copy of electronic token; and
  - time period indicated in the copy of electronic token.

9. The method as claimed in claim 8, wherein the copy of the electronic token associated with the electronic payment card is obtained from a database, the database being adapted to store the copy of the electronic token.

10. The method as claimed in claim 8 further comprises:

- setting the copy of electronic token as invalid for further request to authenticate the electronic payment card in respect of one or more further transactions initiated using the electronic payment card.

11. A method implemented by a mobile device for communicating electronic token, the method comprising:

- receiving a first request for an electronic token from an electronic payment card associated with the mobile device via a first communication link when the electronic payment card is in close proximity to the mobile device;
- generating an electronic token including a time period indicating a validity of the electronic token;
- associating the electronic token with the electronic payment card, wherein the electronic token is adapted to be stored in a memory of the electronic payment card;
- transmitting the electronic token to the electronic payment card via the first communication link such that electronic token is stored in the memory of the electronic payment card; and
- transmitting a copy of the electronic token to a server via a second communication link, such that the electronic payment card is authenticated by the server based on a validity of the electronic token.

12. The method as claimed in claim 11, wherein the electronic payment card is one of: a credit card, a debit card, an automated teller machine (ATM) card, a fleet card, stored-value card, prepaid card, and a gift card.

13. The method as claimed in claim 11, wherein the first request is received through an application available in the memory of the mobile device via the first communication link.

14. The method as claimed in claim 11, wherein the first communication link is independent of the second communication link, the first communication link being a proximity based communication link available between the mobile device and the

electronic payment card, and the second communication link being one of a data communication link and a non-data communication link available between the mobile device and the server.

15. The method as claimed in claim 11, wherein the electronic token is an encrypted key of configurable length.

16. The method as claimed in claim 11 further comprising:

- receiving, through the application via the second communication link, response from the server based on at least one of:
  - validity of the copy of electronic token;
  - comparison of an electronic token received in the second request with the copy of electronic token, the electronic token being sent by the electronic payment card to the server; and
  - time period indicated in the copy of electronic token.

17. A method implemented by a mobile device for communicating electronic token to a electronic payment card, the method comprising:

- receiving a first request for an electronic token from the electronic payment card associated with the mobile device via a first communication link when the electronic payment card is in close proximity to the mobile device;
- generating the electronic token including a time period indicating a validity of the electronic token;
- associating the electronic token with the electronic payment card, wherein the electronic token is adapted to be stored in a memory of the electronic payment card;
- storing a copy of the electronic token associated with the electronic payment card in a memory; and
- transmitting the electronic token to the electronic payment card via the first communication link such that electronic token is stored in the memory of the electronic payment card, wherein the electronic payment card is authenticated based on a validity of the electronic token.

18. The method as claimed in claim 17, wherein the first request is received through an application available in the memory of the mobile device via the first communication link.

19. The method as claimed in claim 17 further comprises:

- receiving, through an application via a second communication link, a second request for an electronic token associated with the electronic payment card from a server, the second request corresponding to authentication of the electronic payment card in respect of a transaction initiated using the electronic payment card;
- fetching a copy of the electronic token associated with the electronic payment card from a memory;
- transmitting, through the application via the second communication link, the copy of the electronic token associated with the electronic payment card to the server; and
- receiving, through the application via the second communication link, response from the server based on at least one of:
  - validity of the copy of electronic token;
  - comparison of an electronic token received in the second request with the copy of electronic token, the electronic token being sent by the electronic payment card to the server; and
  - time period indicated in the copy of electronic token.

20. The method as claimed in claim 19, wherein the first communication link is independent of the second communication link, the first communication link being a proximity based communication link available between the mobile device and the electronic payment card, and the second communication link being one of a data communication link and a non-data communication link available between the mobile device and the server.

21. A server for communicating electronic token to a electronic payment card, the server comprising:

- a first receiving unit to receive, in respect of the electronic payment card, a first request for an electronic token from a mobile device associated with the electronic payment card via a first communication link, wherein the first request is received in response to a prior request for electronic token received from the electronic payment card by the mobile device via a second communication link when the electronic payment card is in close proximity to the mobile device;
- a processing unit coupled to the first receiving unit to:
  - generate an electronic token including a time period indicating a validity of the electronic token; and
  - associate the electronic token with the electronic payment card, wherein the electronic token is adapted to be stored in a memory of the electronic payment card; and
- transmitting unit coupled to the processing unit to transmit the electronic token to the mobile device via the first communication link, wherein the electronic token is further transmitted to the electronic payment card by the mobile device via the second communication link and is saved in the memory of the electronic payment card, such that the electronic payment card is authenticated based on a validity of the electronic token.

22. The server as claimed in claim 21, wherein the electronic payment card is one of: a credit card, a debit card, an automated teller machine (ATM) card, a fleet card, stored-value card, prepaid card, and a gift card.

23. The server as claimed in claim 21, wherein the first communication link is independent of the second communication link, the first communication link being one of a data communication link and a non-data communication link available between the mobile device and the server, and the second communication link being a proximity based communication link available between the mobile device and the electronic payment card.

24. The server as claimed in claim 21, wherein the electronic token is an encrypted key of configurable length.

25. The server as claimed in claim 21, wherein the processing unit further:
    - stores a copy of the electronic token associated with the electronic payment card in a database.

26. The server as claimed in claim 21 further comprises:
    - a second receiving unit to receive, from a designated intermediary device, a second request to authenticate the electronic payment card in respect of a transaction initiated using the electronic payment card; and
    - an analysis unit coupled to the second receiving unit to:
        - determine availability of an electronic token in the second request, the electronic token being sent by the electronic payment card to the designated intermediary device;
        - upon determination, obtain a copy of an electronic token associated with the electronic payment card; and
        - transmit a response to the mobile device associated with the electronic payment card and the designated intermediary device based on at least one of:
            - validity of the copy of electronic token;
            - comparison of the electronic token in the second request with the copy of electronic token; and
            - time period indicated in the copy of electronic token.

27. The server as claimed in claim 26, wherein the analysis unit obtains a copy of the electronic token associated with the electronic payment card from a database, the database being adapted to store the copy of the electronic token.

28. The server as claimed in claim 26, wherein the analysis unit further:
    - sets the copy of electronic token as invalid for further request to authenticate the electronic payment card in respect of one or more further transactions initiated using the electronic payment card.

29. A mobile device for communicating electronic token, the mobile device comprising:

- a first receiving unit to receive a first request for an electronic token from a electronic payment card associated with the mobile device via a first communication link when the electronic payment card is in close proximity to the mobile device;
- a processing unit coupled to the first receiving unit to:
  - generate an electronic token including a time period indicating a validity of the electronic token; and
  - associate the electronic token with the electronic payment card, wherein the electronic token is adapted to be stored in a memory of the electronic payment card; and
- a transmitting unit coupled to the processing unit to:
  - transmit the electronic token to the electronic payment card via the first communication link such that electronic token is stored in the memory of the electronic payment card; and
  - transmit a copy of the electronic token to a server via a second communication link, such that the electronic payment card is authenticated by the server based on a validity of the electronic token.

30. The mobile device as claimed in claim 29, wherein the electronic payment card is one of: a credit card, a debit card, an automated teller machine (ATM) card, a fleet card, stored-value card, prepaid card, and a gift card.

31. The mobile device as claimed in claim 29, wherein the first request is received through an application available in a memory of the mobile device via the first communication link.

32. The mobile device as claimed in claim 29, wherein the first communication link is independent of the second communication link, the first communication link being a proximity based communication link available between the mobile device and the electronic payment card, and the second communication link being one of a data communication link and a non-data communication link available between the mobile device and the server.

