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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
10 January 2019 (10.01.2019)

WIPO | PCT

(10) International Publication Number
WO 2019/009803 A1

(51) International Patent Classification:
G06Q 20/32 (2012.01) *H04W 84/18* (2009.01)
H04W 76/10 (2018.01) *H04W 48/16* (2009.01)
H04W 88/06 (2009.01)

(21) International Application Number:
PCT/SG2018/050321

(22) International Filing Date:
02 July 2018 (02.07.2018)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
201741023345 03 July 2017 (03.07.2017) IN

(71) Applicant: **GP NETWORK ASIA PTE. LTD.** [SG/SG]; 6, Shenton Way, #38-01 OUE Downtown, Singapore 068809 (SG).

(72) Inventor: **SOMASUNDARAM, Manicavasagam**; B6, #304, Challagatta Road, Shriram Spandhana, Bangalore 560037 (IN).

(74) Agent: **MCLAUGHLIN, Michael Gerard** et al.; McLaughlin IP Pte. Ltd., 24A Mosque Street, Singapore 059504 (SG).

(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, JO, 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,

WO 2019/009803 A1

(54) Title: PROCESSING PAYMENTS

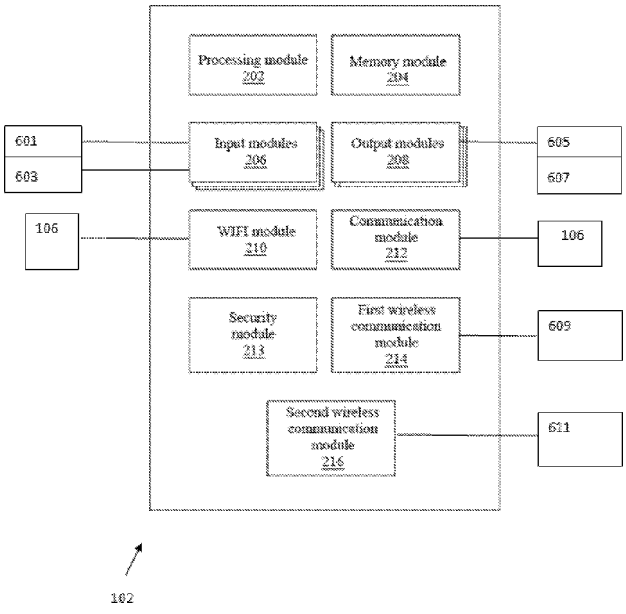

FIG 6

(57) Abstract: A method of operating a payment terminal comprises receiving an activation input, and in response thereto outputting a first wireless signal for communicating with an external payment device of a first type and a second wireless signal for communicating with an external payment device of a second type. The first and second wireless signals are formatted in respective mutually different first and second protocols. The method further comprises receiving a reply to one of the first and second wireless signals and in response to the reply, terminating outputting of the other of the first and second wireless signals.

[Continued on next page]

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

Published:

— *with international search report (Art. 21(3))*
— *in black and white; the international application as filed contained color or greyscale and is available for download from PATENTSCOPE*

PROCESSING PAYMENTS

Field of the invention

The invention is in the field of payment technology.

Discussion of the related art:

Cashless payments are becoming well used, largely for convenience. Such payments may involve cards or mobile phones. Internet connectivity is a limitation while using mobile phones to implement cashless electronic transactions.

Even though the reach of the Internet is spreading, it is not certain that the user using a mobile device is connected to Internet all the time. Also, use of the Internet may not also be affordable to large sections of the society in parts of the world. In such scenarios, completing an electronic transaction over mobile phones may not be feasible.

Further, conventionally, a merchant may have to deploy different types of payment terminals for enabling different types of digital payments. As an example, the merchant may have to deploy a payment terminal to accept payment using cards. Additionally, the merchant may have to deploy yet another terminal to support payment via mobile phones. Even if such an additional terminal is deployed, the terminal may only support mobile phones that use a specific type of communication technology, such as NFC.

There is a need to improve the situation.

Summary

In a first aspect a payment terminal is used to output signals corresponding to two communication protocols or methods so that when a device capable of responding to one of the two protocols or methods is brought into proximity with the terminal, communication can occur.

In a second aspect a payment terminal is provided and is able to communicate using two different communication methods. In use it outputs signals related to both methods so as to initiate

communication with a payment device such as a mobile phone or payment card by means of one of the two methods. Communication being established by one of the two methods, the other method is terminated.

In a third aspect, there is provided a method of operating a payment terminal comprising receiving an activation input, and in response thereto outputting a first wireless signal for communicating with an external payment device of a first type and a second wireless signal for communicating with an external payment device of a second type, wherein the first and second wireless signals are formatted in respective mutually different first and second protocols, receiving a reply to one of the first and second wireless signals and in response to the reply, terminating outputting of the other of the first and second wireless signals.

The method may further comprise processing the reply to authenticate the external payment device to thereby establish a communication channel.

The method may further comprise processing the reply to authenticate the external payment device, and after the processing step implementing the terminating step.

The wireless signals may comprise an NFC signal and a Bluetooth signal.

The method may further comprise processing the reply to authenticate the external payment device to thereby establish a communication channel and receiving from the communication channel data indicative of a user; receiving, at an input, data indicative of a transaction amount and transferring the data indicative of a user and data indicative of a transaction amount to a server.

The method may further comprise processing the reply to authenticate the external payment device to thereby establish a communication channel and receiving from the communication channel data indicative of a user and a one-time verifier for identifying a current transaction; receiving, at an input, data indicative of a transaction amount, transferring the data indicative of a user, data indicative of the one-time verifier and data indicative of a transaction amount to a server.

The method may further comprise outputting a new one-time verifier over the communication channel.

The method may further comprise communicating, with a server, information indicative of which of the first and second wireless signals is responded to.

In a fourth aspect there is disclosed a payment terminal for communicating wirelessly with an external device having a processing device and a store holding instructions to control the processing device to cause the payment terminal to respond to an activation input to output a first wireless signal for communicating with an external payment device of a first type and a second wireless signal for communicating with an external payment device of a second type, wherein the first and second wireless signals are formatted in respective mutually different first and second protocols, and in response to receiving a reply to one of the first and second wireless signals to terminate outputting of the other of the first and second wireless signals.

The payment terminal may further comprise a keypad for providing the activation signal, a display for displaying information under control of the processing device, and an output device for communicating with a server.

The payment terminal may further comprise a first wireless device configured to output the first wireless signal and a second wireless device configured to output the second wireless signal, both under control of the processing device.

The payment terminal may further comprise a security device comprising a store for security keys, the security device being configured to use the keys to encrypt or decrypt data for use by the terminal.

A personal area network device may be configured to output the first wireless signal.

A near field communication device may be configured to output the second wireless signal.

In a fifth aspect a system is provided for processing payments. The system comprises a payment terminal comprising a first wireless communication module and a second wireless communication

module. The first module is capable of initiating and establishing proximity communication using a first communication method that is different from a second communication method. The second module is capable of initiating and establishing proximity communication using the second communication method. The payment terminal is configured to receive an input to initiate a transaction; cause the first module and the second module to attempt to initiate communication using their respective method. An external entity capable of being communicated with by one of the first and second methods can be brought into proximity with the payment terminal, so that communication may be initiated between the payment terminal and the external entity depending upon which of one of the communication modules is successful.

The first wireless communication module may be a personal area network module. The second wireless communication module may be a near field communication module. The payment terminal may be further configured to terminate attempts to establish communication channel with any other external entity using the first wireless communication module and the second wireless communication module till said transaction is concluded. The external entity maybe one of a card and a portable communication device, wherein the payment terminal may be further configured to identify whether the communication established is with one of a near field communication tag of the card, a near field communication module of the portable communication device or a personal area network module of the portable communication device. The payment terminal may be further configured to communicate to a server whether the communication established is with one of the near field communication tag of the card, the near field communication module of the portable communication device or the personal area network module of the portable communication device. The external entity may be a portable communication device, wherein the payment terminal may be configured to: receive at least data identifying a user attempting to make a payment connected to the transaction, up on establishing communication with the portable communication device; and communicate at least the data identifying the user, data identifying a merchant and data identifying payment amount to a server to process the transaction, thereby enabling the portable communication device to make payment without using the Internet. The payment terminal may be further configured to: receive, from the external entity, location validation data; verify, based on the location validation data, whether payment can be accepted using the payment terminal; and decline transaction if verified that payment cannot be accepted, or process transaction if verified that payment can be accepted. The external entity may be a card with which near field communication is capable of being established,

the payment terminal is configured to: read, from the card, data identifying a user and data to be used as a onetime verifier; write, to the card , a new one-time verifier; and communicate the data identifying the user and the data to be used as the one-time verifier to a server, wherein the one-time verifier is used to verify whether the one-time verifier is what is expected from the card for the current transaction to either reject the transaction or proceed with the transaction. The payment terminal may be further configured to communicate for each transaction, to a server, a unique one-time verifier, wherein the one-time verifier may be used to verify whether the one-time verifier is what is expected from the payment terminal for the current transaction to either reject the transaction or proceed with the transaction. The external entity may be a portable communication device, the payment terminal may be configured to: receive, from the portable communication device, data identifying a user and data to be used as a one-time verifier; update, in the portable communication device, a new one-time verifier; and communicate the data identifying the user and the data to be used as the one-time verifier to a server , wherein the one-time verifier is used to verify whether the one-time verifier is what is expected from the portable communication device for the current transaction to either reject the transaction or proceed with the transaction.

In another aspect, a method is provided for processing payments. The method comprises receiving an input to initiate a transaction at a payment terminal. Thereafter, a first wireless communication module and a second wireless communication module, provided in the payment terminal, attempt to establish a communication channel with an external entity. The first wireless communication module is capable of establishing proximity communication using a first communication channel that is different from a second communication channel, which the second wireless communication module is capable of establishing. The method further comprises, establishing the communication channel with the external entity using one of the first wireless communication module and the second wireless communication module, based on which one of the communication modules is successful in establishing the communication channel with the external entity.

In yet another aspect, a system is provided for processing payments. The system comprises a payment terminal comprising a personal area network (PAN) module. The payment terminal is configured to cause the PAN module to broadcast identifier. The system further comprises a portable communication device. The device is configured to receive identifier broadcasted by the payment terminal; send a request automatically to establish a communication channel with the

PAN module of the payment terminal, if signal strength of the broadcasted identifier is over a first threshold; and continue to retain communication with the PAN module of the payment terminal, once the communication channel is established, even if signal strength between the device and the PAN module of the payment terminal falls below the first threshold, till a transaction is concluded.

In still another aspect, a method is provided for processing payments. The method comprises broadcasting an identifier by a personal area network module of a payment terminal; receiving, by a portable communication device, the identifier broadcast by the payment terminal; sending automatically, by the portable communication device, a request to establish a communication channel with the personal area network module of the payment terminal, if signal strength of the broadcasted identifier is over a first threshold. The method further includes, retaining communication between the portable communication device and the personal area network module of the payment terminal, once the communication channel is established, even if signal strength between the portable communication device and the personal area network module of the payment terminal falls below the first threshold, till a transaction is concluded.

There is also disclosed a system for processing payments, the system comprising: a payment terminal comprising a personal area network module, wherein the payment terminal is configured to cause the personal area network module to broadcast identifier; and a portable communication device configured to: receive identifier broadcasted by the payment terminal; send a request automatically to establish a communication channel with the personal area network module of the payment terminal, if signal strength of the broadcasted identifier is over a first threshold; and continue to retain communication with the personal area network module of the payment terminal, once the communication channel is established, even if signal strength between the portable communication device and the personal area network module of the payment terminal falls below the first threshold, till a transaction is concluded.

The first threshold may be configured such that the portable communication device and the payment terminal are within 20 centimetres of each other to establish the communication channel. The first threshold may be configured such that the portable communication device and the payment terminal are within 10 centimetres of each other to establish the communication channel.

The first threshold may be configured such that the portable communication device and the payment terminal are within a preconfigured distance of each other to establish the communication channel.

At least one of the payment terminal or the portable communication device may be configured to terminate the established communication channel, if the signal strength between the portable communication device and the personal area network module of the payment terminal falls below a second threshold.

The second threshold may be remotely reconfigurable.

The payment terminal may be configured to: receive at least data identifying a user attempting to make a payment connected to the transaction, up on establishing the communication channel; and communicate at least the data identifying the user, data identifying a merchant and data identifying payment amount to a server to process the transaction, thereby enabling the portable communication device to make payment without using the Internet.

The payment terminal may be further configured to: receive, from a server, data corresponding to account balance of a user making a payment using the portable communication device; and communicate the data corresponding to the account balance to the portable communication device via the communication channel.

The payment terminal may be further configured to: receive, from a server, data corresponding to transaction information; and communicate at least a part of the data corresponding to the transaction information to the portable communication device via the communication channel.

The payment terminal may be incapable of displaying the account balance of the user; and the portable communication device is configured to display the account balance of the user post the transaction.

The identifier may comprise data identifying compatibility, wherein the portable communication device is configured to consider the payment terminal for automatically requesting to establish

the communication channel, if the identifier received by the portable communication device comprises the data identifying compatibility.

The payment terminal may be configured to: receive an input indicating an amount to be transferred; receive an input to begin broadcasting of the identifier, after the input indicating the amount is received; and communicate data corresponding to the amount and a merchant connected to the payment terminal, to the portable communication device, once the communication channel is established, wherein the amount and information corresponding to the merchant are displayed on the portable communication device.

The first threshold may be remotely reconfigurable.

The personal area network module may be one of a BLUETOOTH low energy module or a BLUETOOTH module.

There is also disclosed a method for processing payments, the method comprising: broadcasting identifier by a personal area network module of a payment terminal; receiving, by a portable communication device, identifier broadcasted by the payment terminal; sending automatically, by the portable communication device, a request to establish a communication channel with the personal area network module of the payment terminal, if signal strength of the broadcasted identifier is over a first threshold; and retaining communication between the portable communication device and the personal area network module of the payment terminal, once the communication channel is established, even if signal strength between the portable communication device and the personal area network module of the payment terminal falls below the first threshold till as transaction is concluded.

