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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
29 January 2015 (29.01.2015)

WIPO | PCT

(10) International Publication Number
WO 2015/011655 A1

(51) International Patent Classification:
G06Q 20/40 (2012.01) *G06Q 20/32* (2012.01)
G06Q 20/12 (2012.01)

(21) International Application Number:
PCT/IB2014/063339

(22) International Filing Date:
23 July 2014 (23.07.2014)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

2013/05673	26 July 2013 (26.07.2013)	ZA
2013/06923	16 September 2013 (16.09.2013)	ZA

(71) Applicant: VISA INTERNATIONAL SERVICE ASSOCIATION [US/US]; P.O. Box 8999, San Francisco, CA 94128 (US).

(72) Inventor: BADENHORST, Cornelius Johannes; 21 Bergkruine Street, Eversdal, 7550 Cape Town (ZA).

(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, 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, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, 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, 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).

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))*

— *of inventorship (Rule 4.17(iv))*

Published:

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

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*

(54) Title: PROVISIONING PAYMENT CREDENTIALS TO A CONSUMER

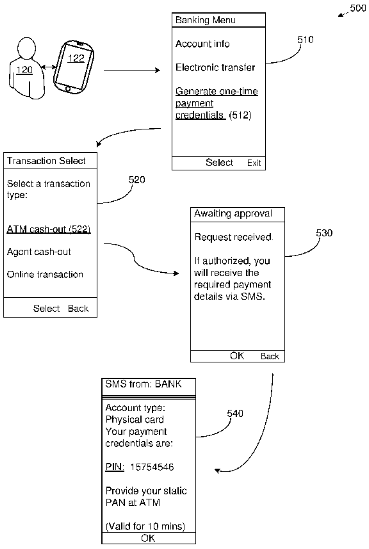


FIG. 5

(57) Abstract: A method and system for provisioning payment credentials to a consumer are disclosed. A remotely accessible server receives a request for payment credentials required to conduct a transaction, the request originating from an electronic device of a consumer. A transaction type associated with the transaction is determined, the transaction type being one of a plurality of predefined transaction types wherein each transaction type is associated with a predefined payment credential format. The remotely accessible server obtains payment credentials in the payment credential format associated with the determined transaction type and transmits the obtained payment credentials to the electronic device of the consumer for use in conducting the transaction.

PROVISIONING PAYMENT CREDENTIALS TO A CONSUMER

CROSS-REFERENCES TO RELATED APPLICATIONS

[0001] This application claims priority to South African provisional patent application number 2013/05673 entitled “Authorization Based on Transaction Type”, filed on 26 July 2013, and to South African provisional patent application number 2013/06923 entitled “Authorization Based on Transaction Type”, filed on 16 September 2013, both of which are incorporated by reference herein.

BACKGROUND

[0002] Various systems and methods are used to provision payment credentials to a consumer for the purpose of conducting one or more financial transactions.

[0003] Such payment credentials typically include payment account details such as a card number in the form of a Primary Account Number (PAN), a card expiry date and/or a Card Verification Value (CVV). Alternatively, or in combination with payment account details, the payment credentials may also include a passphrase, passcode, Personal Identification Code (PIN), or the like. These payment credentials may, for example, be valid for only a single use (often referred to as “one-time payment credentials”) or for a predefined timeframe.

[0004] In one example of such a system, a consumer requests payment credentials using a mobile device. If authorized, payment credentials including a single-use PAN are issued to the consumer. The consumer may then provide the payment credentials to a merchant in order to conduct a transaction.

[0005] Provisioning payment credentials to a consumer in this manner may present security risks. For example, payment credentials may be intercepted by unscrupulous parties and used for conducting fraudulent transactions. Furthermore, systems and methods for provisioning payment credentials to consumers may be inflexible in the sense that they are limited to a single payment credential format, which may not be accepted at all payment acceptance points.

[0006] The present invention aims to alleviate these and other problems, at least to some extent.

BRIEF SUMMARY

[0007] In accordance with the invention there is provided a method of provisioning payment credentials to a consumer, the method conducted at a remotely accessible server and comprising the steps of:

receiving a request for payment credentials required to conduct a transaction, the request originating from an electronic device of a consumer;

determining a transaction type associated with the transaction, the transaction type being one of a plurality of predefined transaction types wherein each transaction type is associated with a predefined payment credential format;

obtaining payment credentials in the payment credential format associated with the determined transaction type; and

transmitting the obtained payment credentials to the electronic device of the consumer for use in conducting the transaction.

[0008] Further features provide for the request for payment credentials to include a consumer transaction selection; for the transaction type to be determined at least partially based on the consumer transaction selection included in the request; and for the step of determining the transaction type associated with the transaction to include checking an account type associated with an account of the consumer and determining the transaction type at least partially based on the account type. The transaction type may be obtained from a consumer record stored in a database containing details of the account of the consumer.

[0009] The account type may be one of an account associated with a corresponding physical payment card and an account not associated with a corresponding physical payment card. Different predefined payment credential formats may be respectively associated with an account associated with a corresponding physical payment card and an account not associated with a corresponding physical payment card.

[0010] Yet further features provide for the account to be a mobile wallet account; for the remotely accessible server to be operated by a mobile banking system; and for the transaction to be a mobile banking transaction.

[0011] The request for payment credentials may be a request for single-use payment credentials. Alternatively, the payment credentials may be valid for conducting a plurality of transactions of the transaction type or for conducting one or more transactions of the transaction type within a predefined timeframe.

[0012] Still further features provide for the step of obtaining payment credentials in the payment credential format associated with the transaction type to include requesting the payment credentials from an external credential generating module; alternatively, for the step of obtaining payment credentials in the payment credential format associated with the transaction type to include generating the payment credentials at the remotely accessible server.

[0013] Further features provide for the request for payment credentials to include a consumer identifier; for the consumer identifier to be an identifier of the electronic device of the consumer; and for the electronic device of the consumer to be a mobile phone. The identifier of the electronic device of the consumer may be a Mobile Subscriber Integrated Services Digital Network Number (MSISDN) of the mobile phone of the consumer.

[0014] The payment credential format associated with the determined transaction type may include one or a combination of: a bank account number, a Primary Account Number (PAN), a pseudo PAN, a card expiry date, a Card Verification Value (CVV), a passcode, a passphrase, a Personal Identification Number (PIN), a token, a barcode, and a Quick Response (QR) code.

[0015] The predefined transaction types may include: an e-commerce transaction, an online payment, an online banking transaction, a physical card present transaction, a mobile banking transaction, a money transfer, an agent cash-out transaction, a cardless withdrawal or purchase transaction, an automated teller machine (ATM) cash withdrawal, a transaction against an account associated with a corresponding physical payment card, or a transaction against an account not associated with a corresponding physical payment card.

[0016] A further feature provides for the predefined transaction types to include an ATM cash withdrawal, and for the payment credential format associated with the ATM cash withdrawal to be a PAN and a PIN.

[0017] According to one aspect, the account type is an account associated with a corresponding physical payment card, the physical payment card having a static PAN, the predefined transaction types include an ATM cash withdrawal, and the payment credential format associated with the ATM cash withdrawal is a PIN only.

[0018] A yet further feature provides for the predefined transaction types to include an e-commerce transaction, and for the payment credential format associated with the e-commerce transaction to be a PAN, a card expiry date, and a CVV.