33. The mobile device as claimed in claim 29, wherein the electronic token is an encrypted key of configurable length.

34. The mobile device as claimed in claim 29 further comprising:

- a second receiving unit to receive, through the application via the second communication link, response from the server based on at least one of:
  - validity of the copy of electronic token;
  - comparison of an electronic token received in the second request with the copy of electronic token, the electronic token being sent by the electronic payment card to the server; and
  - time period indicated in the copy of electronic token.

35. A mobile device for communicating electronic token to a electronic payment card, the mobile device comprising:

- a first receiving unit to receive a first request for an electronic token from the electronic payment card associated with the mobile device via a first communication link when the electronic payment card is in close proximity to the mobile device;
- a processing unit coupled to the first receiving unit to:
  - generate the electronic token including a time period indicating a validity of the electronic token;
  - associate the electronic token with the electronic payment card, wherein the electronic token is adapted to be stored in a memory of the electronic payment card; and
  - store a copy of the electronic token associated with the electronic payment card in a memory; and
- a transmitting unit coupled to the generating unit to transmit the electronic token to the electronic payment card via the first communication link such that electronic token is stored in the memory of the electronic payment card, wherein the electronic payment card is authenticated based on a validity of the electronic token.

36. The mobile device as claimed in claim 35, wherein the first request is received through an application available in the memory of the mobile device via the first communication link.

37. The mobile device as claimed in claim 35 further comprises:

- a second receiving unit to receive, through an application via a second communication link, a second request for an electronic token associated with the electronic payment card from a server, the second request corresponding to authentication of the electronic payment card in respect of a transaction initiated using the electronic payment card.

38. The mobile device as claimed in claim 37, wherein:

- the processing unit further fetches a copy of the electronic token associated with the electronic payment card from a memory; and
- the transmitting unit further transmits, through the application via the second communication link, the copy of the electronic token associated with the electronic payment card to the server.

39. The mobile device as claimed in claim 38, wherein:

- the second receiving unit further receives, through the application via the second communication link, response from the server based on at least one of:
  - validity of the copy of electronic token;
  - comparison of an electronic token received in the second request with the copy of electronic token, the electronic token being sent by the electronic payment card to the server; and
  - time period indicated in the copy of electronic token.

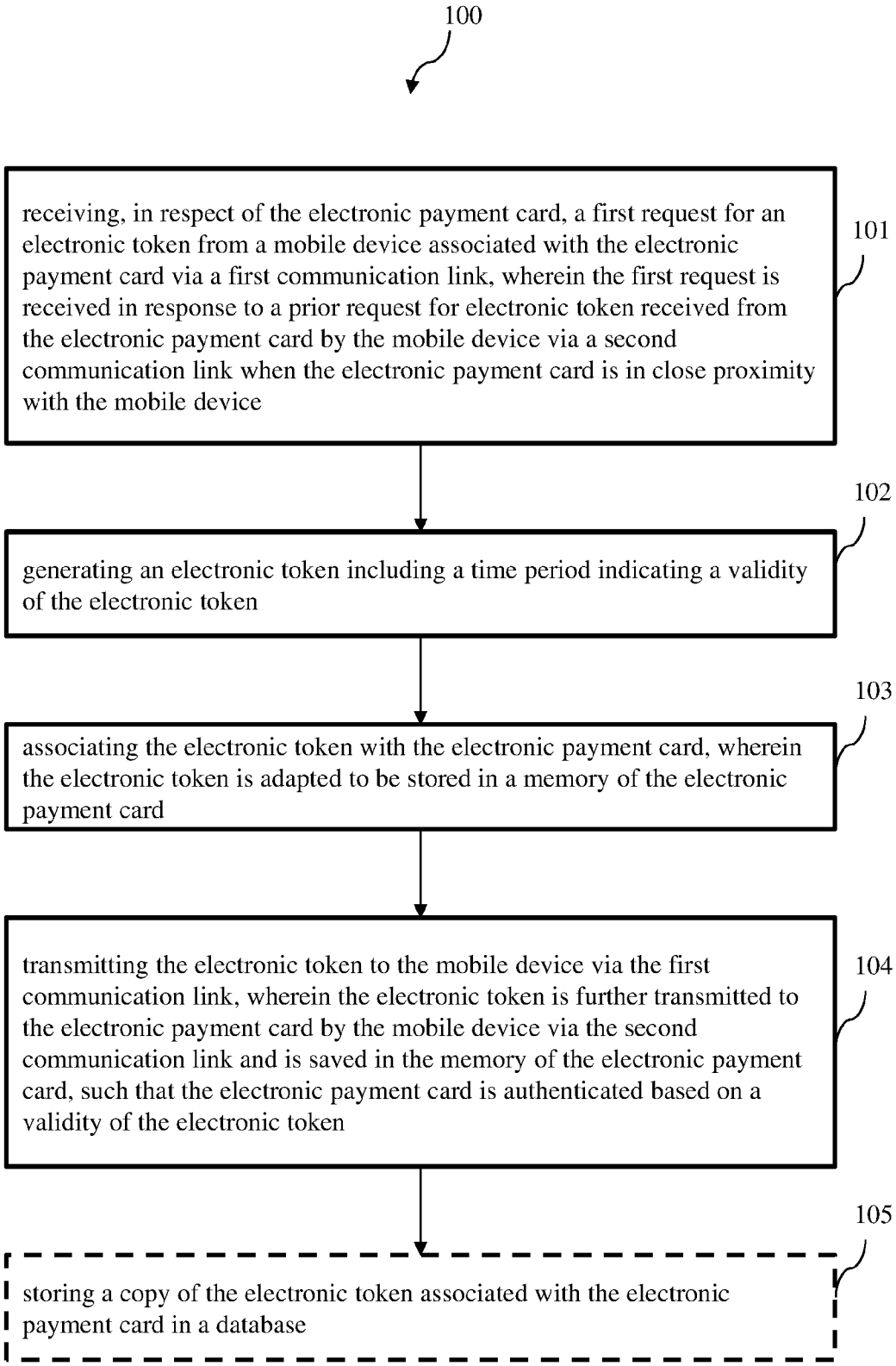
100
receiving, in respect of the electronic payment card, a first request for an electronic token from a mobile device associated with the electronic payment card via a first communication link, wherein the first request is received in response to a prior request for electronic token received from the electronic payment card by the mobile device via a second communication link when the electronic payment card is in close proximity with the mobile device
101
generating an electronic token including a time period indicating a validity of the electronic token
102
associating the electronic token with the electronic payment card, wherein the electronic token is adapted to be stored in a memory of the electronic payment card
103
transmitting the electronic token to the mobile device via the first communication link, wherein the electronic token is further transmitted to the electronic payment card by the mobile device via the second communication link and is saved in the memory of the electronic payment card, such that the electronic payment card is authenticated based on a validity of the electronic token
104
storing a copy of the electronic token associated with the electronic payment card in a database
105