Brief description of drawings

In the various figures:

FIG. 1 illustrates a system 100 for processing payments;

FIG. 2 is a block diagram of a payment terminal 102 of the system 100;

FIGs. 3A-3F, are flow charts of an exemplary method of processing payments by the system 100;

FIG. 4A illustrates an amount entered in the payment terminal 102,

FIG. 4B illustrates a user interface of an application of a smartphone 104b that is opened by the user to make payment;

FIG. 4C illustrates a user interface of the application of the smartphone 104b searching for payment terminals 102;

FIG. 4D illustrates a smartphone 104b paired with the payment terminal 102 via BLE channel after having the smartphone 104b brought close to the payment terminal 102;

FIG. 4E illustrates a user interface of the application of the smartphone 104b, where the user is providing input to approve payment;

FIG. 4F illustrates a user interface of the application of the smartphone 104b, where it is shown that the transaction is being processed;

FIG. 4G illustrates a user interface of the application of the smartphone 104b, where transaction information is displayed after successful transaction;

FIG 5A shows a highly schematic diagram of an exemplary transaction packet;

FIG5B shows another transaction packet; and

FIG 6 shows a block schematic diagram of an embodiment of a payment terminal showing how some connections to the payment terminal may be carried out.

Detailed description

In the following description, reference to a phone or smartphone is not intended to be restrictive as to a particular type of portable communication device; the terms are used for convenience and the intention is to cover any type of portable communication device.

Disclosed is a system that is capable of processing payments, without the need for Internet usage by a user making a payment. The payment may be made, for example, using a near field communication (NFC) enabled card or a smartphone with NFC or Bluetooth low energy (BLE) technology.

The payment is facilitated by a payment terminal deployed at a merchant location. The payment terminal may include a personal area network module (BLE module) and a NFC module. In an embodiment, at the initiation of a transaction, the payment terminal is configured to attempt to initiate communication using both BLE and NFC simultaneously, with an external entity presented by the consumer/user to make the payment. The external entity can be a NFC enabled card or a

smartphone with NFC or BLUETOOTH low energy (BLE) technology, with an application installed therein to transact with payment terminals.

In another embodiment, the transaction terminal is configured to try one of the BLE and NFC for a period of time and then if unsuccessful to try the other of the BLE and NFC, and if necessary to repeat the trying of both BLE and NFC one after the other.

In an embodiment, once the payment terminal is successful in establishing a communication channel with the external entity via one of BLE and NFC, the payment terminal is configured to disable (from attempting to establish communication with any other external entity) the other technique, until the initiated transaction is concluded.

In another embodiment, the payment terminal ceases to emit one of the two outputs as soon as it detects a signal return of the other of the two outputs. This may save battery power in a battery driven terminal.

In an embodiment, a communication channel with the payment terminal is established via NFC, wherein the user brings a card or an NFC enabled smartphone in proximity to the payment terminal. The payment terminal reads data from the card/NFC module of the phone and communicates it to the backend server to process the initiated payment transaction. Note that, the merchant is not instructing the payment terminal regarding which communication means to use, rather the payment terminal is automatically deciding on its own.

In an embodiment, a communication channel with the payment terminal is established via BLE, wherein the user brings a BLE enabled smartphone in proximity to the payment terminal. The payment terminal receives data from the BLE module of the phone and communicates it to the backend server to process the initiated payment transaction. Note that, even in this case, the merchant is not instructing the payment terminal regarding which communication means to use, rather the payment terminal is automatically deciding on its own.

In case of BLE, the payment terminal communicates transaction information (received from a backend server), such as amount deducted and balance in the user's account, to the user's smartphone via the communication channel established via BLE. Hence, the user is not only able

to make payment, but also get an update on the transaction and account without using Internet or relying on SMS or similar alternatives.

Referring to FIG. 1, a system 100 for processing payments has a payment terminal 102 which can receive payments via external entities such as NFC enabled cards 104a and portable communication devices 104b. The payment terminal 102 in use communicates with a server 106 via a communication network 108.

The payment terminal 102 may be, for example, card readers, smartphones, POS systems, tablets, phablets, computers and laptops, among other computing devices.

Now referring to FIG. 2, an embodiment of the payment terminal 102 includes a processing module 202, a memory module 204, input modules 206, output modules 208, a WIFI module 210, a communication module 212, a security module 213, a first wireless communication module 214 and a second wireless communication module 216. The memory module 204 is connected to a bus connecting it to the processor module 202. The processing module 202 is connected to all the other modules by a bus 123. The processing module 202 operates under the control of executable instructions stored in the memory module 204 to perform the functionality of the payment terminal 102, and in general calls the other modules of the device to perform their functionality.

Referring now to FIG.6, in this embodiment the input modules 206 are connected to a key pad 601 and stylus 603. The output modules 208 are connected to a display screen 605 and printer 607. The WiFi module is shown connected via a wireless link to the server 106, and the communications module 212 is shown connected via a wired link to the server 106. It will be understood that in use probably only one of the links to the server 106 will be employed. The first wireless communications module 214 is connected to an NFC antenna and the second wireless communications module is connected to a Bluetooth antenna 611. In some embodiments the antennas are integral with the respective wireless communication modules.

Returning to Fig 2, the processing module 202 is implemented in the form of one or more processors and may be implemented as appropriate in hardware, computer executable instructions, firmware, or combinations thereof. Computer executable instruction or firmware implementations of the processing module 202 may include computer-executable or machine-

executable instructions written in any suitable programming language to perform the various functions described.

In an embodiment the memory module 204 comprises a permanent memory such as hard disk drive, eMMC, SSD or EEPROM. The memory module may be configured to store data, and executable program instructions that are implemented by the processor 202. The memory module 204 may be implemented in the form of a primary and a secondary memory with primary memory being hard-wired memory and secondary memory being removable memory such as an SD card. The memory module 204 may store additional data and program instructions that are loadable and executable on the processor 202, as well as data generated during the execution of these programs. Further, the memory module 204 may be volatile memory, such as random-access memory and/or a disk drive, or non-volatile memory. The memory module 204 may comprise of removable memory such as a Compact Flash card, Memory Stick, Smart Media, Multimedia Card, Secure Digital memory, or any other memory storage.

In the presently described embodiment, the input modules 206 provide an interface for input devices such as keypad, touch screen, mouse, microphone and stylus among other input devices. The output modules 208 provide an interface for output devices such as display screen, speakers, printer and haptic feedback devices, among other.

In the presently described embodiment the input modules 206 and output modules 208 are also used to exchange data between the payment terminal 102 and data derived by the terminal from NFC enabled cards 104a, portable communication devices 104b with the server 106.

In one embodiment the WIFI module is used by the payment terminal 102 to communicate with the server 106 via the communication network 108.

In one embodiment, the communication module 212 is used by the payment terminal 102 to communicate with the server 106 via the communication network 108. In one embodiment the communication module 212 is a GPRS module. In other embodiments, other modules that enable telecommunication are employed.

In embodiments the communication module 212 includes a modem, a network interface card (such as an Ethernet card), a communication port, or a Personal Computer Memory Card International Association (PCMCIA) slot, among others. In one embodiment the communication module 212 includes devices supporting both wired and wireless protocols. In one embodiment data in the form of electronic signals are transferred via the communication module 212. In other embodiments one or more of electromagnetic, optical, among other signals are used.

In an embodiment, the payment terminal uses digital keys to encrypt decrypt and authenticate data exchanged between the terminal 102 and external entities 104. The keys in this embodiment are held in a security module 213. This security module houses all the keys that are to be used by the device, and is a one-time write only device. The keys are written into the security module 213 in a secure environment. The security module 213 is designed in such a way that keys cannot be directly read from the module. When encryption is required, data is pumped into the security module 213 which in turn returns encrypted data after processing using the keys. There is no way to access the keys directly from the security module 213, thereby ensuring safety of the keys. Likewise, to decrypt data, it is pumped into the security module 213 which processes it using the keys to return decrypted data.

The security module 213 may be deployed in the form of software, firmware, hardware or combination thereof.

In an embodiment, the first wireless communication module 214 is a personal area network module (hereinafter, referred to as module). In the presently described embodiment the PAN module a BLUETOOTH low energy (BLE) module. In other embodiments technologies that are analogous to BLE in the current context, may be used.

In an embodiment, the second wireless communication module 216 is a near-field communication module (hereinafter, referred to as NFC module). In other embodiments, technologies that are analogous to NFC in the current context may be used.

Therefore, it may be noted that the payment terminal 102 has the first wireless communication module 214, capable of establishing proximity communication with external entities 104, using a first communication channel or protocol (e.g., BLE) that is different from a second communication

channel or protocol (e.g., NFC), which the second wireless communication module 216 is capable of establishing.

A high-level description will now be given of an embodiment of the payment terminal in operation with respect to Figs 2 and 6.

Initially a processor of the processing module 202 is in an idle state, and in this embodiment the two wireless communication modules 214, 216 are also idle. The terminal is "woken" by an input from the keypad 601 to its input module 206, which interrupts the idle process of the processing module 202 via bus 123. The processing module takes instruction over the bus 123 from the memory module 204, and processes this to provide an output over bus 123 to the first and second warless communication modules 214,216, which thereby begin to emit their respective interrogation signals, i.e. BLE and respectively NFC signals, to seek out an external device 104. The interrogation signals are sent out via the respective antennas 609, 611.

When a response to one of the two interrogation signals is received by one of the two antennas 609 611, the respective wireless communication module calls the processing module 202 over the bus 123, and based upon stored instructions in the memory module 204, the processing module 202 instructs the other respective wireless communication module to cease emitting its interrogation signal. For simplicity, suppose first wireless communication module, BLE module 214, receives a response and thus second wireless communication module 216 is instructed to go to an idle state.

Data received from an external device 104 over antenna 609 is passed along bus 123 to security module 213 which decrypts that data under control of the processing module 202 using digital keys stored therein as described elsewhere in this document. This enables the payment terminal to authenticate the external device 104 (e.g. phone application or card). If appropriate, and after the authentication is performed some information is sent to screen 605 for display- for example instructing a user/merchant to perform an operation such as "input amount" "input pin".

The response to any such instruction is received by the input modules 206, for example an input made to the keypad 601. This is then processed by processing modules 202, and depending upon the outcome of processing either more information is displayed on screen 605 to facilitate further

rounds of instructions and response, or the transaction information is sufficient for sending to the server 106.

In due course the processing module 202 instructs one of the WiFi modules 210 and the communication module 212 to interact with the server 106 on the basis of data received and processed by the terminal 102.

In response to the data received from the terminal 102 the server 106 returns data via one of the WiFi module 210 and the communication module 212. This data is processed by processing module 202 via bus 123 and if appropriate information derived from the data is displayed via the output modules 208 on the display screen 605 and/or printer 607.

At the end of the transaction the processing module returns to its idle state.

At some time during the processing of the transaction the terminal 102 may send data to the external device 104, typically such data being encrypted by keys stored in the security module 213. As described elsewhere data sent to the external device may comprise, for example, a one-time code for security purposes.

In FIGs. 3A-3F, the tasks carried out by one embodiment of the payment terminal 102, the external entity 104 (types of external entities 104a, 104b are referred to as external entity 104 in some instances to facilitate easier reading of this document) and the server 106, are discussed.

At step 302, the payment terminal 102 receives an input indicating amount to be charged. As an example, merchant uses a physical or digital keypad provided in or on the payment terminal 102 to receive the input indicating the amount to be charged. As an example, referring to FIG. 4A, the merchant has entered an amount of Rs. 350, which the merchant intends to receive from the user/customer.

At step 304, the payment terminal 102 receives an input to initiate a transaction with the external entity 104. As an example, again referring to FIG.4A, after entering the amount, the user of the payment terminal 102 presses the return key to provide the instant input. It may be noted that,

pressing of the return key may be interpreted as a confirmation of the amount discussed in the previous step, and the input discussed in the current step.

At step 306, in response to the initiation input, the payment terminal 102 (e.g. processing module 202 of the payment terminal 102) causes the first wireless communication module 214 (hereinafter referred to a BLE module 214 to facilitate easier reading of this document) and the second wireless communication module 216 (hereinafter referred to a NFC module 216 to facilitate easier reading of this document) to attempt to establish communication with an external entity 104. As an example, both the modules 214, 216 may be switched on in response to the initiation input and thereafter attempt to establish the communication channel. Alternatively, both the modules 214, 216 may already be on (but in "sleep" or "power saving" mode), but at this instance, begin attempting to initiate and thus establish the communication channel with the external entity 104.

At step 308, both the BLE module 214 and the NFC module 216 attempt to establish the communication channel. As an example, in the case of the BLE module 214, the BLE module 214 may begin broadcasting its identifier. On the other hand, in case of NFC module 216, the NFC module 216 generates electromagnetic field. It may be noted that, the merchant is not specifying which of the modules 214, 216 should be used, rather the payment terminal 102 is configured to use both the modules 214, 216 to attempt establishing of a communication channel, and in due course after authentication establish the communication channel via one of the suitable modules 214, 216.

Referring to the step 310 in FIG. 3B, it may be noted that, although it appears as if the external entity 104 is deciding whether the external entity 104 is NFC or BLE enabled, it would be well understood that the step 310 is presented only for the sake of explanation. It may be appreciated that, external entity 104, as discussed earlier, may be a NFC enabled card 104a (such as credit card, debit card, access card, corporate card or food card) or a portable communication device 104b (e.g., smartphone) with one or more of BLE or NFC capabilities. We will discuss the transaction flow in case of BLE enabled portable communication device 104b later. Now we discuss a scenario wherein the external entity 104 is a NFC enabled card 104a or a NFC enabled portable communication device 104b. It may be noted that, in case of portable communication device 104b

with NFC and BLE capabilities, which one of those should be used may be defined by default application settings, user defined settings in the application or availability of the module.