[0019] According to a further aspect, the account type is an account associated with a corresponding physical payment card, the physical payment card having a static PAN, the predefined transaction types include an e-commerce transaction, and the payment credential format associated with the e-commerce transaction is a card expiry date and a CVV.

[0020] A still further feature provides for the predefined transaction types to include an agent cash-out transaction, and for the payment credential format associated with the agent cash-out transaction to be a PAN.

[0021] Further features provide for the step of receiving the request for payment credentials to be preceded by the step of establishing a communication channel with the electronic device of the consumer; for communications between the remotely accessible server and the electronic device of the consumer to be by way of one of Short Message Service (SMS) protocol, Unstructured Supplementary Service Data

(USSD) protocol, a secure Internet connection, and data communication enabled by a mobile software application installed on the electronic device of the consumer.

[0022] The invention extends to a system for provisioning payment credentials to a consumer, the system comprising a remotely accessible server in communication with an electronic device of a consumer, the remotely accessible server including:

a request receiving component for receiving a request for payment credentials required to conduct a transaction, the request originating from the electronic device of the consumer;

a type determining component for determining a transaction type associated with the transaction, the transaction type being one of a plurality of predefined transaction types wherein each transaction type is associated with a predefined payment credential format;

a credential obtaining component for obtaining payment credentials in the payment credential format associated with the determined transaction type; and

a transmitting component for transmitting the obtained payment credentials to the electronic device of the consumer for use in conducting the transaction.

[0023] Further features provide for the credential obtaining component to be configured to request the payment credentials required to conduct the transaction from an external credential generating module; for the external credential generating module to be operated by an issuer of the consumer or by a payment processor; and for the issuer to be an issuing bank of the consumer; alternatively, for the credential obtaining component to be configured to generate the payment credentials.

[0024] The invention may further extend to a computer program product for provisioning payment credentials to a consumer, the computer program product comprising a computer-readable medium having stored computer-readable program code for performing the steps of:

receiving a request for payment credentials required to conduct a transaction, the request originating from an electronic device of a consumer;

determining a transaction type associated with the transaction, the transaction type being one of a plurality of predefined transaction types wherein each transaction type is associated with a predefined payment credential format;

obtaining payment credentials in the payment credential format associated with the determined transaction type; and

transmitting the obtained payment credentials to the electronic device of the consumer for use in conducting the transaction.

[0025] The computer-readable medium may be a non-transitory computer-readable medium, and the computer-readable program code may be executable by a processing circuit.

[0026] In order for the invention to be more fully understood, implementations thereof will now be described with reference to the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

[0027] FIG. 1A is a schematic diagram illustrating an embodiment of a system for provisioning payment credentials to a consumer according to the invention;

[0028] FIG. 1B is a block diagram illustrating a first embodiment of a remotely accessible server according to the invention;

[0029] FIG. 1C is a block diagram illustrating a second embodiment of a remotely accessible server according to the invention;

[0030] FIG. 2 is a swim-lane flow diagram illustrating a method of provisioning payment credentials to a consumer using the system of FIG. 1A;

[0031] FIG. 3 is a swim-lane flow diagram illustrating a method of provisioning payment credentials to a consumer using the system of FIG. 1A;

[0032] FIG. 4 is a flow diagram of an exemplary implementation of a method of provisioning payment credentials to a consumer according to the invention;

[0033] FIG. 5 is a flow diagram of an exemplary implementation of a method of provisioning payment credentials to a consumer according to the invention;

[0034] FIG. 6 illustrates a block diagram of a computing device that can be used in various embodiments of the invention; and

[0035] FIG. 7 illustrates a block diagram of a communication device that can be used in various embodiments of the invention.

DETAILED DESCRIPTION WITH REFERENCE TO THE DRAWINGS

[0036] A system and method for provisioning payment credentials to a consumer is provided. A remotely accessible server receives a request for payment credentials required to conduct a transaction, the request originating from an electronic device of a consumer. A transaction type associated with the transaction is determined, the transaction type being one of a plurality of predefined transaction types wherein each transaction type is associated with a predefined payment credential format. The remotely accessible server obtains payment credentials in the payment credential format associated with the determined transaction type. These payment credentials are then transmitted to the electronic device of the consumer for use in completing the transaction.

[0037] FIG. 1A illustrates an embodiment of a system (100) for provisioning payment credentials to a consumer. The system (100) comprises a remotely accessible server (110), a plurality of consumers (120) each having an electronic device (122), and an issuer (130).

[0038] The remotely accessible server (110) has access to a database (112) containing a plurality of consumer records (114). In one embodiment, the remotely accessible server (110) is one or more mobile money servers of a mobile banking system, typically operated by an entity known as a mobile money operator. In such a case, each consumer (120) may have a registered mobile wallet account held at the remotely accessible server (110) and the consumer record (114) contains details thereof, such as a consumer account number, a consumer account type, personal information of the consumer, funds available, details of payment instruments, payment credential formats, or the like. In further embodiments, the remotely accessible server (110) is a server of a traditional financial institution such as a bank or other financial services provider.

[0039] The electronic device (122) may be any electronic communications device capable of communicating over a communications network, such as a cellular communications network. The term should be interpreted to specifically include all mobile or cellular phones, including so-called “feature phones” and smartphones, and may also include other electronic devices such as computers, laptops, handheld personal computers, personal digital assistants, tablet computers, and the like.

[0040] In the embodiment of FIG. 1A, the electronic device (122) is a mobile phone of the consumer (120). In the case where the electronic device (122) is a mobile phone and the remotely accessible server (110) is associated with a mobile money operator, a mobile money or mobile banking platform may typically be used to allow the consumer (120) to conduct financial transactions via the electronic device (122).

[0041] Examples of well-known mobile money transactions are cash-in transactions, cash-out transactions, person-to-person payments, top-up of airtime services, and bill payments. Cash-out transactions may include cash-outs at mobile money agents and/or automated teller machine (ATM) cash withdrawals.

[0042] The remotely accessible server (110) is configured to transmit communications to and receive communications from the electronic devices (122) over a communications network, which is a mobile communications network (140) in this embodiment. The remotely accessible server (110) is further configured to receive communications from and transmit communications to the issuer (130) over a communications network, which may be, among many others, a mobile communications network or, as in the embodiment of FIG. 1A, the Internet (150).

[0043] Embodiments provide for communications between the remotely accessible server (110) and the electronic device (122) and/or between the remotely accessible server (110) and the issuer (130) to be secure communications across an encrypted communication channel such as Hypertext Transfer Protocol Secure (HTTPS), Transport Layer Security / Secure Sockets Layer (TLS/SSL) or other secure channel or channels.

[0044] The issuer (130) may be any entity authorized to issue payment credentials to the consumer (120). In this embodiment, the issuer (130) is an issuing bank of the consumer (120). In another embodiment, the issuer (130) may be a secure financial gateway or a payment processing network. In some embodiments, the issuer is an issuer processor, in other words, a payment processing entity that can connect financial service providers such as mobile money operators to a payment processing network such as VisaNet^{TM}.