FIGURE 1a

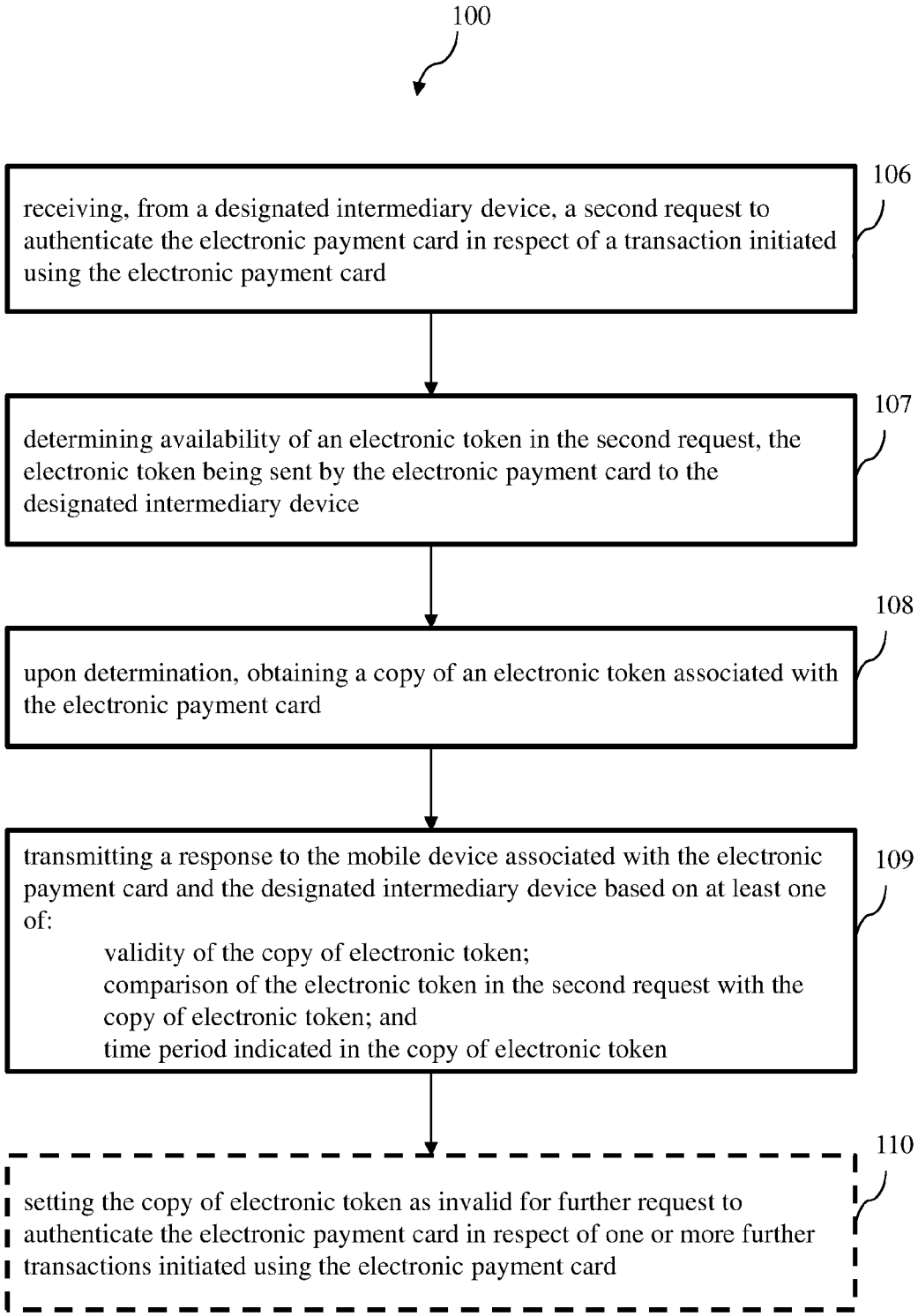
100
receiving, from a designated intermediary device, a second request to authenticate the electronic payment card in respect of a transaction initiated using the electronic payment card
106
determining availability of an electronic token in the second request, the electronic token being sent by the electronic payment card to the designated intermediary device
107
upon determination, obtaining a copy of an electronic token associated with the electronic payment card
108
transmitting a response to the mobile device associated with the electronic payment card and the designated intermediary device based on at least one of:
validity of the copy of electronic token;
comparison of the electronic token in the second request with the copy of electronic token; and
time period indicated in the copy of electronic token
109
setting the copy of electronic token as invalid for further request to authenticate the electronic payment card in respect of one or more further transactions initiated using the electronic payment card
110

FIGURE 1b

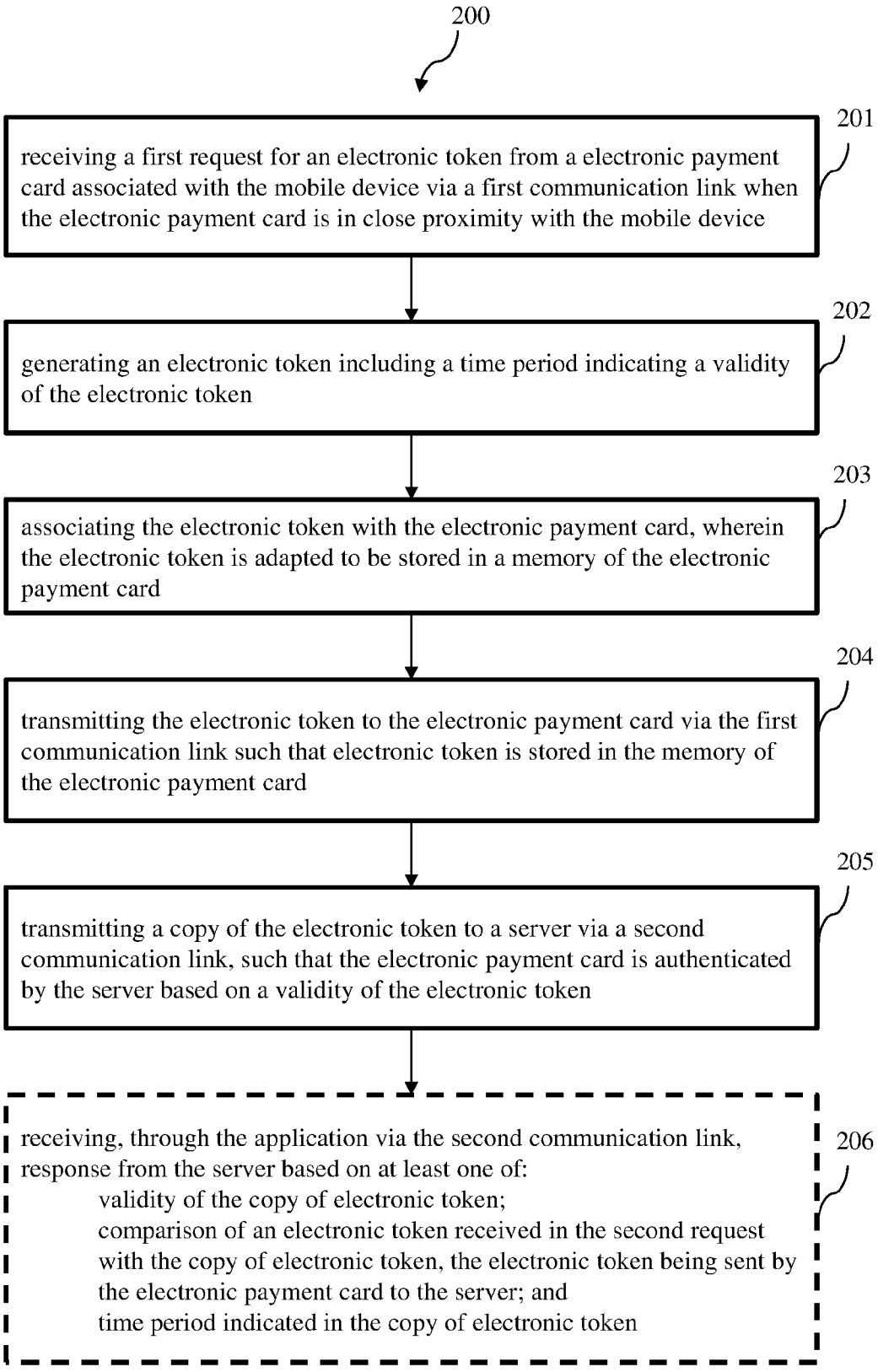
200
receiving a first request for an electronic token from a electronic payment card associated with the mobile device via a first communication link when the electronic payment card is in close proximity with the mobile device
201
generating an electronic token including a time period indicating a validity of the electronic token
202
associating the electronic token with the electronic payment card, wherein the electronic token is adapted to be stored in a memory of the electronic payment card
203
transmitting the electronic token to the electronic payment card via the first communication link such that electronic token is stored in the memory of the electronic payment card
204
transmitting a copy of the electronic token to a server via a second communication link, such that the electronic payment card is authenticated by the server based on a validity of the electronic token
205
receiving, through the application via the second communication link, response from the server based on at least one of:
validity of the copy of electronic token;
comparison of an electronic token received in the second request with the copy of electronic token, the electronic token being sent by the electronic payment card to the server; and
time period indicated in the copy of electronic token
206