Referring to step 312, external entity 104 is in close proximity to the payment terminal 102 for detection. As an example, once the merchant has the payment terminal 102 ready to accept payment, the user/customer may bring the NFC card 104a or NFC device 104b close (to the extent required for NFC) to the payment terminal 102.

By way of explanation, in some embodiments the NFC card/device 104a, 104b carries encrypted data so that only the payment terminal 102 of the embodiment can interact correctly with the NFC card/device of the embodiment. This gives rise to a phenomenon known as "locking" the card/device.

Referring to step 314, the payment terminal 102 detects and attempts to unlock external entity 104 by authenticating it. Once authentication has been successfully carried out, a communication channel becomes established; that is, only after authentication has been successful will transaction data be sent.

Therefore, after detecting the NFC card 104a or NFC device 104b, the payment terminal 102 has established the communication channel with the external entity 104 using one of the first wireless communication module 214 and the second wireless communication module 216, based on which one of the communication modules 214, 216 is successful in initiating the communication channel with the external entity 104. In this case, payment terminal 102 has established the communication channel with the external entity 104 using the second wireless communication module 216 (NFC module 216). Hence the communication channel thus established may be referred to as NFC channel.

In the present embodiment, once a response to one of the BLE and NFC signals is received the payment terminal 102 terminates any attempt to establish communication channel with any other external entity using the first wireless communication module 214 and the second wireless communication module 216 until the said transaction is concluded.

In another embodiment, upon establishing a communication channel, that is not only receiving a response to the output signal from the payment terminal but also authenticating the external device so data communication may start, the payment terminal terminates the other, non-responded to communication module from further outputs until the present transaction is concluded.

Using the NFC channel that is established, the payment terminal 102 coordinates with the external entity 104 to unlock external entity 104. Known (or that may be developed in future) security technologies deployed at the card/device level and at the payment terminal 102 may be used for unlocking the NFC card 104a or NFC device 104b. In case the payment terminal 102 fails to unlock, then the transaction is, in the present embodiment, terminated (transaction concluded).

Referring to step 316, once unlocking is successful, the payment terminal 102 reads a user token from the card memory. The user token is data identifying a user attempting to make a payment connected to the transaction, analogous to a card number on a credit card.

In one embodiment, in addition to reading the user token, the external entity 104 stores data that is used as a one-time verifier. In this embodiment the stored one-time verifier is also read by the payment terminal 102 to improve security.

The one-time verifier may be understood as data unique for each transaction that is attempted. It may be further noted that, in case of NFC card 104a, a new onetime verifier may be written to the card 104a each time the existing one-time verifier is read by a payment terminal 102 to process a transaction. It may be further noted that, some smartphone may not allow writing this data to its NFC module, in which case the provision of one-time verifier as implemented in the foregoing example may not be provided.

By way of explanation, referring to Fig 5A, a transaction data packet 500 typically contains customer token 501, customer identifier 503, transaction amount 505 and merchant ID 507. If a hacker were able to sniff data when a user paid or tried to pay a bill for at a terminal, then it is possible that the hacker could can pay the same amount at the same terminal multiple times. This is referred to sometimes as a “replay attack”. So, it is desirable to differentiate between legit transactions and replay attacks.

In the present embodiment there is a safety mechanism in place to detect 'replay attacks'. In replay attacks, a hacker sniffs the data being exchanged between two devices and replays the same multiple times. In order for the system to be able to detect and flag such attacks, it is necessary to introduce something fresh into the data packet every single time. In the embodiment, see Fig 5B, this is achieved in one or both of a) maintaining and increment a counter on the card after each transaction, and b) sending the time stamp on the payment device as part of the data packet.

Thus, the packet 520 of the embodiment not only includes customer token 501, customer identifier 503, transaction amount 505 and merchant ID 507, but also the counter-number 509 stored on the card/device and also the time stamp 511 of the transaction.

In an embodiment, the data read from the NFC card 104a or NFC module of a mobile device 104b (or data communicated via BLE) includes data that enables the payment terminal 102 to identify whether the data it is gathering is from a NFC card 104a or a NFC module of a mobile device 104b (or via BLE of a mobile device). Therefore, the payment terminal 102 (or the server 106, or both) is capable of identifying whether the communication established is with one of a near field communication tag of the card 104a, a near field communication module of the portable communication device 104b or a personal area network module 214 of the portable communication device 104b. It may be noted that, such a provision enables the server 106 establish the data sets that are required to process the transaction. As an example, in case of NFC card 104a, a one-time verifier is required, whereas in case of NFC module from a mobile device 104b, the one-time verifier may not be required (due to the constraints discussed earlier) to process the transaction.

In an embodiment, the data read from the NFC card/device 104a, 104b or received via BLE includes location validation data. In other words, the payment terminal 102 receives location validation data from the external entity 104. The location validation data is used to verify whether payment can be accepted using the payment terminal 102.

In one embodiment data is written to the external entity 104, e.g. card 104a, and terminals are set to reject cards carrying that code except where the terminal is at the venue of concern. At

completely closed group payments environments like a corporate canteen, where the payment device is expected to accept payments from only one corporate(s), the check is done locally at the payment device level itself. If the device does not find the customer card populated with a specific identifier (identifying the corporate) then transaction is declined right away. A server call is not required).

In case it is determined that payment cannot be accepted, then the transaction is declined. On the other hand, if verified that payment can be accepted, then the transaction is processed. The verification that is being discussed may be carried out by the payment terminal 102.

Alternatively, the verification can be carried out by the server 106, or both.

In other cases where the payment devices are located in general retail, the check happens at the server 106. The customer identifier is also part of the data packet that is sent to the server. A rule is set at the back end that prohibits customers with a particular customer identifier from paying at a certain location (e.g. identified by merchant ID 507 which, it will be recalled, is also part of the transaction data packet).

As an implementation example, a company may have issued NFC cards 104a to its employees for use within the food court deployed in their campus. In case the card 104a is used to make a payment at a payment terminal 102 outside the campus, the payment terminal 102 (or server 106), upon reading the location validation data, may decline the transaction.

Now referring to step 318, the payment terminal 102 writes a new one-time verifier to the external entity 104. As an example, the new one-time verifier is written to the NFC card 104a. In case NFC module of the mobile device 104b allows such writing, then even in case of NFC enabled mobile device 104b, the new one-time verifier is written to the NFC module of the mobile device 104b in an embodiment. The new one-time verifier is used for the next transaction. The new one-time verifier may be a per-configured increment/decrement in comparison to the existing one-time verifier. Alternatively, the one-time verifiers may be a randomly generated code, which may be based on known logic. In an embodiment, the new one-time verifier is generated by the payment terminal 102. At step 320, the new one-time verifier is recorded in the NFC card 104a or NFC module of the mobile device 104b (if 1such provision is provided).

It should be noted that, the one-time verifier adds freshness to the data gathered from the external entity 104 for each transaction. As an example, in case only user token was to be gathered (as done conventionally), which is also constant, then a rogue system with access to the user token can misuse the user token to carryout transactions.

Referring to step 322, the payment terminal 102 bundles the user token, one-time verifier (if any), merchant ID, terminal ID, one-time verifier of payment terminal 102, source (NFC card/mobile or BLE) used to get user data and transaction information. In an embodiment, the payment terminal 102 may bundle the new one-time verifier as well. It may be noted that, apart from the one-time verifier corresponding to the external entity 104, there can be a one-time verifier for the payment terminal 102 as well. Hence, a rogue system with information (e.g., merchant ID or terminal ID) about the payment terminal 102 may still be presented with resistance in case of misuse. In an embodiment, the user may have to communicate a PIN as well to the payment terminal 102 to authorise the transaction. In some embodiment, PIN may be required only for transactions beyond a certain preconfigured amount.

Additionally, the payment terminal 102 may bundle authentication and security data along with other data to enhance the security features.

Referring to step 324, the payment terminal 102 sends the bundled information to the server 106. The payment terminal 102 may use WIFI module 2to send the information to the server 106. Alternatively, the payment terminal 102 may use GPRS module to send the information to the server 106. Alternatively, the payment terminal may encrypt the bundled information using the security module 213 for security purposes before communicating it to the server 106.

Referring to step 326, the server 106 receives the bundled information from the payment terminal 102.

Referring to step 328, the server 106 processes the transaction. The conventional steps involved in processing the transaction are not discussed, to prevent obscuring attention from steps that may be unconventional. The onetime verifier of the external entity 104 and one-time verifier of the payment terminal 102 are used to decide whether the payment request should be declined or

further processed. The one-time verifier (corresponding to payment terminal 102) is used to verify whether the one-time verifier is what is expected from the payment terminal 102 for the current transaction to either reject the transaction or proceed with the transaction. Likewise, the one-time verifier (corresponding to external entity 104) is used to verify whether the one-time verifier is what is expected from the external entity 104 for the current transaction to either reject the transaction or proceed with the transaction.

In an embodiment, the payment terminal 102 may even communicate the new one-time verifier corresponding to the external entity 104 to the server 106, so that the server 106 knows what to expect from the external entity 104 in the next transaction.

In an embodiment, the new one-time verifier of the external entity 104 or the payment terminal 102 is a known change compared to the previous one-time verifier. Hence, the e server 106 may just have to verify the one-time verifier with the previous one to either decline or proceed with the transaction.

In an embodiment, the server 106 communicates a new one-time verifier for the payment terminal 102 for use in the next transaction.

In case of absence of one-time verifier from the external entity 104, where it was expected, or wrong one-time verifier, the server 106 may block the external entity 104 from carrying out transaction, till the issue is resolved. Likewise, for the payment terminal 102.

Referring to step 330, the server 106 sends transaction information to the payment terminal 102. The transaction information may include information corresponding to successful payment or payment being declined. The transaction information may also include information corresponding to the amount being credited to the merchant's account and/or selected information about the user/customer who made the payment, among other information.

Referring to step 332, the payment terminal 102 receives the transaction information from the server 106. Some of the information that is received may be outputted (e.g., display) by the payment terminal 102. In some embodiments, some of the transaction information may be

prevented from being outputted by the payment terminal 102, whereas such information may be outputted on the external device 104 (e.g., phone).

Referring to step 334, once the transaction is concluded, the payment terminal 102 may be ready for the next transaction (e.g., start at 302).

Now referring to block 310, as may be recollected, we had previously provided the description considering that the user/customer may be using a NFC card 104a or NFC enabled smartphone 104b to make payment. Now we refer to a scenario wherein the user is using a portable communication device 104b (e.g., smartphone) with BLE capabilities to make the payment.

It should be understood that BLE is not essential to the invention, and other protocols would also work, for example "normal" Bluetooth or WiFi.

We may now also refer to FIG. 3E, along with other figures in the FIG. 3 series. As explained earlier, with reference with step 308, both NFC module 216 and BLE module 214 of the payment terminal may be attempting to establish a communication channel. As explained earlier, in the case of the BLE module 214, the BLE module 214 may begin broadcasting its identifier. The identifier may comprise data identifying compatibility.

As an example, referring to FIG 3E and FIG. 4B as well, the user opens a payment application in the portable communication device 104b and activates "pay now" icon. The application causes the BLE module of the BLE-enabled smartphone 104b to search (refer FIG. 4C) for payment terminals 102.

In an embodiment where there are plural payment terminals, the payment terminals typically radiate signals at the same strength, but of course it is highly unlikely that two terminals will be equidistant from any particular portable communication device (smartphone). The radiation of signals to indicate readiness to connect (pair) is sometimes referred to in the art as "advertising" and consists typically of emitting packets of data. The term "pair" is not intended to be restrictive.

The signal strength received at the portable communication device (smartphone) is measured by the smartphone, for example by the application running on the smartphone, and used to

determine the position of the smartphone relative to each of the payment terminals available in the vicinity.

As the first step of pairing, step 30, Fig 3E, the application scans the vicinity and makes a list of 'eligible candidates' that it can establish a connection with. The application is configured to ensure that the portable communication device (smartphone) only pairs with the intended payment terminal. Say for example, a merchant asks the customer to open the application and bring the phone close to payment terminal-A to initiate payment. The application then takes over and determines which payment terminal (among all the eligible payment terminals) is located closest to it. Since the merchant has asked the customer to bring their phone close to payment terminal-A, the application will see that payment terminal-A is only a few inches away whereas the others a few meters away and hence will request to pair with payment terminal-A.

The signal strength logic (establishing connection with the closest available payment terminal) is used ONLY to establish connection.

Once the phone pairs with the payment terminal and hence establishes a connection, the connection remains active up to the point when the application decides to cut off the connection. The connection remains active even when the phone is pulled back away from the terminal and the application continues to talk to the terminal to complete the transaction. Once the application determines that the transaction is complete, the application disconnects and releases the terminal.

The terminal is configured such that it cannot be paired with 2 phones simultaneously. Once a phone is paired or connected to the terminal, the communication channel between phone and terminal is exclusive. That is, no other phone can pair with or otherwise communicate with the terminal. The terminal is effectively locked to that phone and can only be unlocked (disconnected from the phone) by the application OR by physically resetting the payment terminal.

In an embodiment this “locking” is carried out by the terminal being configured to stop advertising when pairing takes place. In one example, the application on the smartphone issues an instruction to the terminal to stop advertising; in another example the terminal is configured to cease advertising without input from the smartphone as soon as pairing has taken place.

The processor of the payment terminal receives this instruction, and in response to stored instructions processes it and disables temporarily the advertising of its ability and presence to pair.

In an embodiment, the application of the smartphone 104b looks for compatible payment terminals 102 by looking at the data identifying compatibility present in the identifier. For example, there may be several BLE or BLUETOOTH devices that may be advertising, however, the application is only interested in identifying payment terminals 102 which may be considered for making payment (therefore be considered for sending a request to pair).