[0045] The remotely accessible server (110) may include a request receiving component (115) for receiving a request for payment credentials required to conduct a transaction, a type determining component (116) for determining a transaction type associated with the transaction, a credential obtaining component (117) for obtaining payment credentials in the payment credential format associated with the determined transaction type, and a transmitting component (118) for transmitting the obtained payment credentials to the electronic device (122) of the consumer (120) for use in conducting the transaction.

[0046] In one embodiment, the credential obtaining component (117) may include a generating component (117A) and a storing component (117B). In such a case, the credential obtaining component (117) is configured to generate the payment credentials and the remotely accessible server (110) may therefore generate the payment credentials itself. This embodiment is illustrated in FIG. 1B.

[0047] In another embodiment, the credential obtaining component (117) is configured to request the payment credentials required to conduct the transaction from an external credential generating module (132), which may typically be operated by the issuer (130). In such a case, the credential obtaining component (117) may include an external request component (117C) and a credential receiving component (117D) in order to be capable of requesting payment credentials from the external credential generating module (132) and receiving the requested payment credentials, respectively. This embodiment is illustrated in FIG. 1C, which is similar to FIG. 1B. Like reference numerals in FIGs. 1A, 1B and 1C refer to like components and entities.

[0048] In some embodiments, the external credential generating module may be operated by a payment processing network such as VisaNet^{TM}. The payment processing network may include data processing subsystems, networks, and operations used to support and deliver authorization services, exception file services, and clearing and settlement services. Payment processing networks, for example, VisaNet™, are able to process credit card transactions, debit card transactions, and other types of commercial transactions. Furthermore, the payment processing network may include one or more servers and may use any suitable wired or wireless network, including the Internet.

[0049] The system (100) enables the consumer (120) to use the electronic device (122) to request payment credentials for use in conducting a transaction. The system (100) may also be configured to carry out at least a portion of the transaction or to complete the transaction. The remotely accessible server (110) associates different payment credential formats with different types of transactions and provisions credentials to consumers accordingly, as will be described in greater detail below.

[0050] The flow diagram (200) of FIG. 2 illustrates an example of a method of provisioning payment credentials to a consumer using the system of FIG. 1. The consumer (120) has a mobile wallet account and is capable of using the electronic device (122) to conduct mobile banking transactions. In this example, the consumer requests single-use ("one-time") payment credentials for use in conducting a single transaction of a particular transaction type.

[0051] At a first stage (202), the consumer (120) uses the electronic device (122) to establish a communication channel with the remotely accessible server (110). Communications between the remotely accessible server (110) and the electronic device (122) of the consumer (120) may typically be effected by way of Short Message Service (SMS) protocol, Unstructured Supplementary Service Data

(USSD) protocol, over a secure Internet connection, or by way of data communication enabled by a mobile software application installed on the electronic device of the consumer. In this example, a USSD session is initiated.

[0052] At a next stage (204), the remotely accessible server (110) presents the electronic device (122) with the option to request payment credentials. Typically, this is presented as a menu option on a display of the electronic device (122). For example, the consumer (120) may be presented with a menu option “Generate one-time payment credentials” in a USSD menu.

[0053] The consumer (120), at a next stage (206), requests payment credentials to be generated. In this embodiment, the consumer (120) also specifies a transaction type for which the credentials are required. The consumer (120) may, for example, have the option of selecting one of the following transaction types: an ATM cash withdrawal, an e-commerce transaction, or an agent cash-out transaction to be performed at a mobile money agent. The term “ATM cash withdrawal” used herein may refer to cash withdrawals or cash-outs performed with or without a payment card at an ATM. In other words, the consumer may be able to effect an ATM cash withdrawal without a physical card. Such a withdrawal is known as a cardless ATM cash withdrawal.

[0054] The request for payment credentials is typically accompanied by a consumer identifier. In a preferred embodiment, for example in a USSD-based system, this identifier is a Mobile Subscriber Integrated Services Digital Network Number (MSISDN) of a mobile phone used by the consumer (120) to request the payment credentials. Alternatively, the consumer identifier may be obtained by requiring the consumer to log into a secure software application or website by, for example, inputting a username and password.

[0055] The remotely accessible server (110) receives the request for payment credentials which originates from the electronic device (122) and then, at a next stage (208), checks the transaction type received from the electronic device (122) of the consumer (120), and looks up a payment credential format associated with the transaction type received in the database (112). In this embodiment, therefore, a consumer transaction selection is used to determine the transaction type. The payment credential format is selected from a plurality of predefined payment credential formats, each transaction type selectable by the consumer being associated with a predefined payment credential format.

[0056] It is envisaged that one or more validation steps may take place before the payment credentials are generated and/or transmitted to the consumer (120). For example, the consumer (120) may be required to enter a PIN or undergo a two and/or three factor authentication process.

[0057] The remotely accessible server (110) is configured to look up a payment credential format corresponding to the transaction type. Payment credentials are then obtained in accordance with the specified format and transmitted to the electronic device (122) of the consumer (120). Numerous payment credential formats may be used, depending on which transactions or payment credential requests the remotely accessible server (110) supports.

[0058] For example, and among many others, the transactions supported may include an e-commerce transaction, an online payment, an online banking transaction, a physical card present transaction, a mobile banking transaction, a money transfer, an agent cash-out transaction, a cardless withdrawal or purchase transaction, an ATM cash withdrawal, a transaction against an account associated with a corresponding physical payment card, and a transaction against an account not associated with a corresponding physical payment card. Each supported transaction type is associated with a specific, predefined payment credential format, which may be the same for two or more transaction types.

[0059] The payment credentials can be generated and transmitted to the consumer (120) in, for example and not limited to, any one or any combination of the following formats: a bank account number, a Primary Account Number (PAN), a pseudo PAN, a card expiry date, a Card Verification Value (CVV), a passcode, a passphrase, a Personal Identification Number (PIN), a token, a barcode, a payment reference number, and a Quick Response (QR) code. The term “pseudo PAN” should be interpreted broadly and includes a token associated with an actual PAN, credentials formatted as a PAN, and obfuscated PANs. Any suitable token which is uniquely associated with payment credentials of the consumer which can be used to complete a transaction against the account of the consumer may be generated and transmitted to the electronic device (122) of the consumer.

[0060] For example, for a transaction of type “A”, the payment credential format associated with the transaction may be a PAN and a PIN. For a transaction of type “B”, the payment credential format associated with the transaction may be a QR code. For a transaction of type “C”, the payment credential format associated with the transaction may be a pseudo PAN. Consumers may thus receive different payment credentials based on the transaction type of the proposed transaction.

[0061] In the embodiment illustrated in FIG. 2, if the transaction type is an e-commerce transaction, the remotely accessible server (110), at a next stage (210), requests the issuer (130) to generate a PAN, a card expiry date, and a CVV as payment credentials for a single use. If the transaction type received from the electronic device (122) of the consumer (120) is an ATM cash withdrawal, the remotely accessible server (110), at a next stage (212), requests the issuer (130) to generate a PAN and a PIN as payment credentials for a single use. Alternatively, if the transaction type received from the electronic device (122) of the consumer (120) is an agent cash-out transaction, the remotely accessible server (110), at a next stage (214), requests the issuer (130) to generate only a PAN as a payment credential for a single use.