FIGURE 2

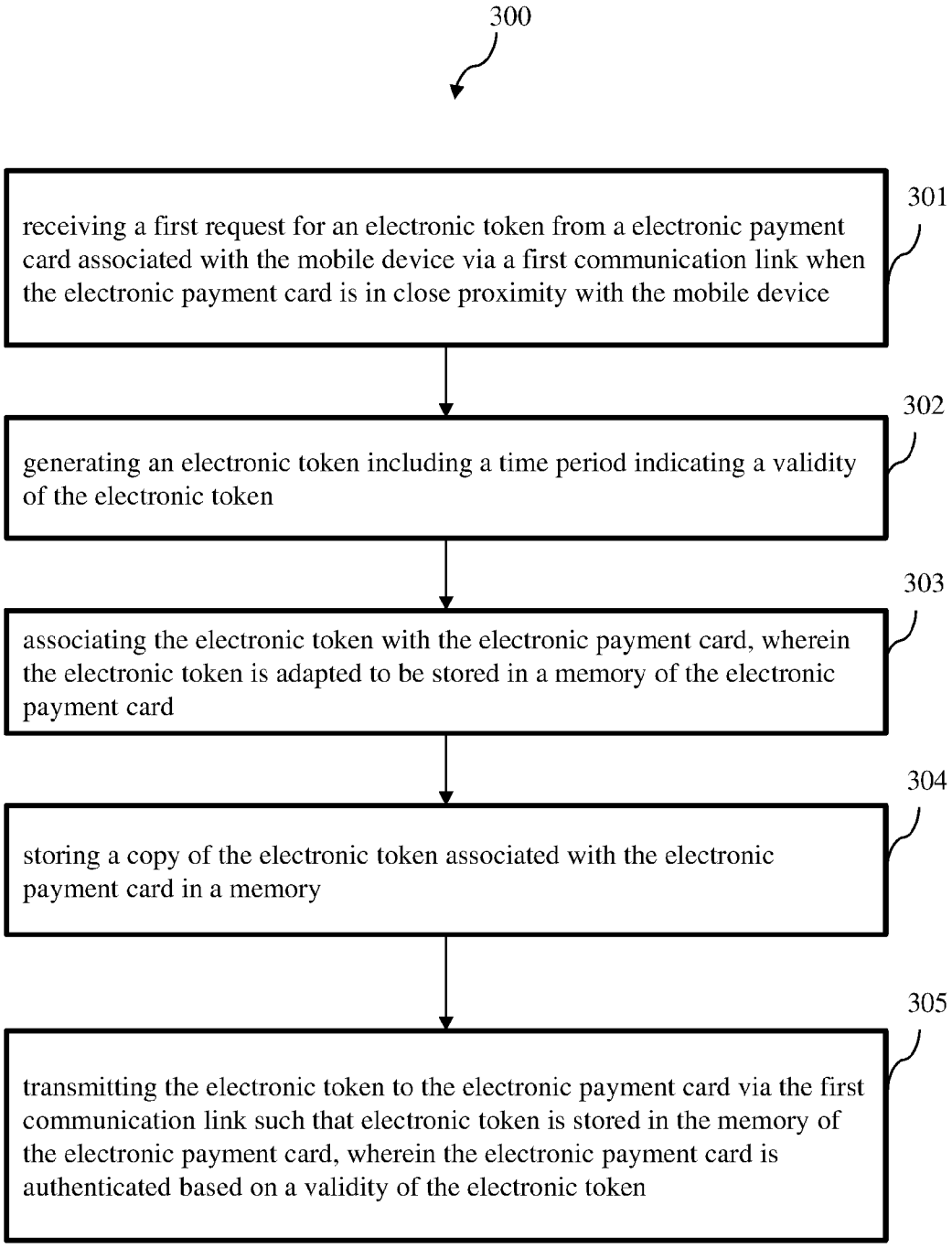
300
receiving a first request for an electronic token from a electronic payment card associated with the mobile device via a first communication link when the electronic payment card is in close proximity with the mobile device
301
generating an electronic token including a time period indicating a validity of the electronic token
302
associating the electronic token with the electronic payment card, wherein the electronic token is adapted to be stored in a memory of the electronic payment card
303
storing a copy of the electronic token associated with the electronic payment card in a memory
304
transmitting the electronic token to the electronic payment card via the first communication link such that electronic token is stored in the memory of the electronic payment card, wherein the electronic payment card is authenticated based on a validity of the electronic token
305

FIGURE 3a

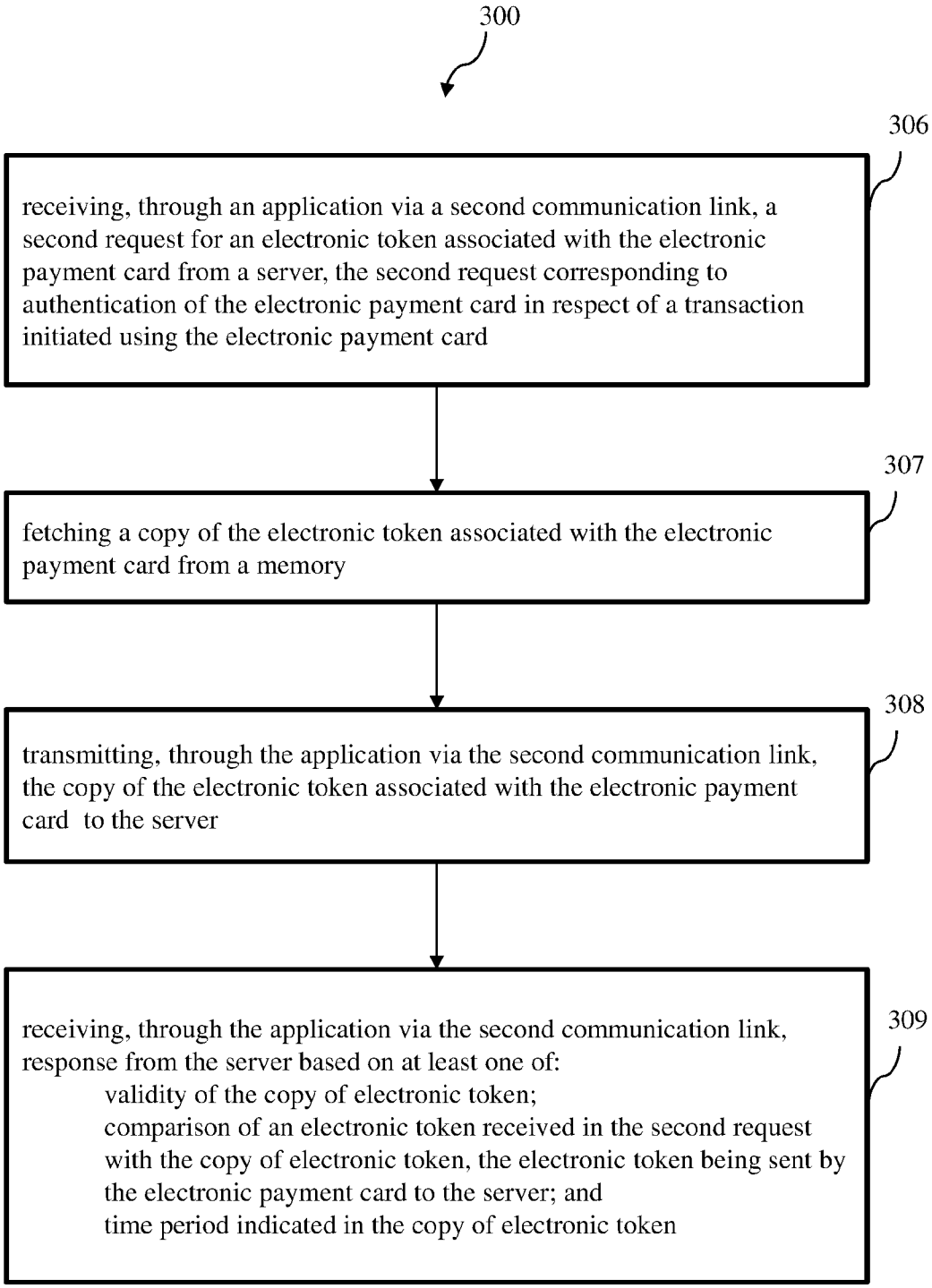
300
306
receiving, through an application via a second communication link, a second request for an electronic token associated with the electronic payment card from a server, the second request corresponding to authentication of the electronic payment card in respect of a transaction initiated using the electronic payment card
307
fetching a copy of the electronic token associated with the electronic payment card from a memory
308
transmitting, through the application via the second communication link, the copy of the electronic token associated with the electronic payment card to the server
309
receiving, through the application via the second communication link, response from the server based on at least one of:
validity of the copy of electronic token;
comparison of an electronic token received in the second request with the copy of electronic token, the electronic token being sent by the electronic payment card to the server; and
time period indicated in the copy of electronic token