The user having moved the portable communication device proximate to a payment terminal so that signal strength is above the first threshold, as shown at FIG 3E, step 31, the smartphone 104b sends a request to that payment terminal 102 to pair.

In one embodiment the request to pair is only sent out, if strength of signal from the payment terminal 102 is above a first threshold.

In another embodiment, the request to pair is sent out as soon as the user activates the "pay now" icon, or similarly instructs the smartphone to commence a transaction.

In a further embodiment, the application displays an indication of one or more terminals to which pairing is possible for example on its display screen, and the user selects one of these, the selection causing a request to pair sequence to initiate.

As an example, consider a merchant location with multiple compatible payment terminals 102. The application of the smartphone 104b would identify and shortlist all of these payment terminals 102, however it has to decide to which one among those a request to pair has to be sent.

In an embodiment, even in a scenario wherein a single payment terminal 102 is identified, the request to pair is not sent unless the signal strength is above the first threshold. In practice, the user experience would be similar to "tap-and-pay" even when using BLE as a channel to make payment. The user takes the smartphone 104b close (refer FIG. 4D) to the payment terminal 102 resulting in increase in the signal strength, and thereby causing the application to request pairing

with the payment terminal 102. Hence, it is to be understood that the smartphone 104b sends a request automatically to establish a communication channel with the personal area network module 214 of the payment terminal 102, if signal strength of the broadcasted identifier is over the first threshold.

The first threshold is configured such that the portable communication device 104a and the payment terminal 102 are within a preconfigured distance of each other to establish the communication channel. The first threshold may be reconfigured remotely via a software update, or may be configured at the payment terminal 102.

In an embodiment, the first threshold is configured such that the portable communication device 104b and the payment terminal 102 are within approximately 20 centimetres of each other to establish the communication channel.

In another embodiment, the first threshold is configured such that the portable communication device 104b and the payment terminal 102 are within approximately 10 centimetres of each other to establish the communication channel.

It is to be understood that, with the configuration of the first threshold, we are able to set an approximate distance between the portable communication device 104b and the payment terminal 102 to proceed with pairing.

At FIG 3E, step 32, the payment terminal 102 receives the request to pair. The payment terminal 102, on receiving the request, co-ordinates with the smartphone 104b using well known protocol, to successfully pair or decline request. In case pairing is successful, the payment terminal 102 has established the communication channel (BLE channel) with the external entity 104 using the first wireless communication module 214 (BLE module 214). Hence the communication channel thus established may be referred to as BLE channel.

Once communication channel is established (paired), the smartphone continues to retain communication with the personal area network module of the payment terminal 102 if signal strength between the smartphone 104b and the personal area network module 214 of the payment terminal 102 falls below the first threshold. In practice, the user brings the smartphone

104b close to the payment terminal 102, causing the smartphone 104b to pair with the payment terminal 102.Thereafter, the user may pull back the smartphone 104b, but communication channel will be retained improving the user's experience and making the transaction process more reliable.

In an embodiment, at least one of the payment terminal 102 or the smartphone 104b is configured to terminate the established communication channel, if the signal strength in the channel between the smartphone 104b and the personal area network module 214 of the payment terminal 102 falls below a second threshold. The second threshold may be controllable. The second threshold may be reconfigured remotely or at the device.

At FIG 3E, step 33, the payment terminal 102 sends transaction information to the smartphone 104b. The information is sent via the BLE channel. Such information may include amount to be transferred and merchant information, among others.

At FIG 3E, step 34 and FIGs. 4D and 4E, the smartphone 104b receives the transaction information sent by the payment terminal 102.

At FIG 3E, step 3and FIG. 4E, the user may activate an icon, thereby causing the smartphone 104b to send approval for payment and communicate data to facilitate the transaction. The data that is communicated (in addition to relevant data that was discussed in the context of NFC) may include real time data as well. Real time data may include data corresponding to time. The one-time verifier may be generated by the smartphone 104b. In an embodiment, the user may have to communicate a PIN as well to authorise the transaction. In some embodiment, PIN may be required only for transactions beyond a certain preconfigured amount.

At FIG 3F, step 36, the payment terminal 102 receives the approval and the data, and steps discussed earlier in connection with step 322 and subsequent steps may be carried out, as may be adapted for this mode of transaction.

Now specifically referring to the steps 332 (FIG. 3D), 37 and 38 (FIG. 3F), the payment terminal 102 receives transaction information from the server 106. It may be noted that, as discussed earlier, the server 106, based on the data received knows that the data was received by the payment

terminal 102 via BLE channel. Hence, the BLE channel can be used to provide an update, corresponding to the transaction, to the user. Therefore, apart from the typical data sent by the server 106, the server 106 sends and the payment terminal 102 receives data corresponding to the account balance of the user making a payment using the smartphone 104b. The payment terminal 102, via the BLE channel, communicates the data corresponding to the account balance to the smartphone104b (refer FIG. 4G). Therefore, the user is not only able to make the payment without using the Internet, but also get an update on the transaction, without using the Internet.

Having completed step 38, the application running on the smartphone 104 sends a command over the communication channel with the payment terminal 102. This command instructs the terminal to start advertising so that further transactions with other smartphones is possible. The command is received by the payment terminal and is processed by the processing circuitry of the payment terminal in accordance with instructions stored in memory of the terminal so that advertising resumes.

In one embodiment, the terminal 102 is also provided with a physical reset device, for example a reset key so that a merchant can re-enable advertising if required. In another embodiment the reset may be carried out remotely, but this might in some cases be less secure than using a physical reset device.

The reset key, when operated can cause the payment terminal to reboot into a quiescent state in which it can start advertising, or may simply override the “stop advertising” command and send to the processing circuitry a “resume advertising” command.

In an embodiment, the payment terminal 102 is further configured to receive, from the server 106, data corresponding to transaction information, and communicate at least a part of the data corresponding to the transaction information to the smartphone 104b via the communication channel.

In an embodiment, the payment terminal 102 is incapable of displaying the account balance of the user; however, the portable communication device 104b is configured to display the account balance of the user post the transaction. Data corresponding to the account balance may be encrypted such that only the user’s smartphone 104b is capable of decrypting said data.

It shall be noted that, some of the encryption, decryption, authentication and security technologies that are typically used at different steps are not discussed, so as not to unnecessarily obscure aspects of the embodiments.

The processes described above is described as a sequence of steps, this was done solely for the sake of illustration. Accordingly, it is contemplated that some steps may be added, some steps may be omitted, the order of the steps 1may be re-arranged, or some steps may be performed simultaneously.

The example embodiments described herein may be implemented in an operating environment comprising software installed on a computer, in hardware, or in a combination of software and hardware.

Although embodiments have been described with reference to specific example embodiments, it will be evident that various modifications and changes may be made to these embodiments without departing from the broader spirit and scope of the system and method described herein. Accordingly, the specification and drawings are to be regarded in an illustrative rather than a restrictive sense.

It will be appreciated that the invention has been described by way of example only. Various modifications may be made to the techniques described herein without departing from the spirit and scope of the appended claims. The disclosed techniques comprise techniques which may be provided in a stand-alone manner, or in combination with one another. Therefore, features described with respect to one technique may also be presented in combination with another technique.

CLAIMS

1. A method of operating a payment terminal comprising:- receiving an activation input, and in response thereto outputting a first wireless signal for communicating with an external payment device of a first type and a second wireless signal for communicating with an external payment device of a second type, wherein the first and second wireless signals are formatted in respective mutually different first and second protocols, receiving a reply to one of the first and second wireless signals and in response to the reply, terminating outputting of the other of the first and second wireless signals.

2. The method of claim 1, further comprising processing the reply to authenticate the external payment device to thereby establish a communication channel.

3. The method of claim 1, further comprising processing the reply to authenticate the external payment device, and after the processing step implementing the terminating step.

4. The method of claim 1, wherein the wireless signals comprise an NFC signal and a Bluetooth signal.

5. The method of claim 1, further comprising processing the reply to authenticate the external payment device to thereby establish a communication channel and receiving from the communication channel data indicative of a user; receiving, at an input, data indicative of a transaction amount and transferring the data indicative of a user and data indicative of a transaction amount to a server.

6. The method of claim 1, further comprising processing the reply to authenticate the external payment device to thereby establish a communication channel and receiving from the communication channel data indicative of a user and a one-time verifier for identifying a current transaction; receiving, at an input, data indicative of a transaction amount, transferring the data indicative of a user, data indicative of the one-time verifier and data indicative of a transaction amount to a server.

7. The method of claim 6, further comprising outputting a new one-time verifier over the communication channel.

8 The method of claim 1, further comprising communicating with a server information indicative of which of the first and second wireless signals is responded to.

9. A payment terminal for communicating wirelessly with an external device having a processing device and a store holding instructions to control the processing device to cause the payment terminal to respond to an activation input to output a first wireless signal for communicating with an external payment device of a first type and a second wireless signal for communicating with an external payment device of a second type, wherein the first and second wireless signals are formatted in respective mutually different first and second protocols, and in response to receiving a reply to one of the first and second wireless signals to terminate outputting of the other of the first and second wireless signals.

10. The payment terminal of claim 9, further having a keypad for providing the activation signal, a display for displaying information under control of the processing device, and an output device for communicating with a server.

11. The payment terminal of claim 9, having a first wireless device configured to output the first wireless signal and a second wireless device configured to output the second wireless signal, both under control of the processing device.

12 The payment terminal of claim 9, further having a security device comprising a store for security keys, the security device being configured to use the keys to encrypt or decrypt data for use by the terminal.

13. The payment terminal of claim 9, having a personal area network device configured to output the first wireless signal.

14. The payment terminal of claim 9, having a near field communication device configured to output the second wireless signal.