[0062] In this embodiment, the payment credentials are generated by the issuer (130) and obtained from issuer (130) by the remotely accessible server (110). In such a case, when the consumer (120), after having received the credentials, subsequently presents these payment credentials to conduct a transaction, the issuer (130) may typically verify that the payment credentials presented match the payment credentials originally generated before ultimately authorizing the transaction. Alternatively, the payment credentials may be generated by the remotely accessible server (110) without routing the request to the issuer (130). In such a case, either or both of an acquirer or the issuer (130) will request the remotely accessible server (110) to validate any payment credentials received before authorizing a transaction, in order to check whether received payment credentials are validly generated payment credentials for the specific transaction or transaction type.

[0063] At a next stage (216), the issuer (130) generates the payment credentials in the required format and transmits the credentials to the remotely accessible server (110). These payment credentials are then forwarded, at a next stage (218), from the remotely accessible server (110) to the electronic device (122) of the consumer (120). The consumer (120), at a final stage (220), receives the payment credentials and may then use them to conduct either one or more transactions only of the specific type, or one or more transactions of various transaction types as long as the payment credentials are accepted payment credentials for each specific transaction type.

[0064] After the payment credentials are forwarded to the electronic device (122) of the consumer (120), it can be used for conducting at least one financial transaction of the particular transaction type. The payment credentials may be single-use ("one-time") payment credentials for conducting one transaction of the particular transaction type. For example, the consumer (120) may request one-time payment credentials for conducting an e-commerce transaction. The remotely accessible server (110) then associates this transaction type with a specific payment credential format, for example, a PAN, a card expiry date, and a CVV in combination. These credentials may then be used once to conduct an e-commerce transaction.

[0065] In some embodiments, payment credentials may only be used to conduct the specific transaction type. However, it should be appreciated that, in alternative embodiments, payment credentials may equally be used to conduct any transaction for which the particular payment credentials are accepted. For example, in the case of a request for payment credentials for an e-commerce transaction, the consumer (120) may use the PAN received with the card expiry date and CVV to perform an agent cash-out transaction at a mobile money agent in a mobile banking environment, in the case where only a PAN is required to conduct such a transaction.

[0066] Furthermore, the payment credentials may be valid for conducting a plurality of transactions of the transaction type, or alternatively, the payment credentials may have a limited period of validity and may be valid for conducting one or more transactions of the transaction type within a predefined timeframe.

[0067] The type of transaction for which the payment credentials are requested may be determined by the remotely accessible server (110), for example, from user account information stored in the database (112) or from a consumer selection in the request itself as is the case in the example of FIG. 2. Alternatively, it may be determined from further information in the request for payment credentials.

[0068] The remotely accessible server (110) may distinguish between transactions against an account associated with a corresponding physical payment card, and transactions against an account not associated with a corresponding physical payment card. In such cases, determining the transaction type associated with a transaction may include checking an account type associated with an account of the consumer and determining the transaction type at least partially based on the account type.

[0069] For example, the consumer may have only a virtual account which is not associated with a physical payment card. When the consumer requests payment credentials, the transaction type may be obtained from a consumer record stored in the database containing details of the account of the consumer, which indicates that the consumer does not have a physical payment card. This feature will be described in greater detail below.

[0070] In a mobile banking system or similar payment network, some consumers may have a physical payment card or “companion plastic card” having payment credentials (e.g. PAN, expiry date and/or CVV) physically provided thereon and/or stored on a chip and/or magnetic stripe of the card, while other consumers may only have payment credentials which are electronically stored or which are dynamic and must be electronically requested. In such cases, consumers may necessarily require different payment credentials for performing transactions.

[0071] For example, in a mobile banking system which makes use of PANs for processing so-called “open-loop” mobile payment transactions between various separate mobile money deployments, if a consumer has an account associated with a physical payment card and requests to perform an agent cash-out transaction, a withdrawal, or a payment transaction, the consumer would already be in possession of a PAN to use for the transaction, as the PAN is typically provided on the payment card. This implementation is referred to as an account with a “static” PAN or permanent PAN.

[0072] Contrastingly, if a consumer who does not have a corresponding physical payment card requests to perform such a transaction, the consumer may not have a static PAN and the issuer would need to provide the consumer with a PAN in order for the consumer to complete the desired transaction.

[0073] The swim-lane flow diagram (300) of FIG. 3 illustrates a further example of a method of provisioning payment credentials to a consumer, using the system of FIG. 1A. In this example, the remotely accessible server (110) is configured to distinguish between accounts associated with physical payment cards and accounts not associated with physical payment cards.

[0074] At a first stage (302), the consumer (120) uses the electronic device (122) to establish a communication channel with the remotely accessible server (110). At a next stage (304), the remotely accessible server (110) presents the electronic device (122) with the option to request payment credentials.

[0075] The consumer (120), at a next stage (306), requests payment credentials to be generated. In this embodiment, the consumer (120) selects to receive payment credentials for performing a cash-out transaction. The consumer (120) may have the option of selecting an ATM cash-out or an agent cash-out transaction to be performed at a mobile money agent. The remotely accessible server (110) then uses the selection and additionally determines whether or not the consumer (120) has a corresponding physical payment card, in other words, a static PAN.

[0076] The remotely accessible server (110) then, at a next stage (308), checks the transaction type received and/or derived as described above, and looks up a payment credential format associated with the transaction type in the database (112). If the transaction type is a transaction against an account associated with a corresponding physical payment card, the remotely accessible server (110), at a next stage (310), requests the issuer (130) to generate only a one-time PIN. If the transaction type is a transaction against an account not associated with a corresponding physical payment card, the remotely accessible server (110), at a next stage (312), requests the issuer (130) to generate a one-time PIN and a one-time PAN.

[0077] The remotely accessible server (110) typically checks the consumer record (114) in the database (112) to determine whether or not the consumer (120) requires a one-time PAN to complete the transaction.

[0078] At a next stage (314), the issuer (130) generates the payment credentials in the required format and transmits the payment credentials to the remotely accessible server (110). These payment credentials are then forwarded, at a next stage (316), from the remotely accessible server (110) to the electronic device (122) of the consumer (120). The consumer (120), at a final stage (318), receives the payment credentials and may then use them to conduct either one or more transactions only of the specific type, or one or more transactions of various transaction types as long as the payment credentials are accepted payment credentials for each specific transaction type.

[0079] It should be appreciated that in some embodiments a consumer transaction selection may be provided to the remotely accessible server, and the transaction type may be determined at least partially based on the consumer transaction selection included in the request. A consumer transaction selection need not be explicitly provided by the consumer. A merchant may provide such a selection, or the transaction selection may be derived from any other suitable information in the request for payment credentials.

[0080] Furthermore, in some embodiments determining the transaction type may include checking an account type associated with an account of the consumer and determining the transaction type at least partially based on the account type. In some embodiments, determining the transaction type may involve using both a transaction selection as set out above and an account type to determine the transaction type and therefore also the relevant payment credential format.

[0081] Two exemplary mobile phone implementations will now be described with reference to FIGs. 4 and 5. In the example shown in the diagram (400) of FIG. 4, the consumer (120) requests payment credentials to be provisioned to the electronic device (122) for conducting an e-commerce transaction.

[0082] At a first stage (410), the consumer (120) accesses a banking menu provided as a USSD-based service using the electronic device (122), which is a mobile phone in the example. The consumer (120) is presented with various banking options, and at a next stage (412) opts for the generation of one-time payment credentials.