FIGURE 3b

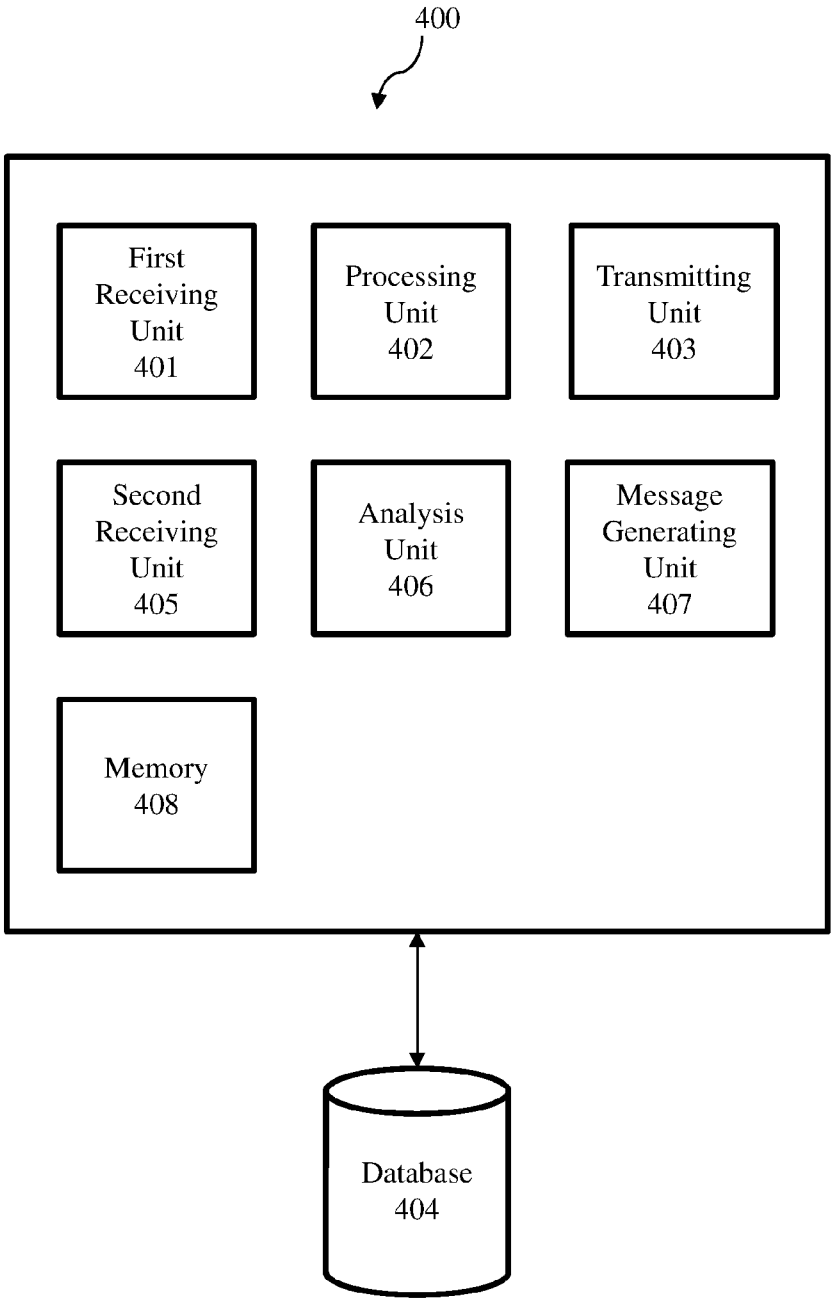
400
First Receiving Unit 401
Processing Unit 402
Transmitting Unit 403
Second Receiving Unit 405
Analysis Unit 406
Message Generating Unit 407
Memory 408
Database 404

FIGURE 4

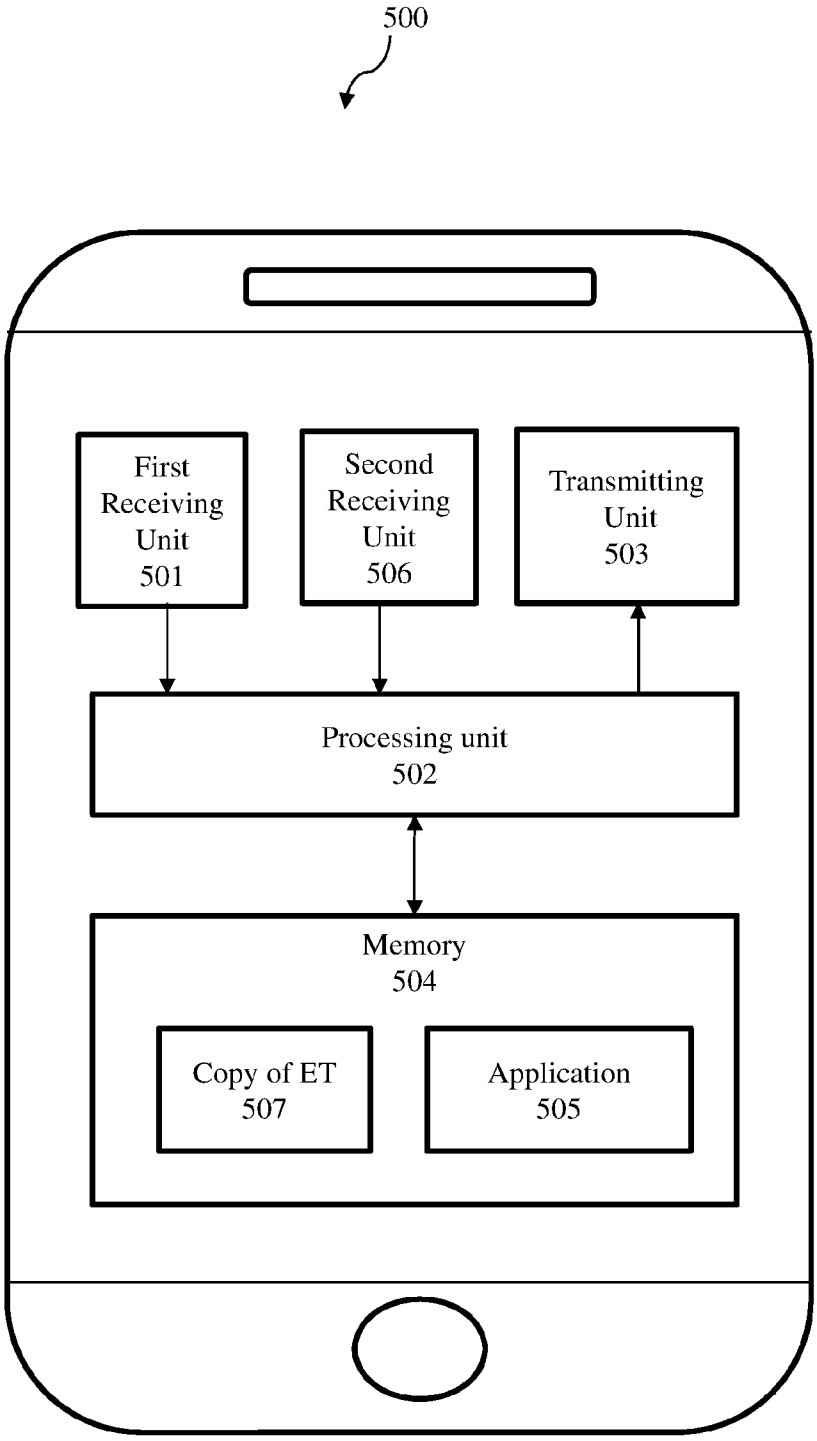
500
First Receiving Unit 501
Second Receiving Unit 506
Transmitting Unit 503
Processing unit 502
Memory 504
Copy of ET 507
Application 505