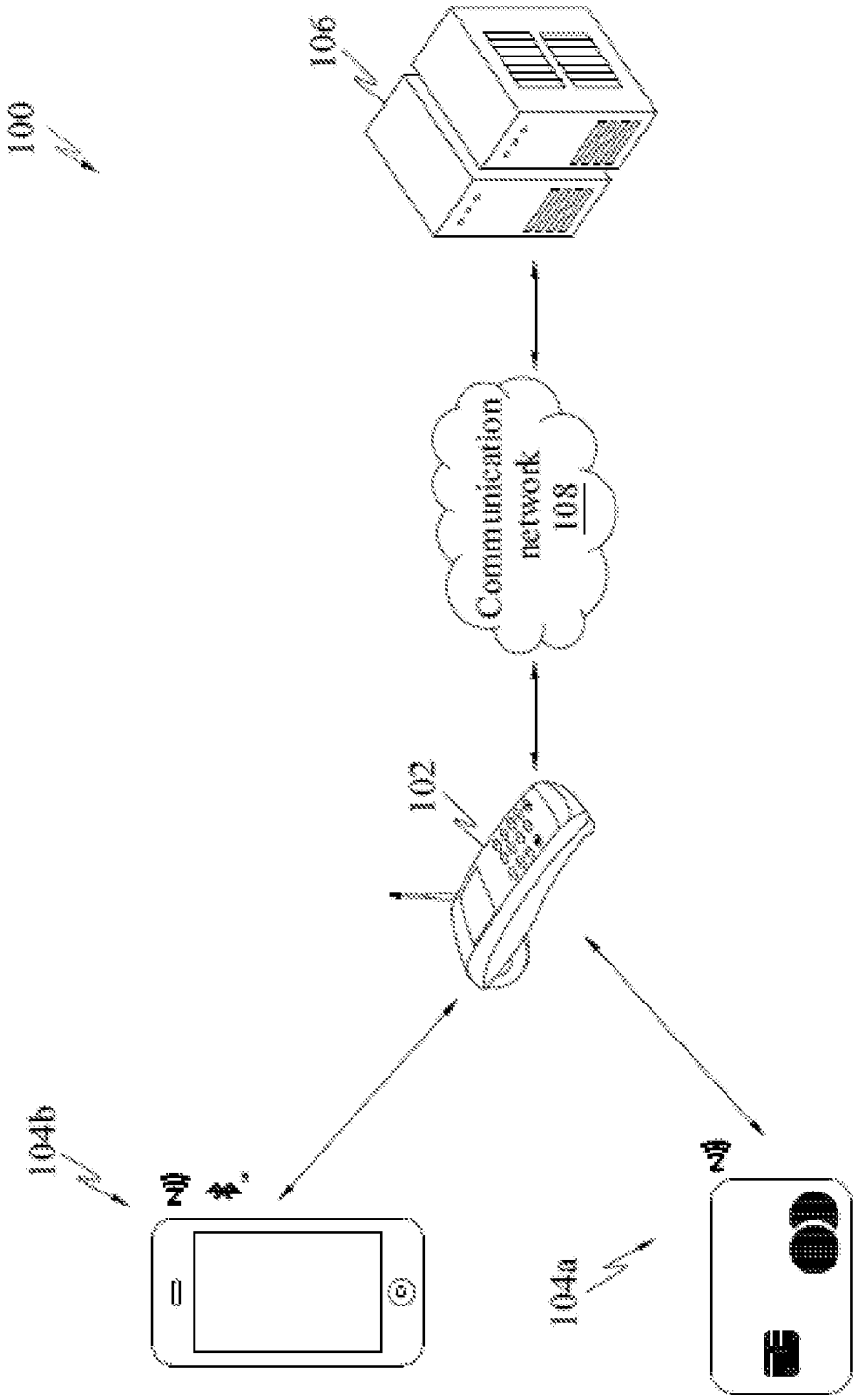

FIG. 1

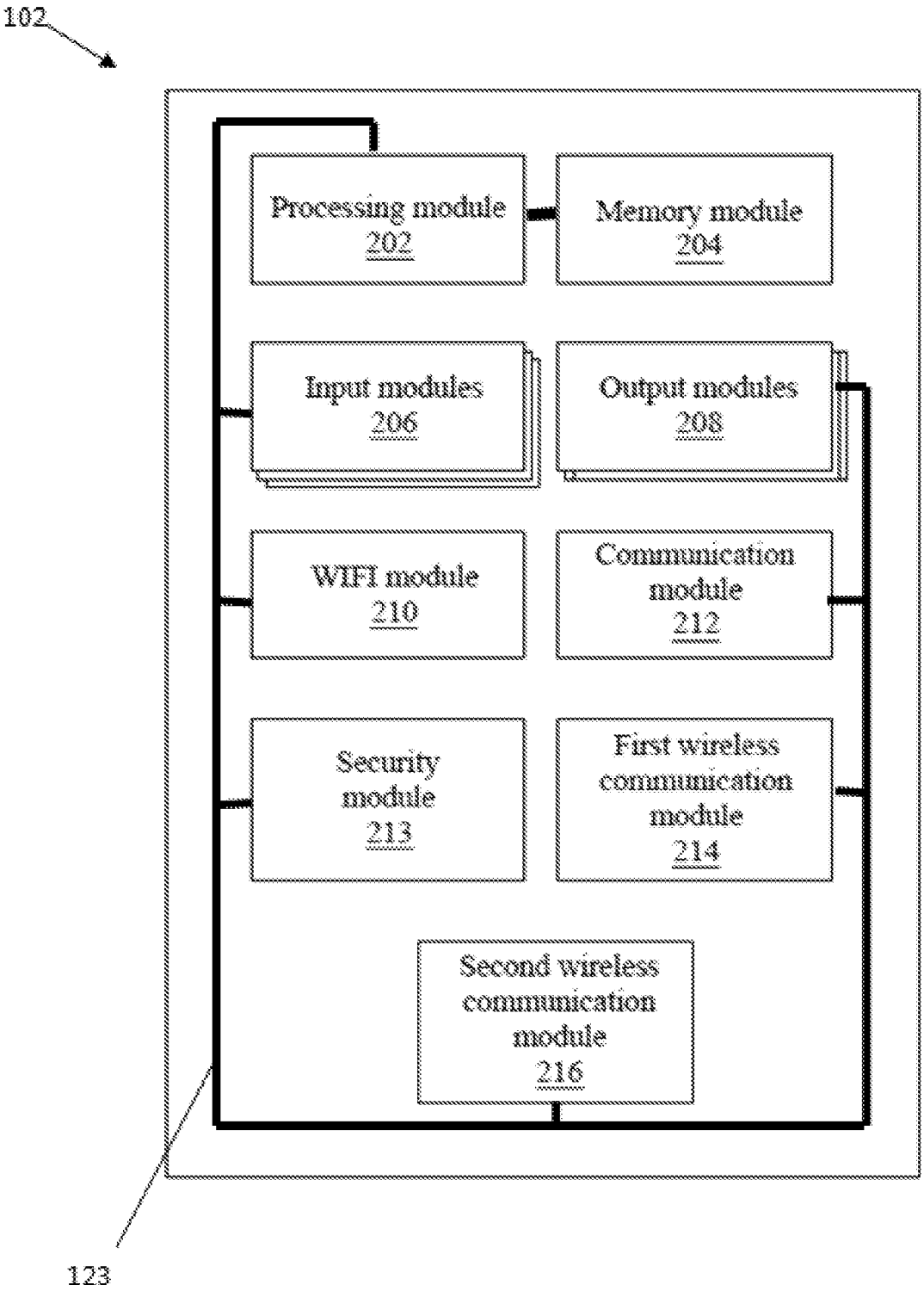
102
Processing module
202
Memory module
204
Input modules
206
Output modules
208
WIFI module
210
Communication module
212
Security module
213
First wireless communication module
214
Second wireless communication module
216
123

FIG 2

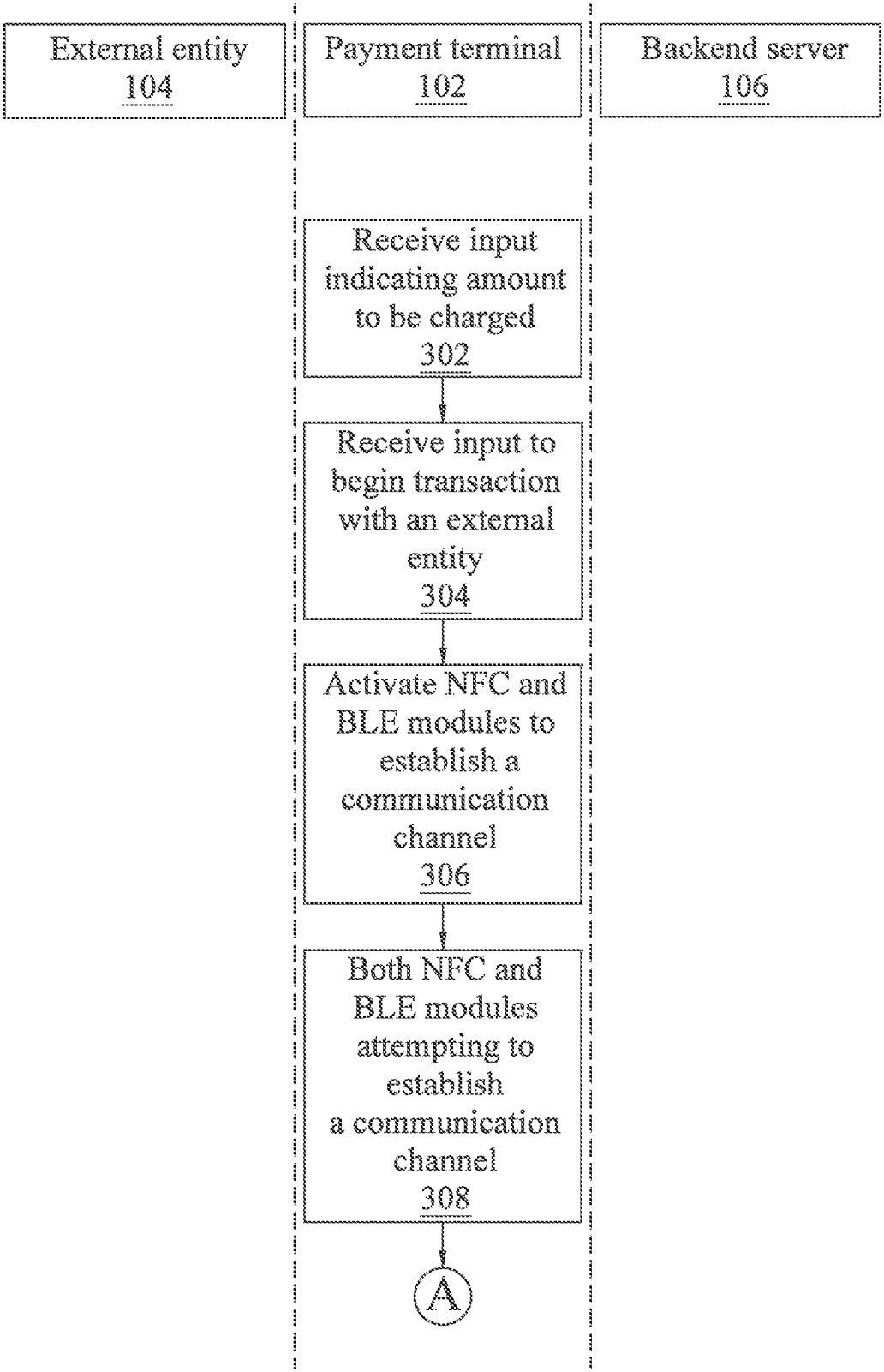
External entity
104
Payment terminal
102
Backend server
106
Receive input indicating amount to be charged
302
Receive input to begin transaction with an external entity
304
Activate NFC and BLE modules to establish a communication channel
306
Both NFC and BLE modules attempting to establish a communication channel
308
A

FIG. 3A

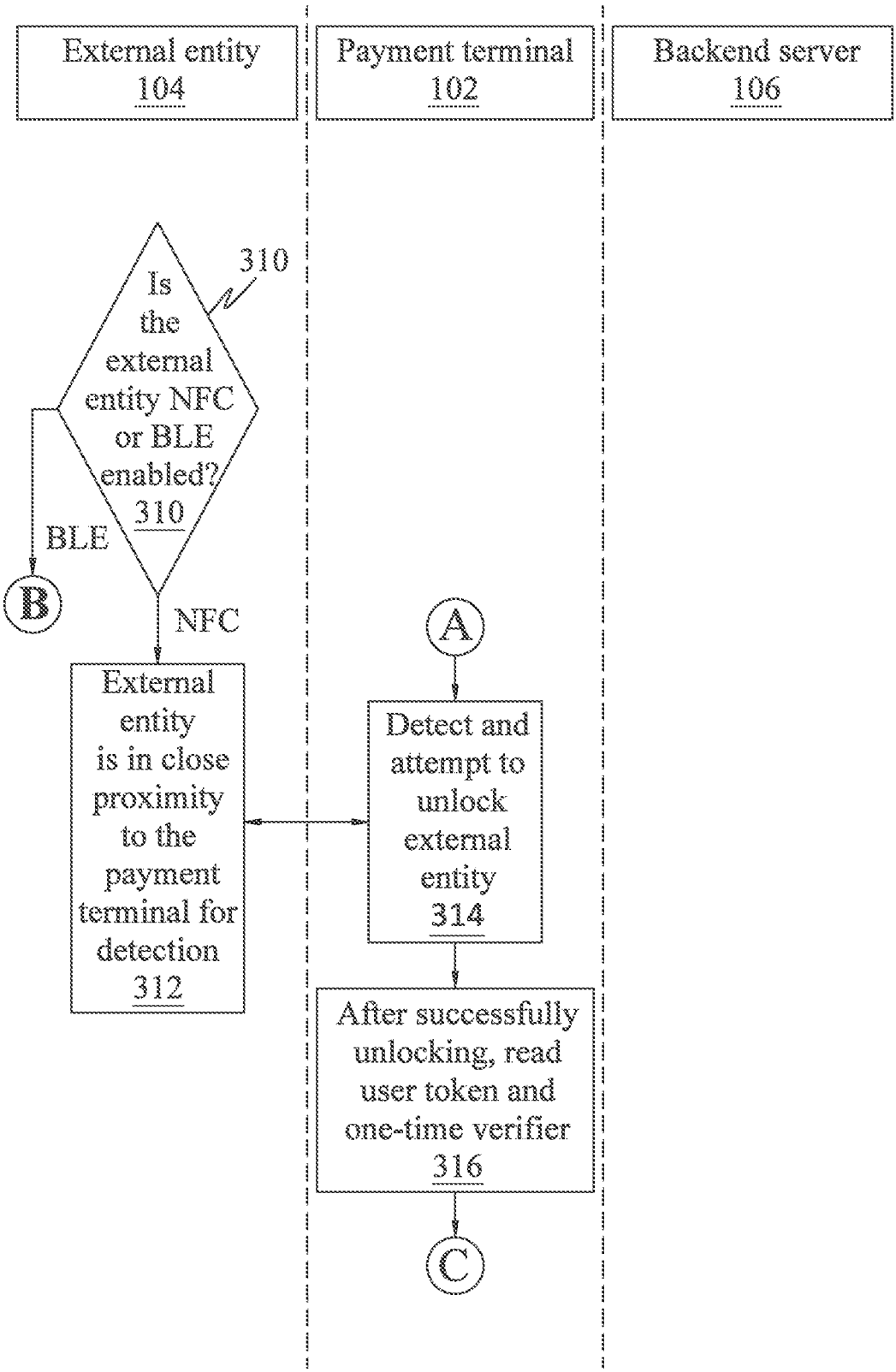
External entity
104
Payment terminal
102
Backend server
106
Is the external entity NFC or BLE enabled?
310
310
BLE
NFC
B
A
External entity is in close proximity to the payment terminal for detection
312
Detect and attempt to unlock external entity
314
After successfully unlocking, read user token and one-time verifier
316
C