[0083] At a next stage (420), the consumer (120) is required to select a transaction type for which the payment credentials must be generated. In this case and primarily for exemplary purposes, the consumer (120) desires payment credentials for conducting an e-commerce transaction, and selects the appropriate menu option at a next stage (422).

[0084] The consumer (120) is presented, at a further stage (430), with a notification that the request has been received and that authorization thereof is in process. One or more validation steps as described above may, of course, be included between the prior stages (420, 430).

[0085] The consumer (120) in this embodiment receives the appropriate payment credentials via one or more SMS messages. As shown in FIG. 4, at a final stage (440), the consumer (120) is provided with a single-use PAN, card expiry date and CVV for use in conducting an e-commerce transaction. In order to provide a higher level of security and in addition to the restriction on the number of times the payment credentials may be used, the payment credentials may have a limited “lifetime”. For example, and as shown in FIG. 4, the payment credentials may only be valid for 10 minutes from the time that they are transmitted to the electronic device (122) of the consumer (120).

[0086] The SMS (440) shown in FIG. 4 also indicates an account type. In this case, the consumer (120) does not have a physical payment card, and does not have a PAN, card expiry date and CVV to use for the transaction, and is thus provided with these payment credentials via SMS.

[0087] In the example shown in FIG. 4, the payment credential format associated with an e-commerce transaction is a Primary Account Number (PAN), a card expiry date, and a Card Verification Value (CVV) when the consumer does not have a physical payment card. In this case, the consumer (120) does not have a static PAN to provide a merchant with, and therefore receives a one-time PAN.

[0088] In some embodiments, the account type may be an account associated with a corresponding physical payment card which has a static PAN. In such a case, the consumer (120) may not need to receive a PAN. The payment credential format associated with an e-commerce transaction for accounts having a physical payment card may be a card expiry date and a CVV. In such a case, the consumer (120) may, for example, when requesting payment credentials for an e-commerce transaction, only receive a card expiry date and a CVV for use with the static PAN. The consumer may of course be capable of using an expiry date and CVV of the physical payment card, but it is envisaged that transaction security may be enhanced by providing such credentials to the consumer via the remotely accessible server (110), for use with the static PAN.

[0089] In some embodiments, the payment credential format associated with an ATM cash withdrawal may be a PAN and a PIN when the account type is an account not associated with a physical payment card and therefore also not with a static PAN. Furthermore, the payment credential format associated with an ATM cash withdrawal may be only a PIN when the account type is an account associated with a corresponding physical payment payment card which has a static PAN. An example of such an implementation is shown in the flow diagram (500) of FIG. 5.

[0090] In this case, the consumer (120) requests payment credentials for conducting a cash-out or cash withdrawal transaction at an ATM, and the consumer (120) does not have an account which includes a physical payment card, also known as a "companion plastic card".

[0091] At a first stage (510), the consumer (120) accesses a banking menu provided as a USSD-based service using the electronic device (122), which is a mobile phone in this embodiment. The consumer (120) is presented with various banking options, and at a next stage (512) opts for the generation of one-time payment credentials.

[0092] At a next stage (520), the consumer (120) is required to select a transaction type for which the payment credentials must be generated. In this case and as an example, the consumer (122) desires payment credentials for conducting an ATM cash-out transaction, and selects the appropriate menu option at a next stage (522).

[0093] The consumer (120) is presented, at a further stage (530), with a notification that the request has been received and that authorization thereof is in process. The remotely accessible server (110) in this case determines, using details of the consumer account (114) that the consumer (120) has a physical payment card, and therefore does not require a PAN for completing the transaction. The remotely accessible server (110) then uses this information and the transaction type received from the electronic device (122) to determine the specific payment credential format required, which is only a PIN in this example.

[0094] The consumer (120) receives the appropriate payment credentials via one or more SMS messages. As shown in FIG. 5, at a next stage (540), the consumer (120) is provided with a single-use PIN which can be entered at a keypad of an ATM to complete the cash-out transaction, together with the static PAN the consumer (120) already possesses. In order to provide a higher level of security, the credentials are only valid for 10 minutes from the moment they are transmitted to the electronic device (122) of the consumer (120).

[0095] In some embodiments, the payment credential format associated with a cash-out transaction at a mobile money agent is a PAN only. In such a case, the consumer (120) may only need to request payment credentials if the consumer (120) does not have a physical payment card. If the consumer (120) has a physical payment card, the static PAN on the physical payment card may be used to perform the cash-out at the agent. Typically, the consumer (120) may be required to present some form of an identity document to validate its identity at the agent before the cash-out is completed. Such validation may also be carried out when completing a number of other transaction types.

[0096] A system and method for provisioning payment credentials to a consumer is therefore provided in which payment credentials, which may be one-time credentials or credentials valid for a plurality of transactions, are generated in a format directly dependent on the type of transaction which the consumer wishes to perform.

[0097] The method described may reduce security risks. For example, if payment credentials are intercepted by an unscrupulous party, the credentials can only be used for a specific type of transaction. This limits the scope of power the intercepting party has to perform fraudulent transactions, and may make subsequent transactions by such a party easier to anticipate and/or trace.

[0098] Furthermore, the system and method provided may bring about increased flexibility in terms of issuing payment credentials to consumers, particularly in the case of one-time payment credentials. This may allow issuers of payment credentials to tailor payment credentials to a desired transaction type according to the available payment acceptance points and financial infrastructure. For example, a PAN may only be provided to a consumer in a case where the consumer does not already have a static PAN, and a CVV and expiry date may only be provided when they are actually required for the transaction type which is to be conducted.

[0099] In other situations where only a PIN or unique code may typically be required, such as at an ATM or point of payment in a retail environment, the payment credentials may be tailored to fit the exact requirements of the financial infrastructure.

[0100] The technology described may serve to limit information sent to the consumer based on the consumer's specific requirements for the transaction.

[0101] It should be understood that the technology described herein may at least partially be implemented as a computer program product for provisioning payment credentials to a consumer. The computer program product may comprise a computer-readable medium having stored computer-readable program code for performing one or more of the steps of: receiving a request for payment credentials required to conduct a transaction, the request originating from an electronic device of a consumer, determining a transaction type associated with the transaction, the transaction type being one of a plurality of predefined transaction types wherein each transaction type is associated with a predefined payment credential format, obtaining payment credentials in the payment credential format associated with the determined transaction type, and transmitting the obtained payment credentials to the electronic device of the consumer for use in conducting the transaction

[0102] The computer-readable medium may be a non-transitory computer-readable medium, and the computer-readable program code may be executable by a processing circuit.

[0103] FIG. 6 illustrates an example of a computing device (600) in which various aspects of the disclosure may be implemented. The computing device (600) may be suitable for storing and executing computer program code. The various participants and elements in the previously described system diagrams may use any suitable number of subsystems or components of the computing device (600) to facilitate the functions described herein.

[0104] The computing device (600) may include subsystems or components interconnected via a communication infrastructure (605) (for example, a communications bus, a cross-over bar device, or a network). The computing device (600) may include at least one central processor (610) and at least one memory component in the form of computer-readable media.

[0105] The memory components may include system memory (615), which may include read only memory (ROM) and random access memory (RAM). A basic input/output system (BIOS) may be stored in ROM. System software may be stored in the system memory (615) including operating system software.