FIGURE 5

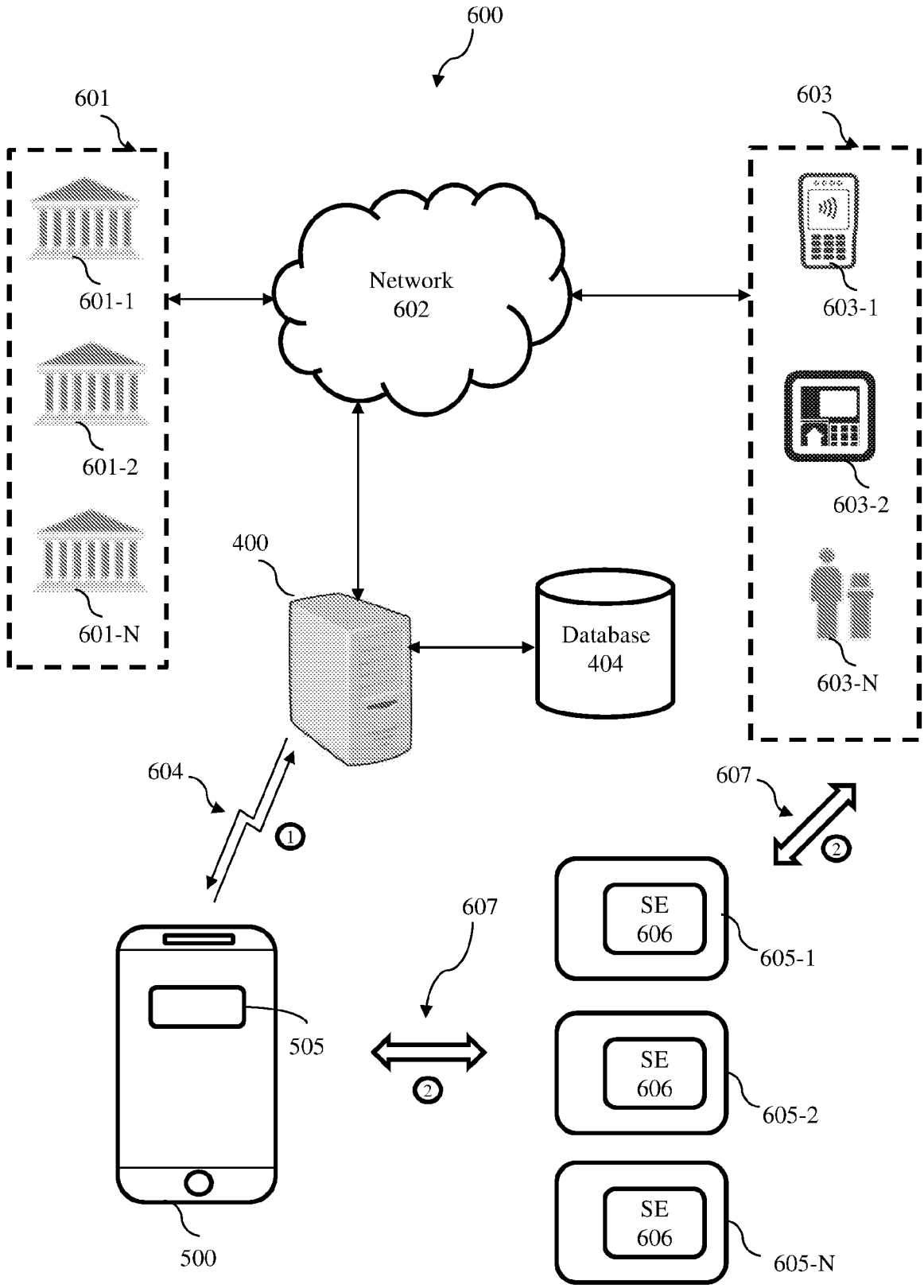
600
601
601-1
601-2
601-N
Network
602
603
603-1
603-2
603-N
400
Database
404
604
1
607
2
607
2
505
500
SE
606
605-1
SE
606
605-2
SE
606
605-N

FIGURE 6

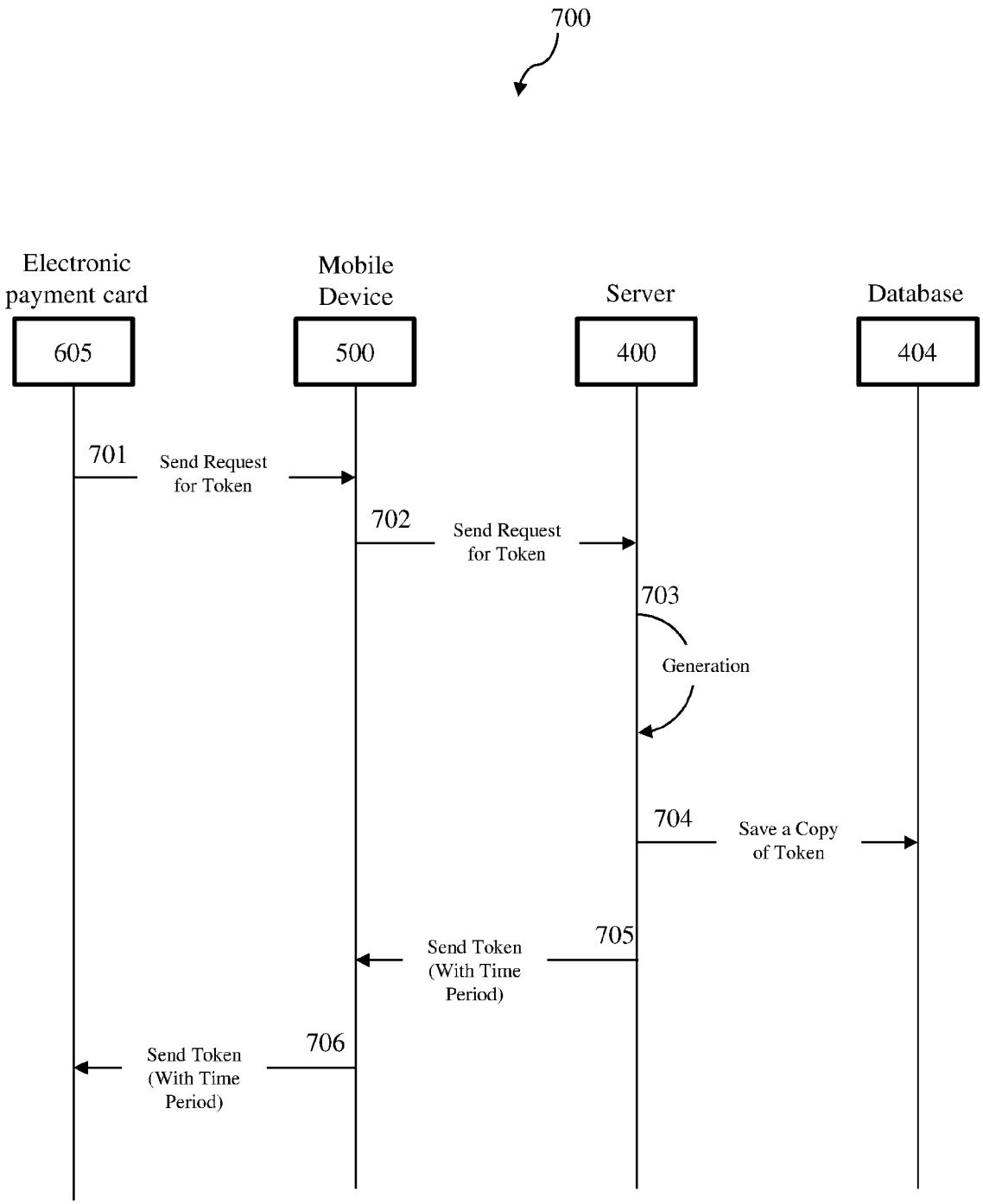
700
Electronic payment card
605
Mobile Device
500
Server
400
Database
404
701
Send Request for Token
702
Send Request for Token
703
Generation
704
Save a Copy of Token
705
Send Token (With Time Period)
706
Send Token (With Time Period)