FIG. 3B

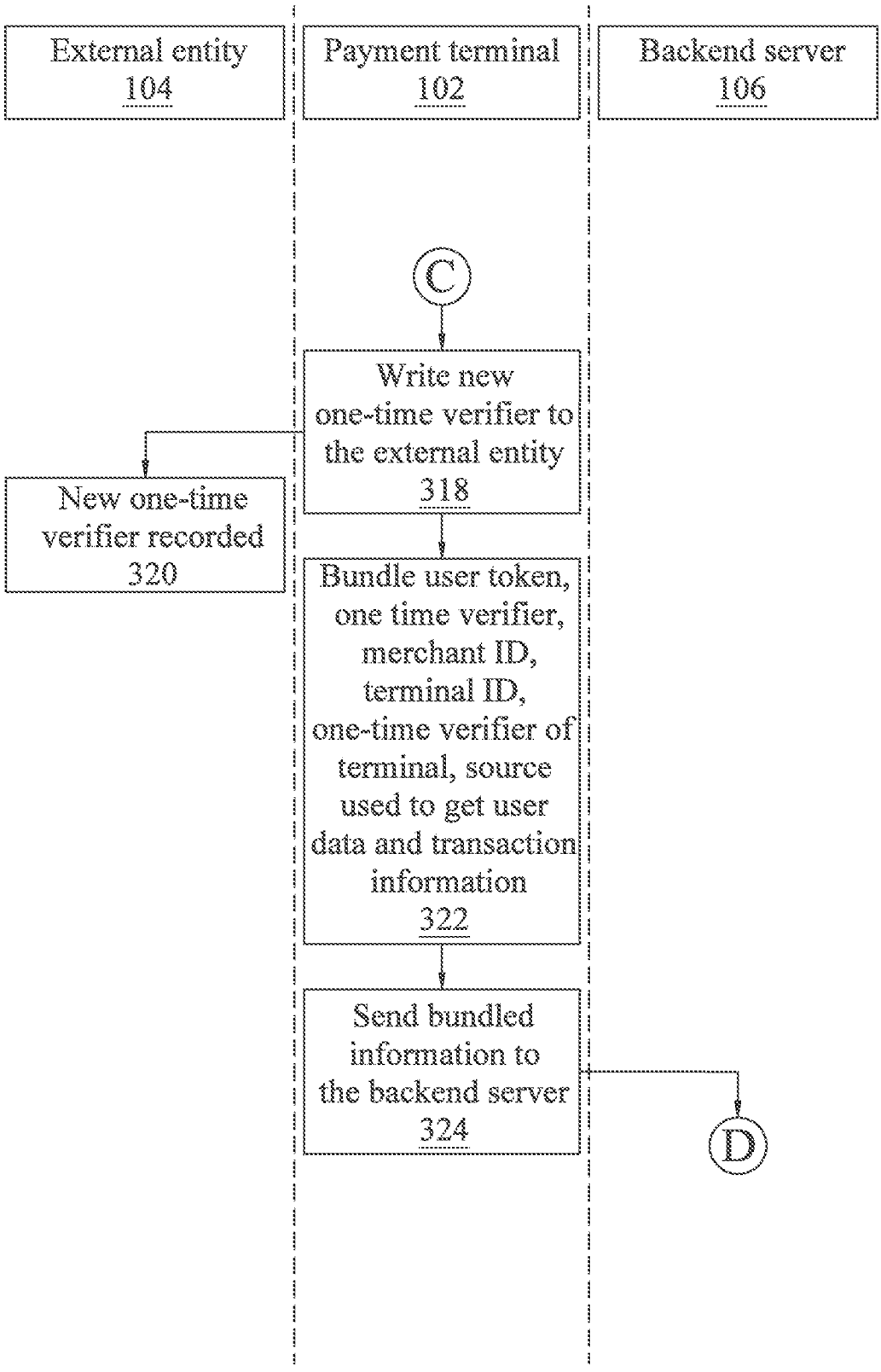
External entity
104
Payment terminal
102
Backend server
106
C
Write new one-time verifier to the external entity
318
New one-time verifier recorded
320
Bundle user token, one time verifier, merchant ID, terminal ID, one-time verifier of terminal, source used to get user data and transaction information
322
Send bundled information to the backend server
324
D

FIG. 3C

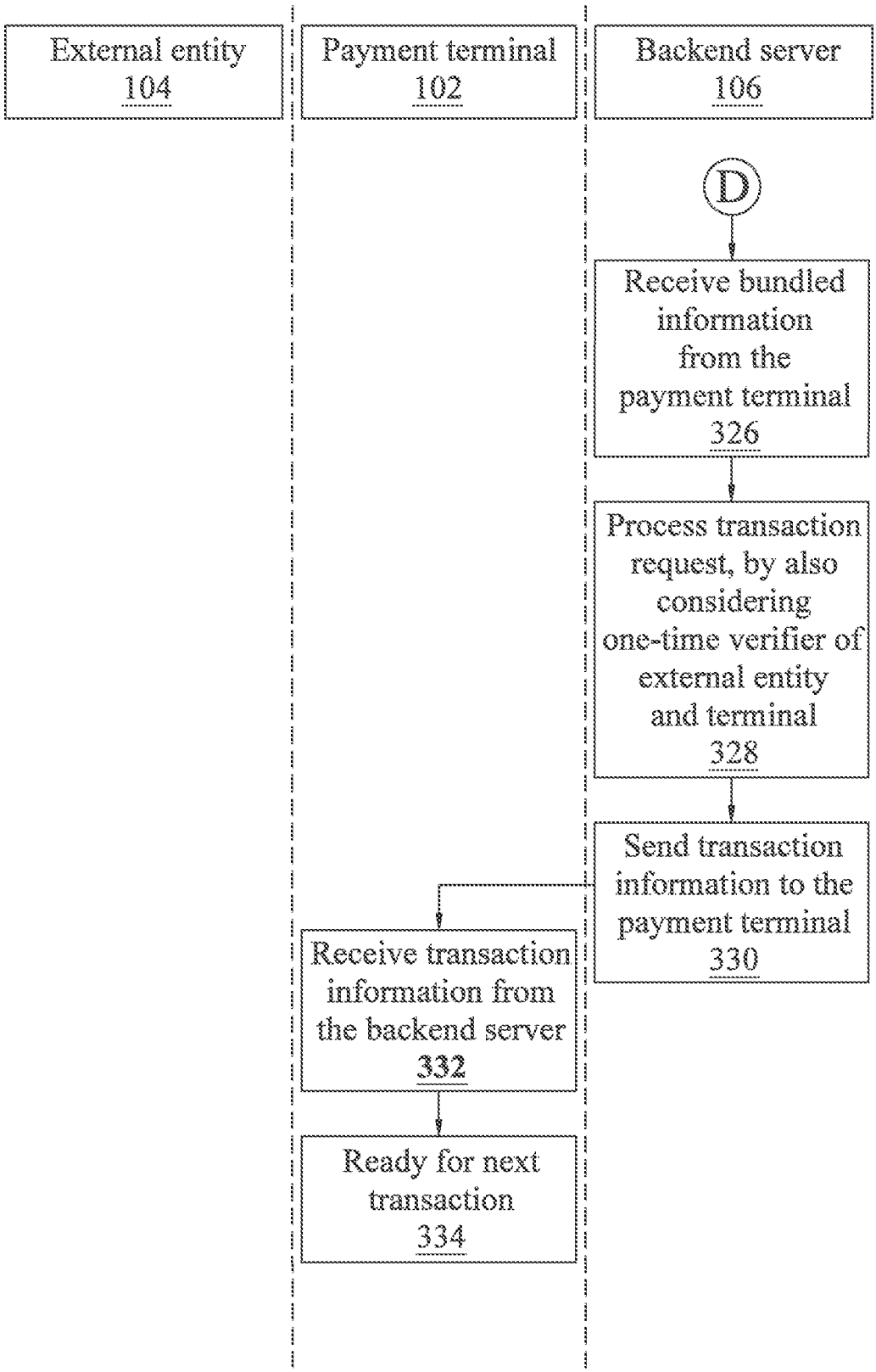
External entity
104
Payment terminal
102
Backend server
106
D
Receive bundled information from the payment terminal
326
Process transaction request, by also considering one-time verifier of external entity and terminal
328
Send transaction information to the payment terminal
330
Receive transaction information from the backend server
332
Ready for next transaction
334

FIG. 3D

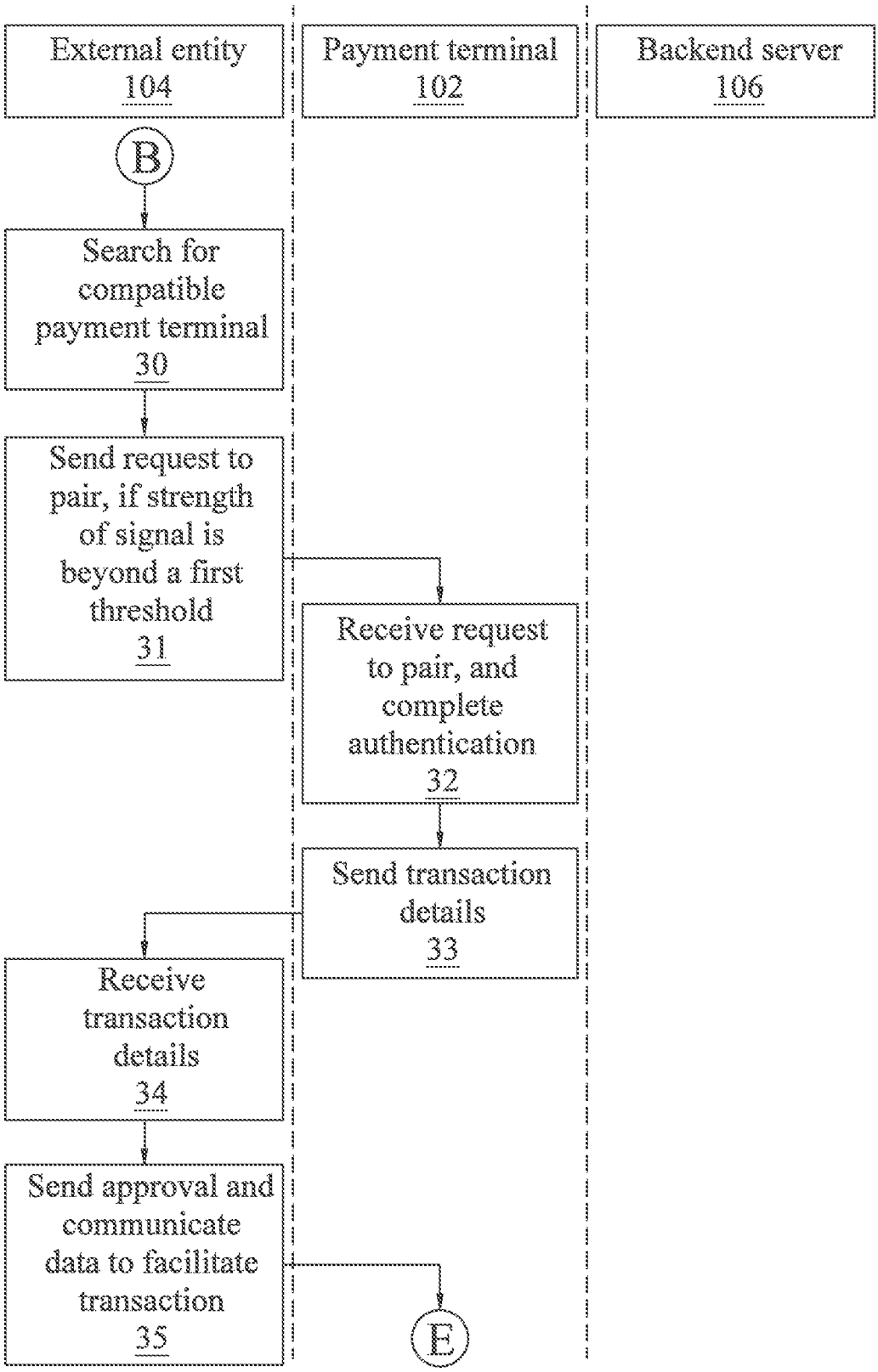
External entity
104
Payment terminal
102
Backend server
106
B
Search for compatible payment terminal
30
Send request to pair, if strength of signal is beyond a first threshold
31
Receive request to pair, and complete authentication
32
Send transaction details
33
Receive transaction details
34
Send approval and communicate data to facilitate transaction
35
E

FIG. 3E

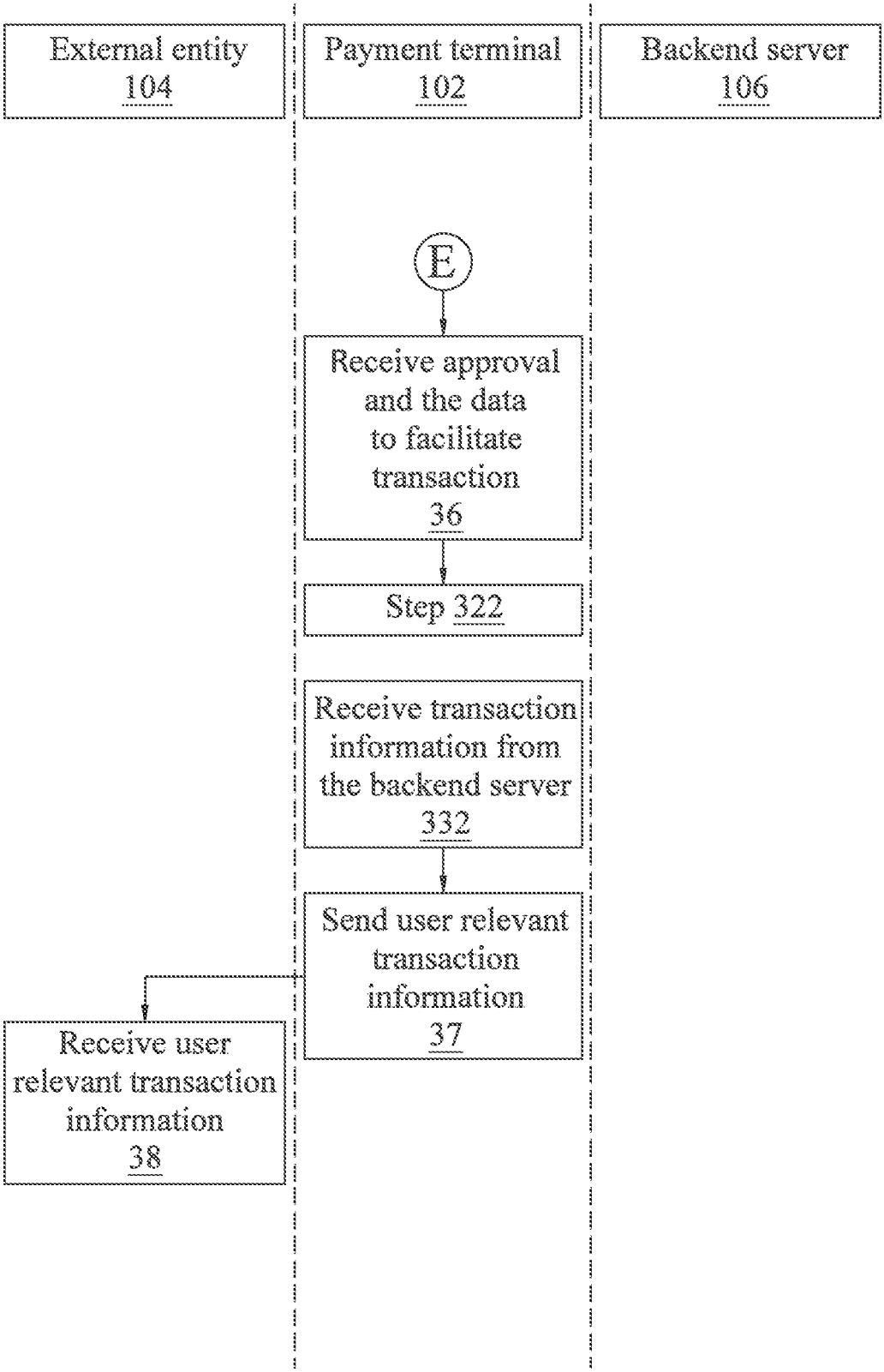
External entity
104
Payment terminal
102
Backend server
106
E
Receive approval and the data to facilitate transaction
36
Step 322
Receive transaction information from the backend server
332
Send user relevant transaction information
37
Receive user relevant transaction information
38