[0106] The memory components may also include secondary memory (620). The secondary memory (620) may include a fixed disk (621), such as a hard disk drive, and, optionally, one or more removable-storage interfaces (622) for removable-storage components (623).

[0107] The removable-storage interfaces (622) may be in the form of removable-storage drives (for example, magnetic tape drives, optical disk drives, floppy disk drives, etc.) for corresponding removable storage-components (for example, a magnetic tape, an optical disk, a floppy disk, etc.), which may be written to and read by the removable-storage drive.

[0108] The removable-storage interfaces (622) may also be in the form of ports or sockets for interfacing with other forms of removable-storage components (623) such as a flash memory drive, external hard drive, or removable memory chip, etc.

[0109] The computing device (600) may include an external communications interface (630) for operation of the computing device (600) in a networked environment enabling transfer of data between multiple computing devices (600). Data transferred via the external communications interface (630) may be in the form of signals, which may be electronic, electromagnetic, optical, radio, or other types of signal.

[0110] The external communications interface (630) may enable communication of data between the computing device (600) and other computing devices including servers and external storage facilities. Web services may be accessible by the computing device (600) via the communications interface (630).

[0111] The external communications interface (630) may also enable other forms of communication to and from the computing device (600) including, voice communication, near field communication, Bluetooth, etc.

[0112] The computer-readable media in the form of the various memory components may provide storage of computer-executable instructions, data structures, program modules, and other data. A computer program product may be provided by a computer-readable medium having stored computer-readable program code executable by the central processor (610).

[0113] A computer program product may be provided by a non-transient computer-readable medium, or may be provided via a signal or other transient means via the communications interface (630).

[0114] Interconnection via the communication infrastructure (605) allows a central processor (610) to communicate with each subsystem or component and to control the execution of instructions from the memory components, as well as the exchange of information between subsystems or components.

[0115] Peripherals (such as printers, scanners, cameras, or the like) and input/output (I/O) devices (such as a mouse, touchpad, keyboard, microphone, joystick, or the like) may couple to the computing device (600) either directly or via an I/O controller (635). These components may be connected to the computing device (600) by any number of means known in the art, such as a serial port.

[0116] One or more monitors (645) may be coupled via a display or video adapter (640) to the computing device (600).

[0117] FIG. 7 shows a block diagram of a communication device (700) that may be used in embodiments of the disclosure. The communication device (700) may be a cell phone, a feature phone, a smart phone, a satellite phone, or a computing device having a phone capability.

[0118] The communication device (700) may include a processor (705) (e.g., a microprocessor) for processing the functions of the communication device (700) and a display (720) to allow a user to see the phone numbers, messages and/or other information. The communication device (700) may further include an input element (725) to allow a user to input information into the device (e.g., input buttons, touch screen, etc.), a speaker (730) to allow the user to hear voice communication, music, etc., and a microphone (735) to allow the user to transmit his or her voice through the communication device (700).

[0119] The processor (705) of the communication device (700) may connect to a memory (715). The memory (715) may be in the form of a computer-readable medium that stores data and, optionally, computer-executable instructions.

[0120] The communication device (700) may also include a communication element (740) for connection to communication channels (e.g., a cellular telephone network, data transmission network, Wi-Fi network, satellite-phone network, Internet network, Satellite Internet Network, etc.). The communication element (740) may include an associated wireless transfer element, such as an antenna.

[0121] The communication element (740) may include a subscriber identity module (SIM) in the form of an integrated circuit that stores an international mobile subscriber identity and the related key used to identify and authenticate a subscriber using the communication device (700). One or more subscriber identity modules may be removable from the communication device (700) or embedded in the communication device (700).

[0122] The communication device (700) may further include a contactless element (750), which is typically implemented in the form of a semiconductor chip (or other data storage element) with an associated wireless transfer element, such as an antenna. The contactless element (750) may be associated with (e.g., embedded within) the communication device (700) and data or control instructions transmitted via a cellular network may be applied to the contactless element (750) by means of a contactless element interface (not shown). The contactless element interface may function to permit the exchange of data and/or control instructions between mobile device circuitry (and hence the cellular network) and the contactless element (750).

[0123] The contactless element (750) may be capable of transferring and receiving data using a near field communications (NFC) capability (or near field communications medium) typically in accordance with a standardized protocol or data transfer mechanism (e.g., ISO 14443/NFC). Near field communications capability is a short-range communications capability, such as radio-frequency identification (RFID), Bluetooth, infra-red, or other data transfer capability that can be used to exchange data between the communication device (700) and an interrogation device. Thus, the communication device (700) may be capable of communicating and transferring data and/or control instructions via both a cellular network and near field communications capability.

[0124] The data stored in the memory (715) may include: operation data relating to the operation of the communication device (700), personal data (e.g., name, date of birth, identification number, etc.), financial data (e.g., bank account information, a bank identification number (BIN), credit or debit card number information, account balance information, expiration date, loyalty provider account numbers, etc.), transit information (e.g., as in a subway or train pass), access information (e.g., as in access badges), etc. A user may transmit this data from the communication device (700) to selected receivers.

[0125] The communication device (700) may be, amongst other things, a notification device that can receive alert messages and access reports, a portable merchant device that can be used to transmit control data identifying a discount to be applied, as well as a portable consumer device that can be used to make payments.

[0126] The foregoing description of the embodiments of the invention has been presented for the purpose of illustration; it is not intended to be exhaustive or to limit the invention to the precise forms disclosed. Persons skilled in the relevant art can appreciate that many modifications and variations are possible in light of the above disclosure.

[0127] Some portions of this description describe the embodiments of the invention in terms of algorithms and symbolic representations of operations on information. These algorithmic descriptions and representations are commonly used by those skilled in the data processing arts to convey the substance of their work effectively to others skilled in the art. These operations, while described functionally, computationally, or logically, are understood to be implemented by computer programs or equivalent electrical circuits, microcode, or the like. The described operations may be embodied in software, firmware, hardware, or any combinations thereof.

[0128] The software components or functions described in this application may be implemented as software code to be executed by one or more processors using any suitable computer language such as, for example, Java, C++, or Perl using, for example, conventional or object-oriented techniques. The software code may be stored as a series of instructions, or commands on a non-transitory computer-readable medium, such as a random access memory (RAM), a read-only memory (ROM), a magnetic medium such as a hard-drive or a floppy disk, or an optical medium such as a CD-ROM. Any such computer-readable medium may also reside on or within a single computational apparatus, and may be present on or within different computational apparatuses within a system or network.

[0129] Any of the steps, operations, or processes described herein may be performed or implemented with one or more hardware or software modules, alone or in combination with other devices. In one embodiment, a software module is implemented with a computer program product comprising a non-transient computer-readable medium containing computer program code, which can be executed by a computer processor for performing any or all of the steps, operations, or processes described.

[0130] Finally, the language used in the specification has been principally selected for readability and instructional purposes, and it may not have been selected to delineate or circumscribe the inventive subject matter. It is therefore intended that the scope of the invention be limited not by this detailed description, but rather by any claims that issue on an application based hereon. Accordingly, the disclosure of the embodiments of the invention is intended to be illustrative, but not limiting, of the scope of the invention, which is set forth in the following claims.