FIGURE 7

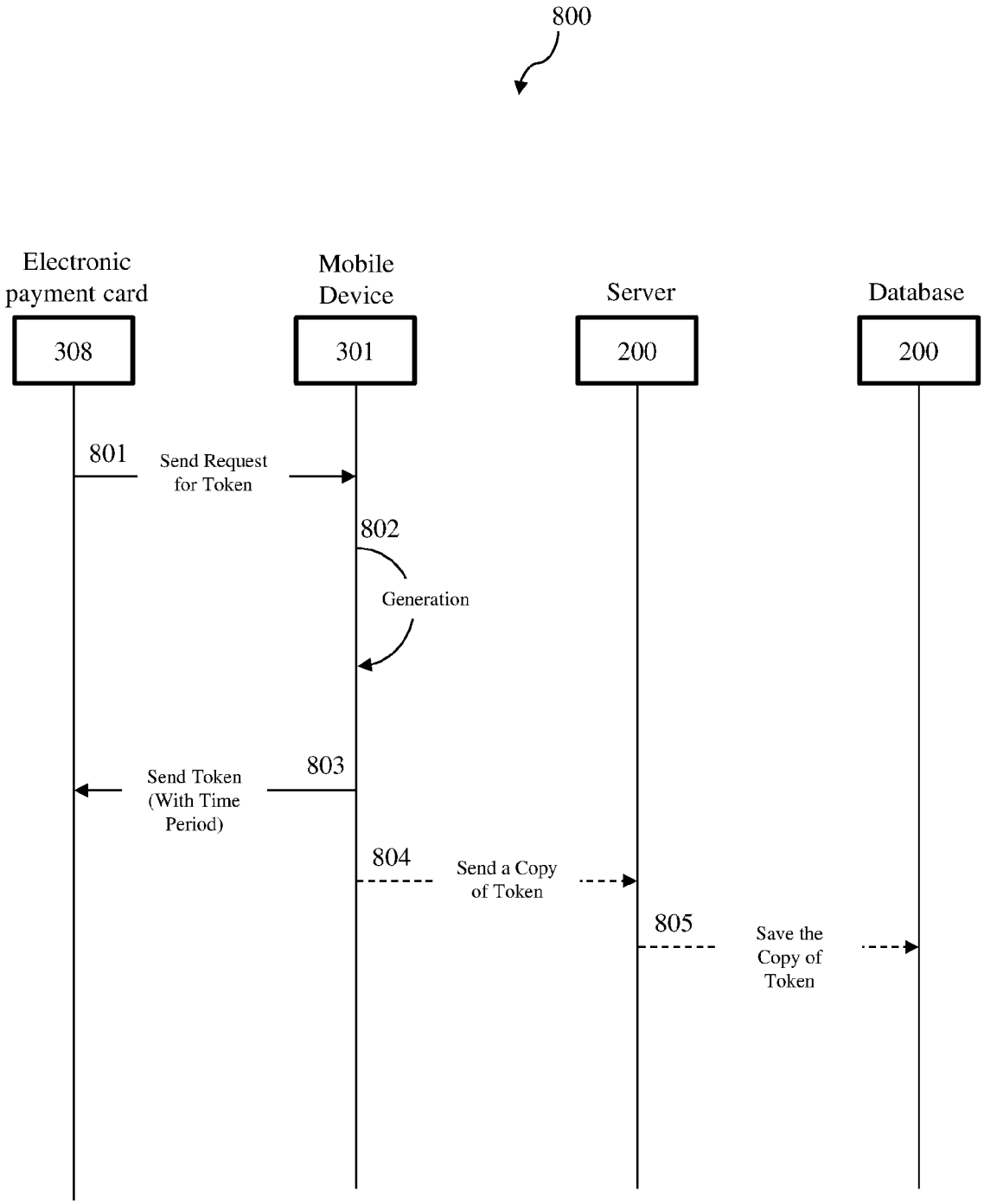
800
Electronic payment card
308
Mobile Device
301
Server
200
Database
200
801
Send Request for Token
802
Generation
803
Send Token (With Time Period)
804
Send a Copy of Token
805
Save the Copy of Token

FIGURE 8

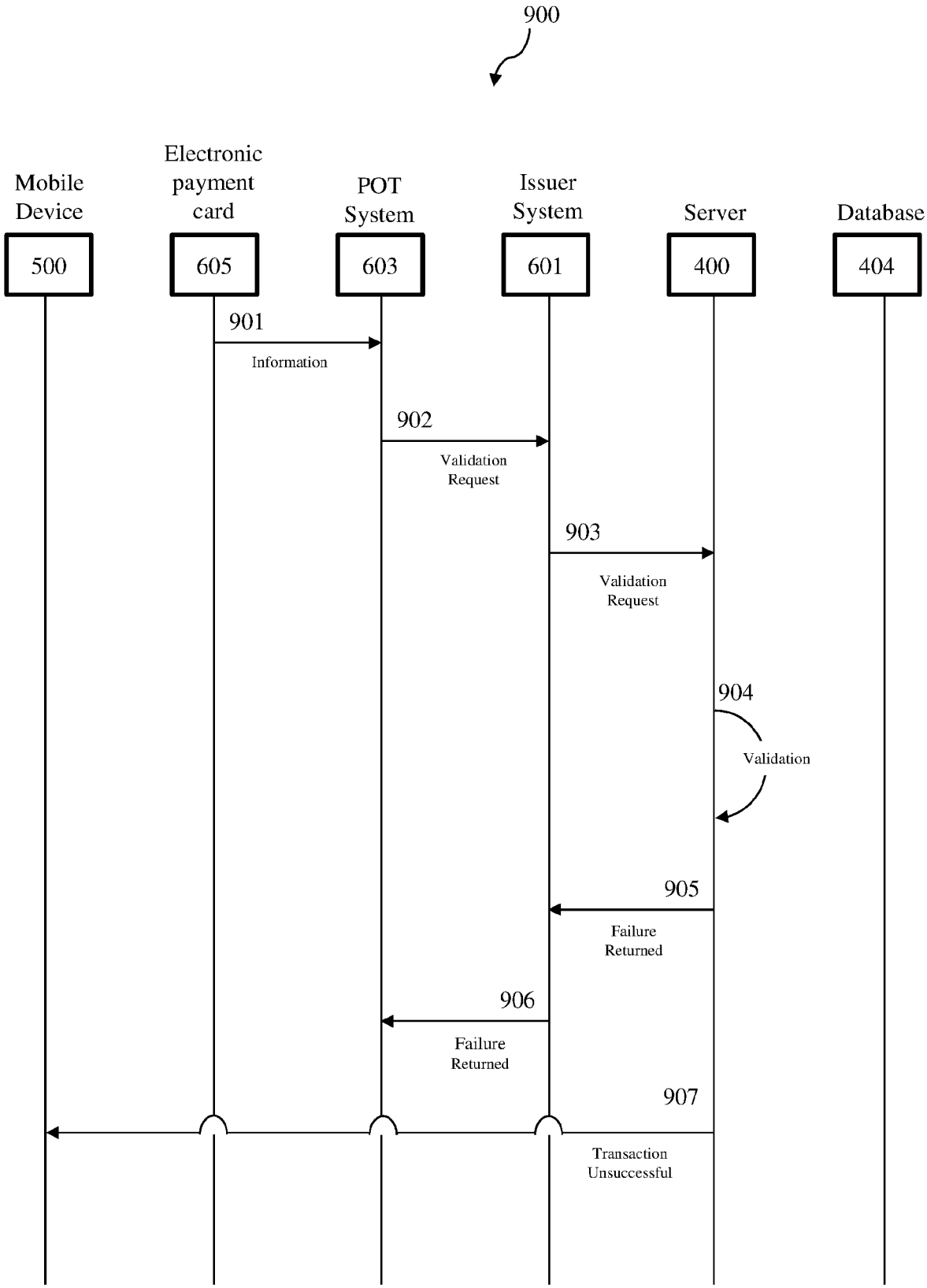
900
Mobile Device
500
Electronic payment card
605
POT System
603
Issuer System
601
Server
400
Database
404
901
Information
902
Validation Request
903
Validation Request
904
Validation
905
Failure Returned
906
Failure Returned
907
Transaction Unsuccessful