FIG. 3F

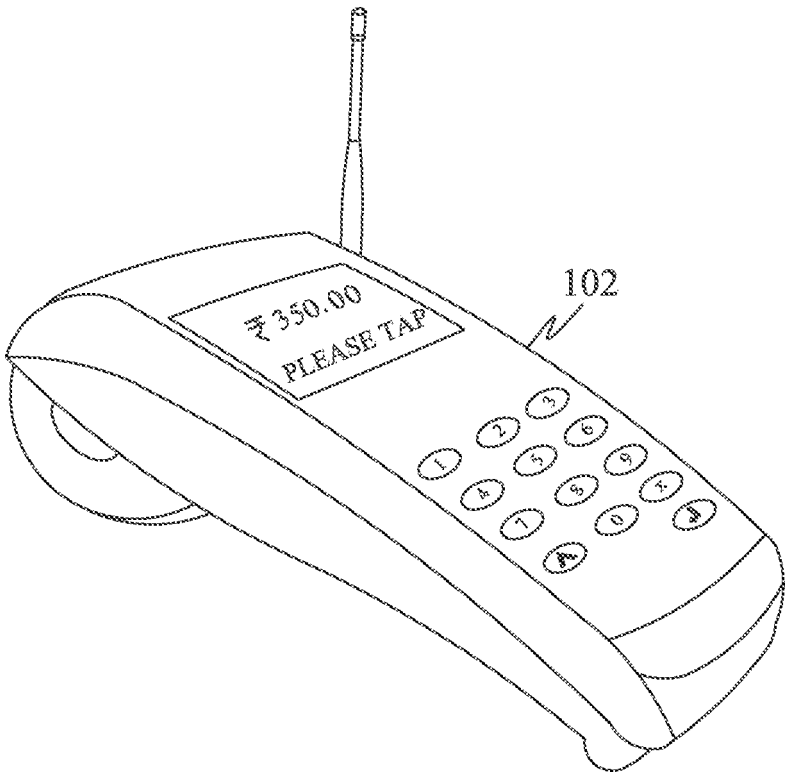

FIG. 4A

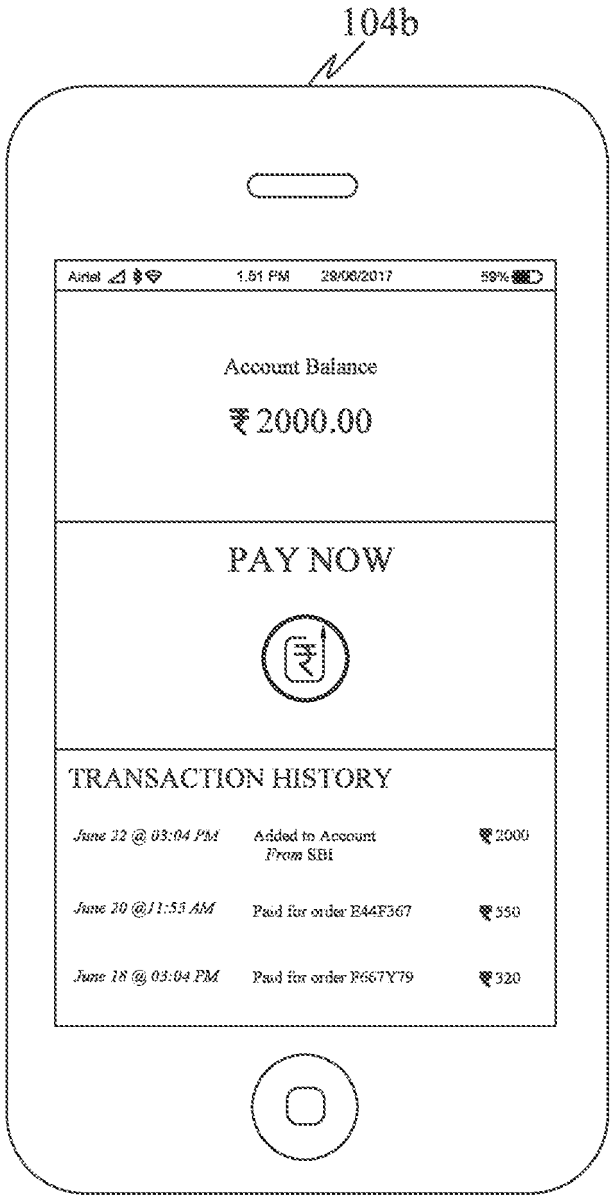
104b
Airtel
1.51 PM
28/06/2017
59%
Account Balance
₹ 2000.00
PAY NOW
TRANSACTION HISTORY
June 22 @ 03:04 PM
Added to Account From SBI
₹ 2000
June 20 @11:53 AM
Paid for order B44F367
₹ 550
June 18 @ 03:04 PM
Paid for order F667Y79
₹ 320

FIG. 4B

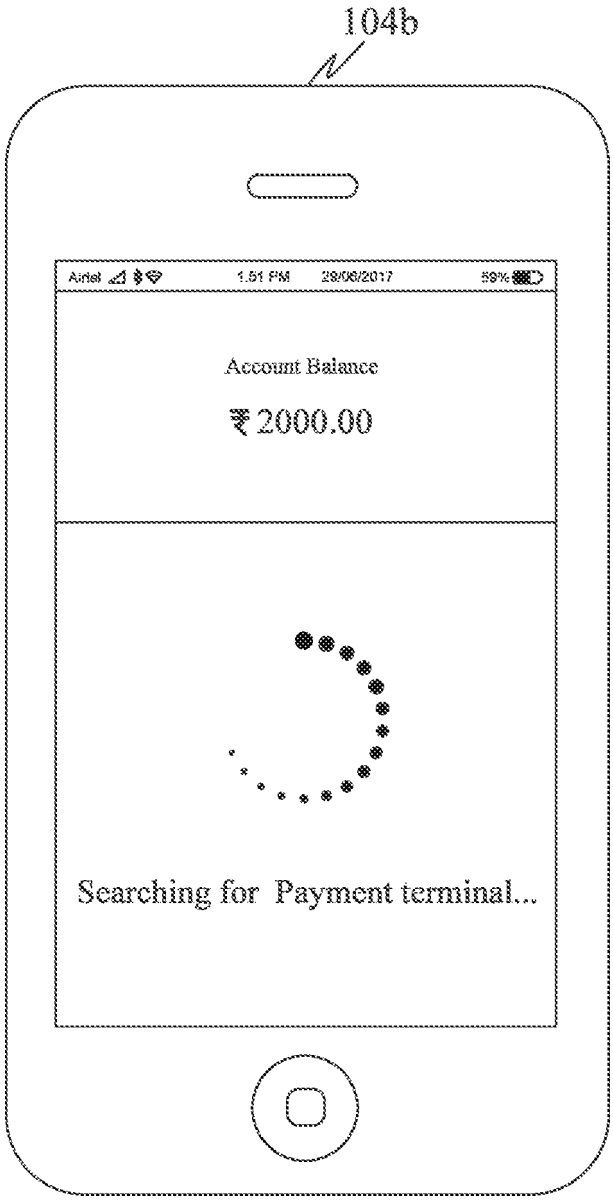
104b
Airtel
1.51 PM
28/08/2017
59%
Account Balance
₹ 2000.00
Searching for Payment terminal...

FIG. 4C

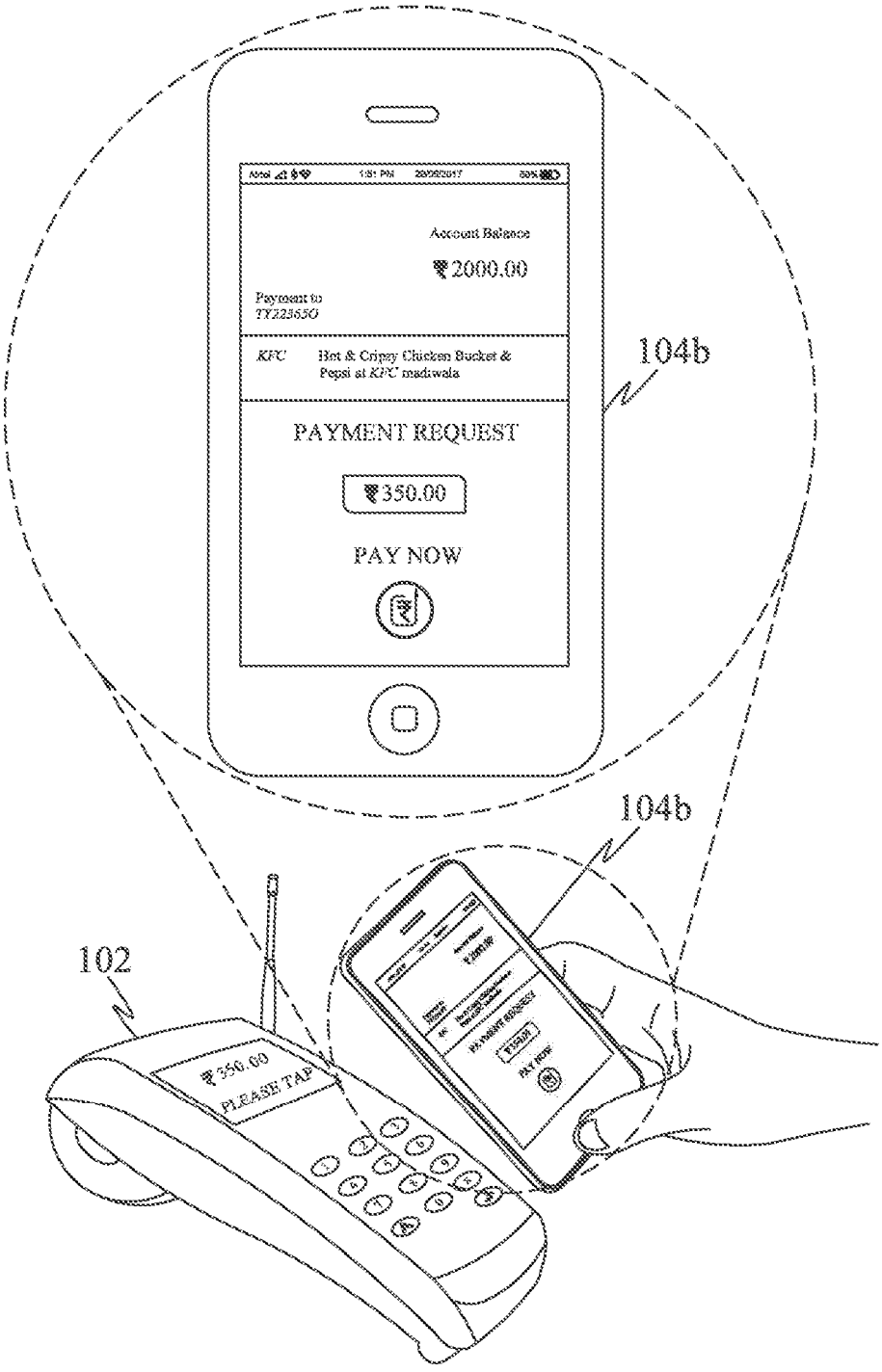
Account Balance
₹2000.00
Payment to
TY223650
KFC
Hot & Crispy Chicken Bucket &
Pepsi at KFC madiwala
PAYMENT REQUEST
₹350.00
PAY NOW
104b
104b
102
₹350.00
PLEASE TAP

FIG. 4D

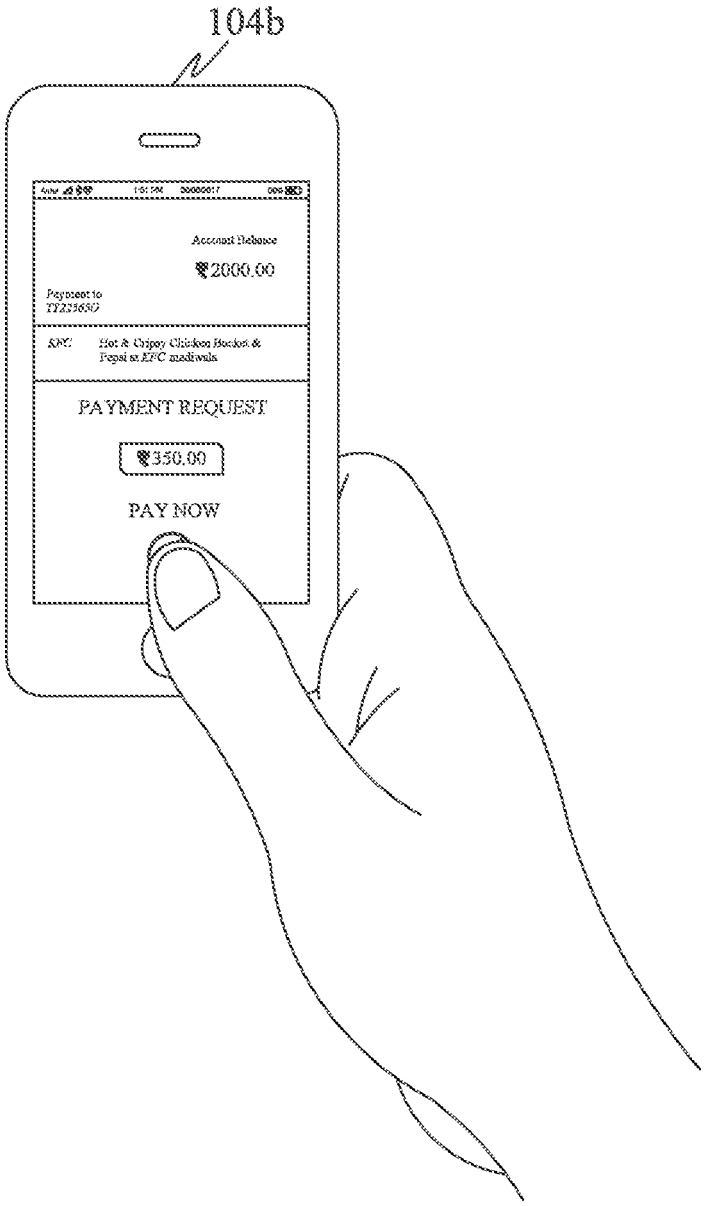
104b
Account Balance
2000.00
Payment to
TY23568O
KFC
Hot & Crispy Chicken Bucket &
Pepsi at KFC madiwala
PAYMENT REQUEST
350.00
PAY NOW