WHAT IS CLAIMED IS:

1. A method of provisioning payment credentials to a consumer, the method conducted at a remotely accessible server and comprising the steps of:

receiving a request for payment credentials required to conduct a transaction, the request originating from an electronic device of a consumer;

determining a transaction type associated with the transaction, the transaction type being one of a plurality of predefined transaction types wherein each transaction type is associated with a predefined payment credential format;

obtaining payment credentials in the payment credential format associated with the determined transaction type; and

transmitting the obtained payment credentials to the electronic device of the consumer for use in conducting the transaction.

2. The method as claimed in claim 1, wherein the request for payment credentials includes a consumer transaction selection, and wherein the transaction type is determined at least partially based on the consumer transaction selection included in the request.

3. The method as claimed in claim 1, wherein the step of determining the transaction type associated with the transaction includes checking an account type associated with an account of the consumer and determining the transaction type at least partially based on the account type.

4. The method as claimed in claim 3, wherein the account type is one of an account associated with a corresponding physical payment card and an account not associated with a corresponding physical payment card, and wherein different predefined payment credential formats are respectively associated with an account associated with a corresponding physical payment card and an account not associated with a corresponding physical payment card.

5. The method as claimed in claim 3, wherein the account is a mobile wallet account.

6. The method as claimed in claim 1, wherein the remotely accessible server is operated by a mobile banking system and wherein the transaction is a mobile banking transaction.

7. The method as claimed in claim 1, wherein the request for payment credentials is a request for single-use payment credentials.

8. The method as claimed in claim 1, wherein the step of obtaining payment credentials in the payment credential format associated with the transaction type includes requesting the payment credentials from an external credential generating module.

9. The method as claimed in claim 1, wherein the step of obtaining payment credentials in the payment credential format associated with the transaction type includes generating the payment credentials at the remotely accessible server.

10. The method as claimed in claim 1, wherein the request for payment credentials includes a consumer identifier.

11. The method as claimed in claim 10, wherein the consumer identifier is an identifier of the electronic device of the consumer.

12. The method as claimed in claim 1, wherein the electronic device of the consumer is a mobile phone.

13. The method as claimed in claim 1, wherein the payment credential format associated with the determined transaction type includes one or a combination of: a bank account number, a Primary Account Number (PAN), a pseudo PAN, a card expiry date, a Card Verification Value (CVV), a passcode, a passphrase, a Personal Identification Number (PIN), a token, a barcode, and a Quick Response (QR) code.

14. The method as claimed in claim 1, wherein the predefined transaction types include one or more of: an Automated Teller Machine (ATM) cash withdrawal, an agent cash-out transaction, and an e-commerce transaction.

15. The method as claimed in claim 1, wherein the predefined transaction types include an Automated Teller Machine (ATM) cash withdrawal and the payment credential format associated with the ATM cash withdrawal is a Primary Account Number (PAN) and a Personal Identification Number (PIN).

16. The method as claimed in claim 4, wherein the account type is an account associated with a corresponding physical payment card, the physical payment card having a static Primary Account Number (PAN), wherein the predefined transaction types include an Automated Teller Machine (ATM) cash withdrawal, and wherein the payment credential format associated with the ATM cash withdrawal is a Personal Identification Number (PIN) only.

17. The method as claimed in claim 1, wherein the predefined transaction types include an e-commerce transaction and the payment credential format associated with the e-commerce transaction is a Primary Account Number (PAN), a card expiry date, and a Card Verification Value (CVV).

18. The method as claimed in claim 4, wherein the account type is an account associated with a corresponding physical payment card, the physical payment card having a static Primary Account Number (PAN), wherein the predefined transaction types include an e-commerce transaction and wherein the payment credential format associated with the e-commerce transaction is a card expiry date and a Card Verification Value (CVV).

19. The method as claimed in claim 1, wherein the predefined transaction types include an agent cash-out transaction, and wherein the payment credential format associated with the agent cash-out transaction is a Primary Account Number (PAN).

20. A system for provisioning payment credentials to a consumer, the system comprising a remotely accessible server in communication with an electronic device of a consumer, the remotely accessible server including:

a request receiving component for receiving a request for payment credentials required to conduct a transaction, the request originating from the electronic device of the consumer;

a type determining component for determining a transaction type associated with the transaction, the transaction type being one of a plurality of predefined transaction types wherein each transaction type is associated with a predefined payment credential format;

a credential obtaining component for obtaining payment credentials in the payment credential format associated with the determined transaction type; and

a transmitting component for transmitting the obtained payment credentials to the electronic device of the consumer for use in conducting the transaction.

21. The system as claimed in claim 20, wherein the credential obtaining component is configured to request the payment credentials required to conduct the transaction from an external credential generating module.

22. The system as claimed in claim 21, wherein the external credential generating module is operated by one of an issuer of the consumer and a payment processor.

23. The system as claimed in claim 20, wherein the credential obtaining component is configured to generate the payment credentials.

24. A computer program product for provisioning payment credentials to a consumer, the computer program product comprising a computer-readable medium having stored computer-readable program code for performing the steps of:

receiving a request for payment credentials required to conduct a transaction, the request originating from an electronic device of a consumer;

determining a transaction type associated with the transaction, the transaction type being one of a plurality of predefined transaction types wherein each transaction type is associated with a predefined payment credential format;

obtaining payment credentials in the payment credential format associated with the determined transaction type; and

transmitting the obtained payment credentials to the electronic device of the consumer for use in conducting the transaction.