FIGURE 9a

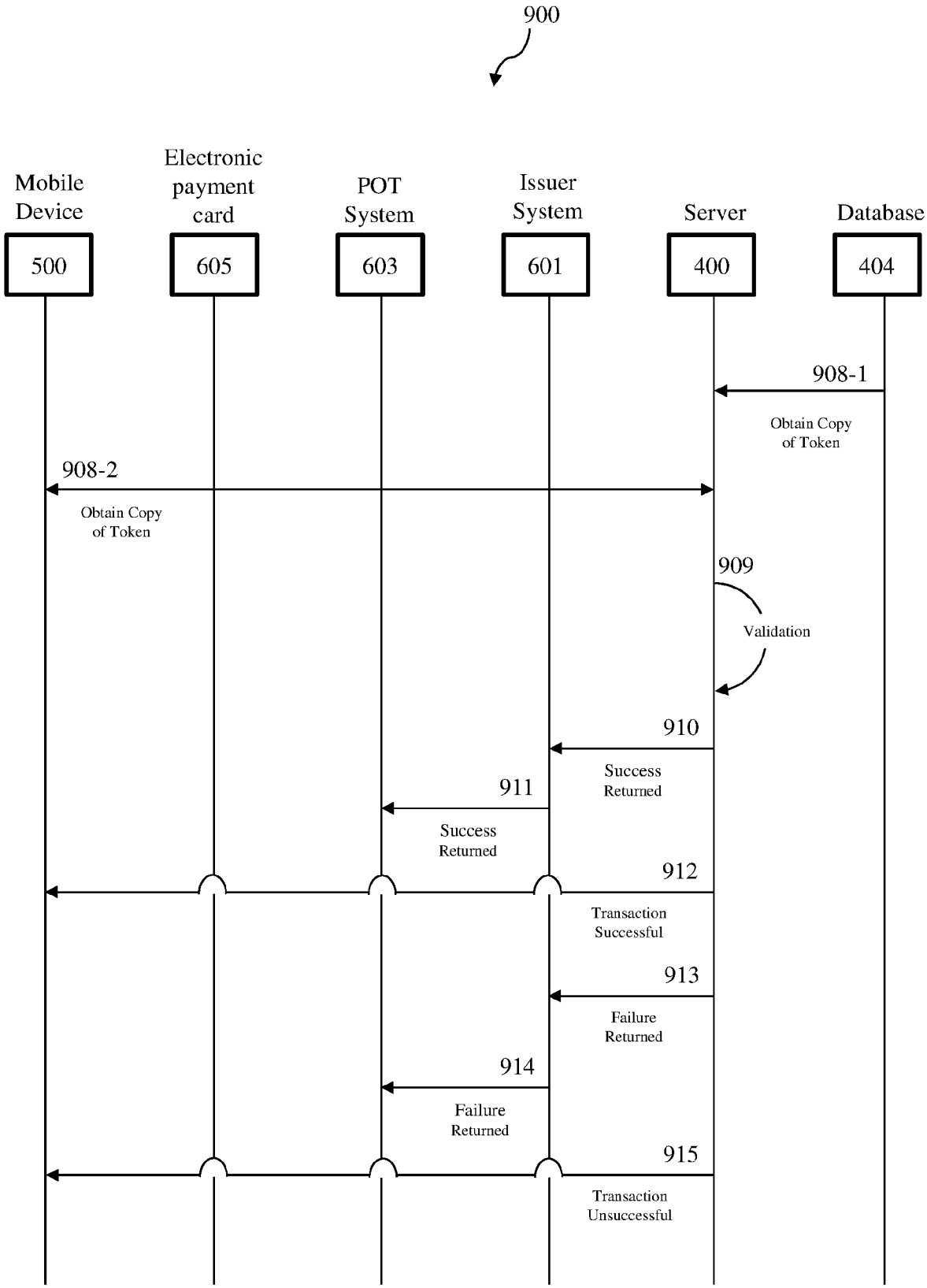
900
Mobile Device
500
Electronic payment card
605
POT System
603
Issuer System
601
Server
400
Database
404
908-1
Obtain Copy of Token
908-2
Obtain Copy of Token
909
Validation
910
Success Returned
911
Success Returned
912
Transaction Successful
913
Failure Returned
914
Failure Returned
915
Transaction Unsuccessful

FIGURE 9b

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IB2017/050016

A. CLASSIFICATION OF SUBJECT MATTER
G06Q20/00,G06Q20/32,G06F17/30,H04L09/00 Version=2017.01

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06Q,G06F,H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

Patseer, IPO Internal Database
Keywords: electronic payment, mobile device, authentication

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US20120290376 A1(INTUIT INC.) 15 November 2012 (15-11-2012) (Abstract, Paragraphs 4, 16, 30, 58-66, 76-77, Claims 1-2, 15 and 33)	21-39

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
20-04-2017	20-04-2017
Name and mailing address of the ISA/ Indian Patent Office Plot No.32, Sector 14,Dwarka,New Delhi-110075 Facsimile No.	Authorized officer Subhash Kumar Singh Telephone No. +91-1125300200

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IB2017/050016

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☒ Claims Nos.: 1-20
because they relate to subject matter not required to be searched by this Authority, namely:
The subject matter of claims 1-20 relate to methods of doing business,
which does not require an international search by the International Searching Authority in accordance with PCT Article 17(2)(a)(i) and [Rule 39.1(iii)].

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying additional fees, this Authority did not invite payment of additional fees.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest and, where applicable, the payment of a protest fee.

☐ The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.

☐ No protest accompanied the payment of additional search fees.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/IB2017/050016

Citation	Pub.Date	Family	Pub.Date
US 20120290376 A1	15-11-2012	IN KOLNP201303581 A	21-02-2014
		EP 2707843 A1	19-03-2014
		AU 2011367804 A1	28-11-2013
		WO 2012154189 A1	15-11-2012
		CA 2835514 A1	15-11-2012