FIG. 4E

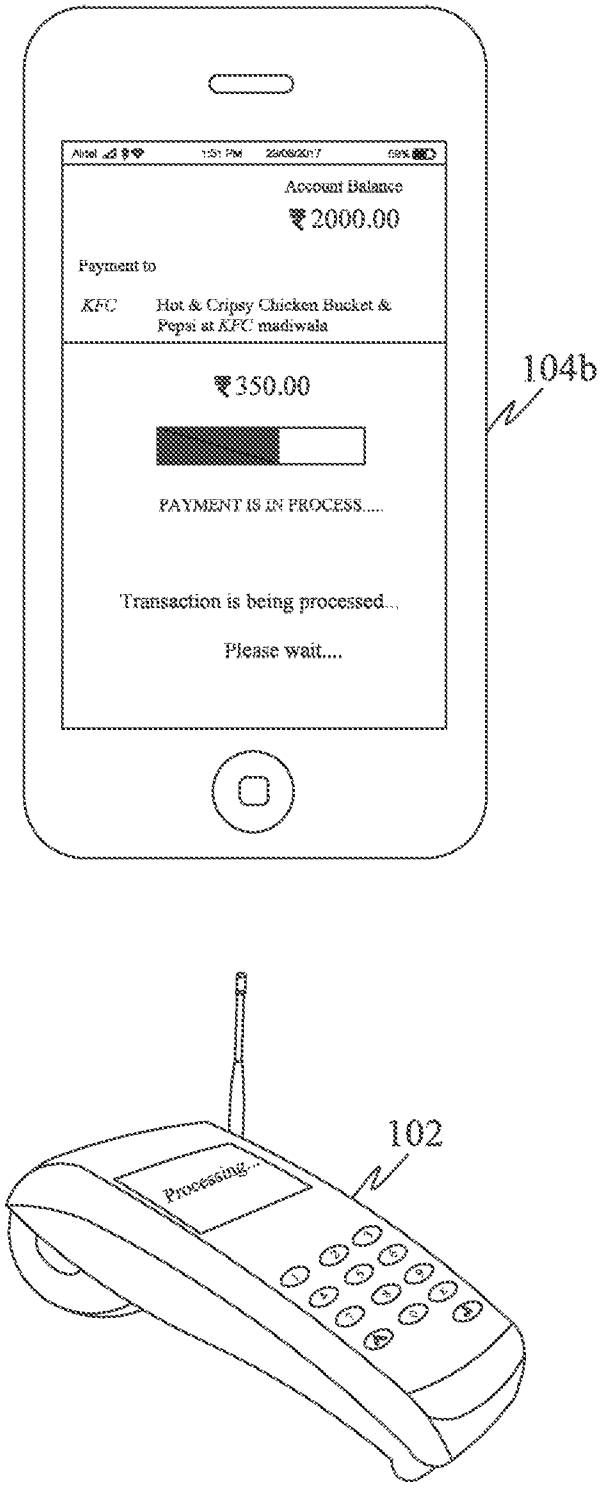
Account Balance
₹2000.00
Payment to
KFC
Hot & Cripsy Chicken Bucket & Pepsi at KFC madiwala
₹350.00
PAYMENT IS IN PROCESS.....
Transaction is being processed...
Please wait....
104b
Processing...
102

FIG. 4F

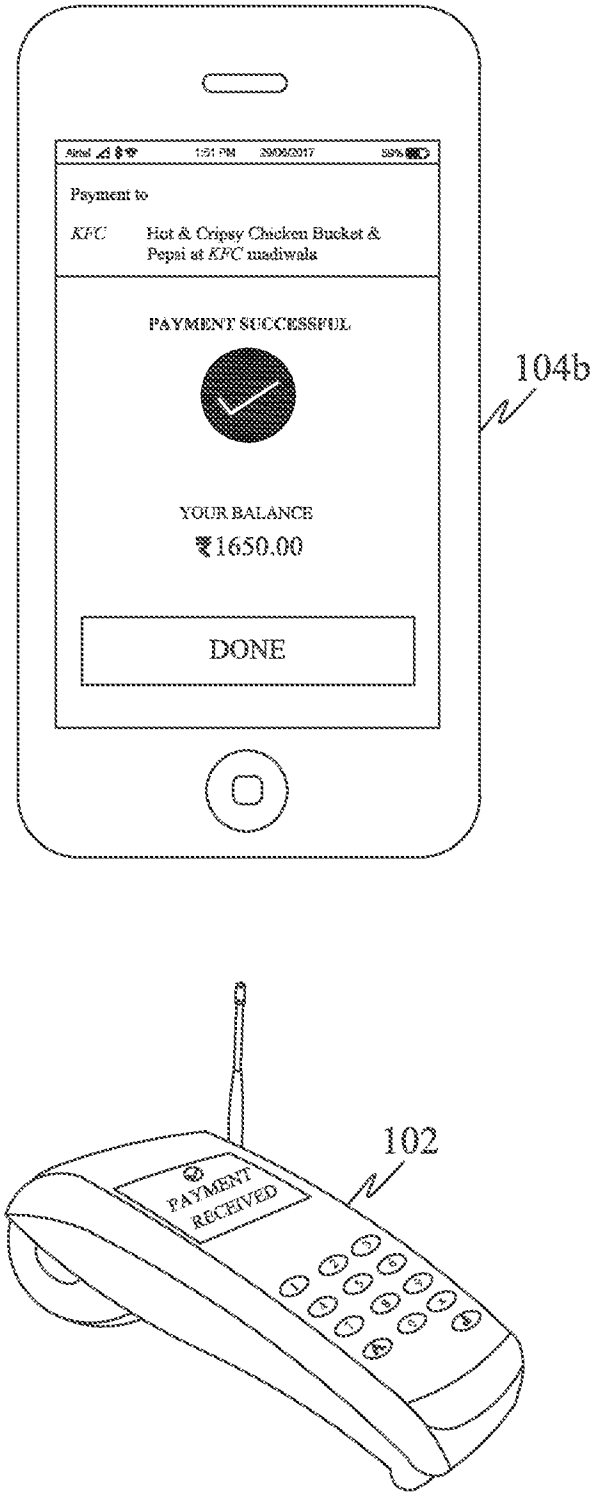
Payment to
KFC
Hot & Crispy Chicken Bucket & Pepsi at KFC madiwala
PAYMENT SUCCESSFUL
YOUR BALANCE
₹1650.00
DONE
104b
PAYMENT RECEIVED
102

FIG. 4G

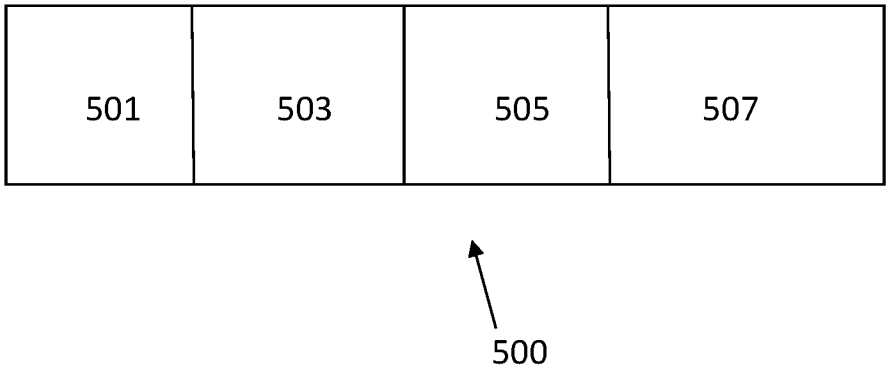

FIG 5A

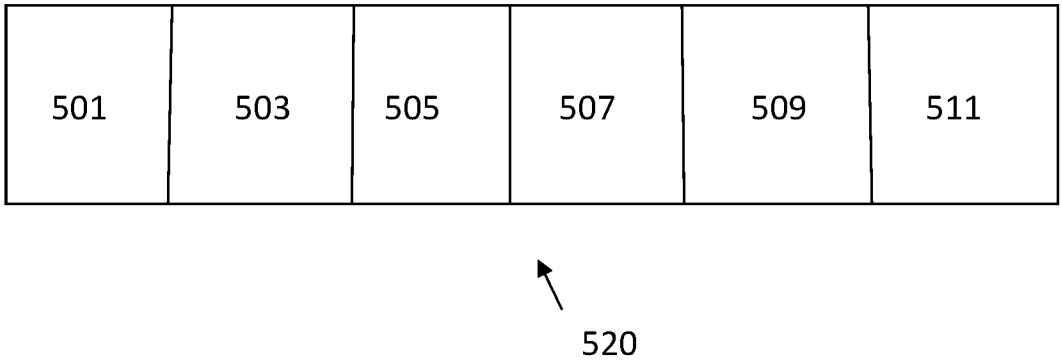

FIG 5B

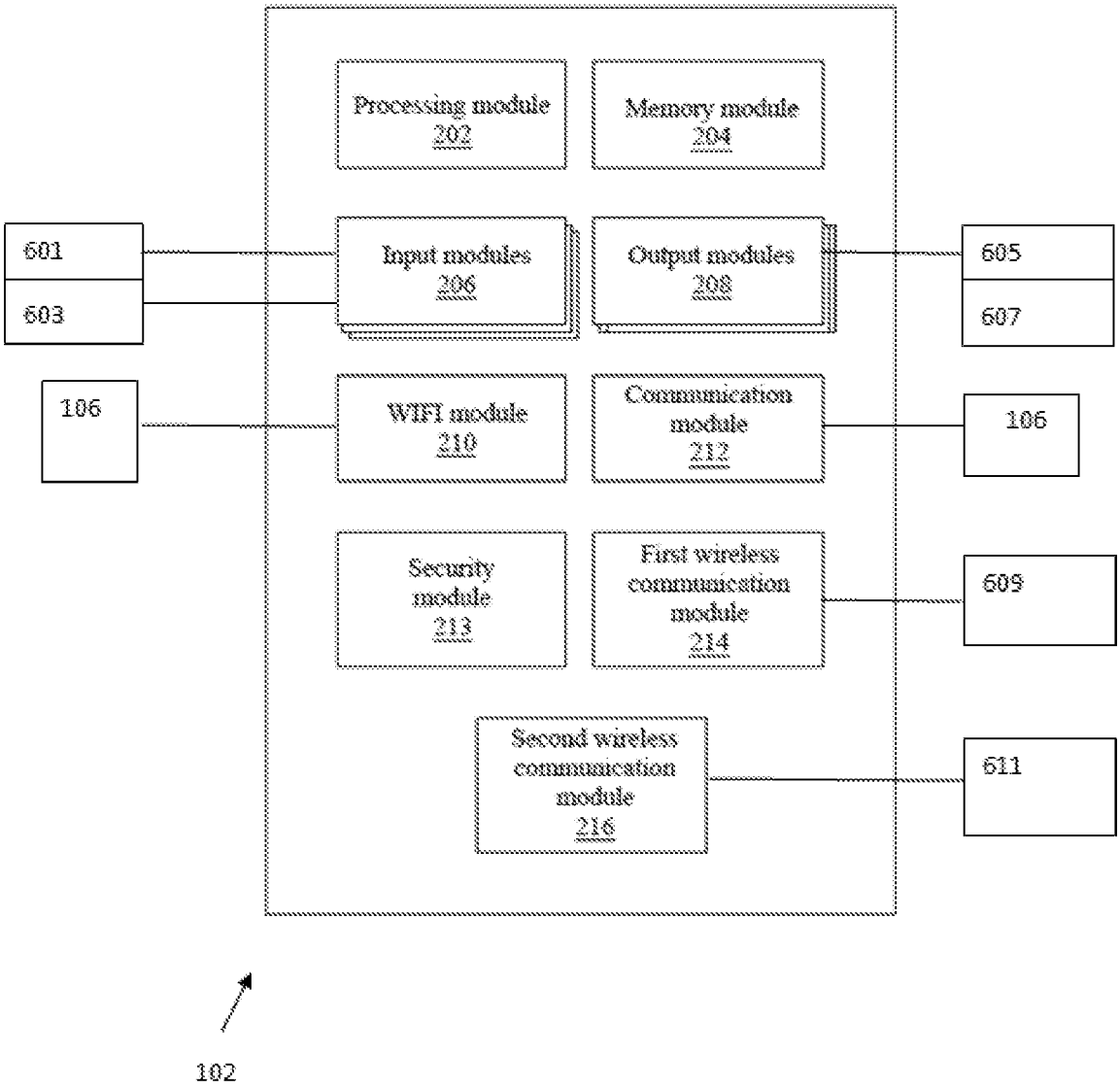
Processing module
202
Memory module
204
601
603
Input modules
206
Output modules
208
605
607
106
WIFI module
210
Communication module
212
106
Security module
213
First wireless communication module
214
609
Second wireless communication module
216
611
102

FIG 6