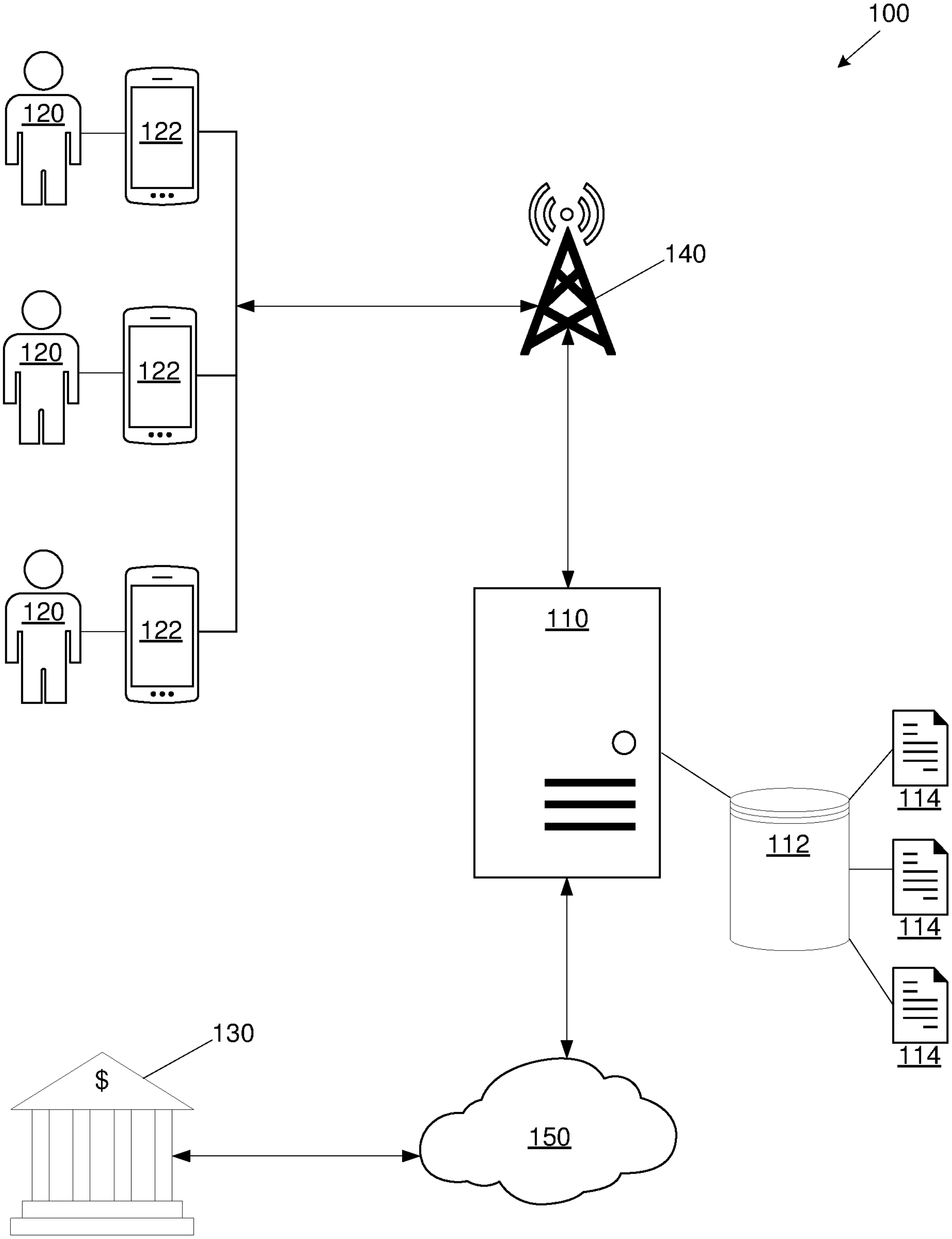


FIG. 1A

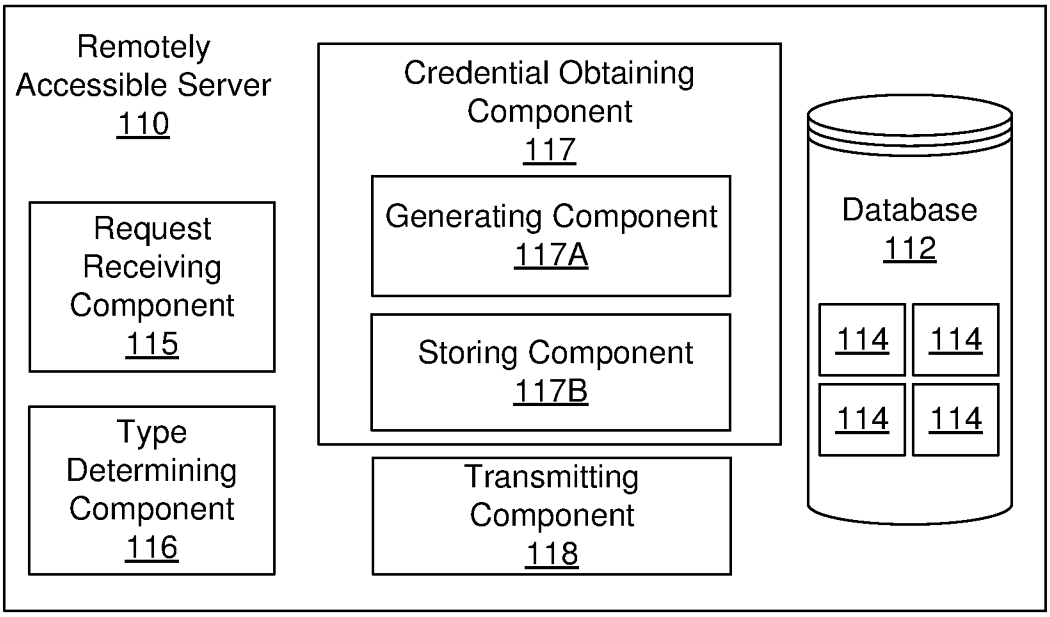

Remotely Accessible Server 110
Request Receiving Component 115
Type Determining Component 116
Credential Obtaining Component 117
Generating Component 117A
Storing Component 117B
Transmitting Component 118
Database 112
114
114
114
114

FIG. 1B

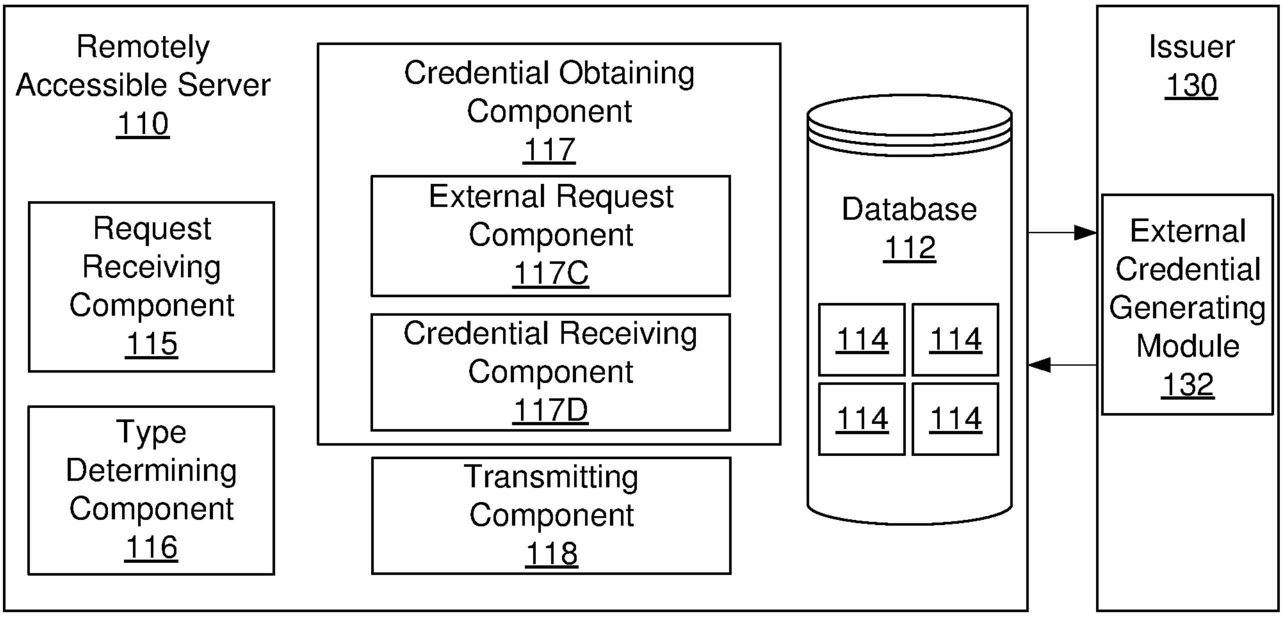

Remotely Accessible Server 110
Request Receiving Component 115
Type Determining Component 116
Credential Obtaining Component 117
External Request Component 117C
Credential Receiving Component 117D
Transmitting Component 118
Database 112
114
114
114
114
Issuer 130
External Credential Generating Module 132

FIG. 1C

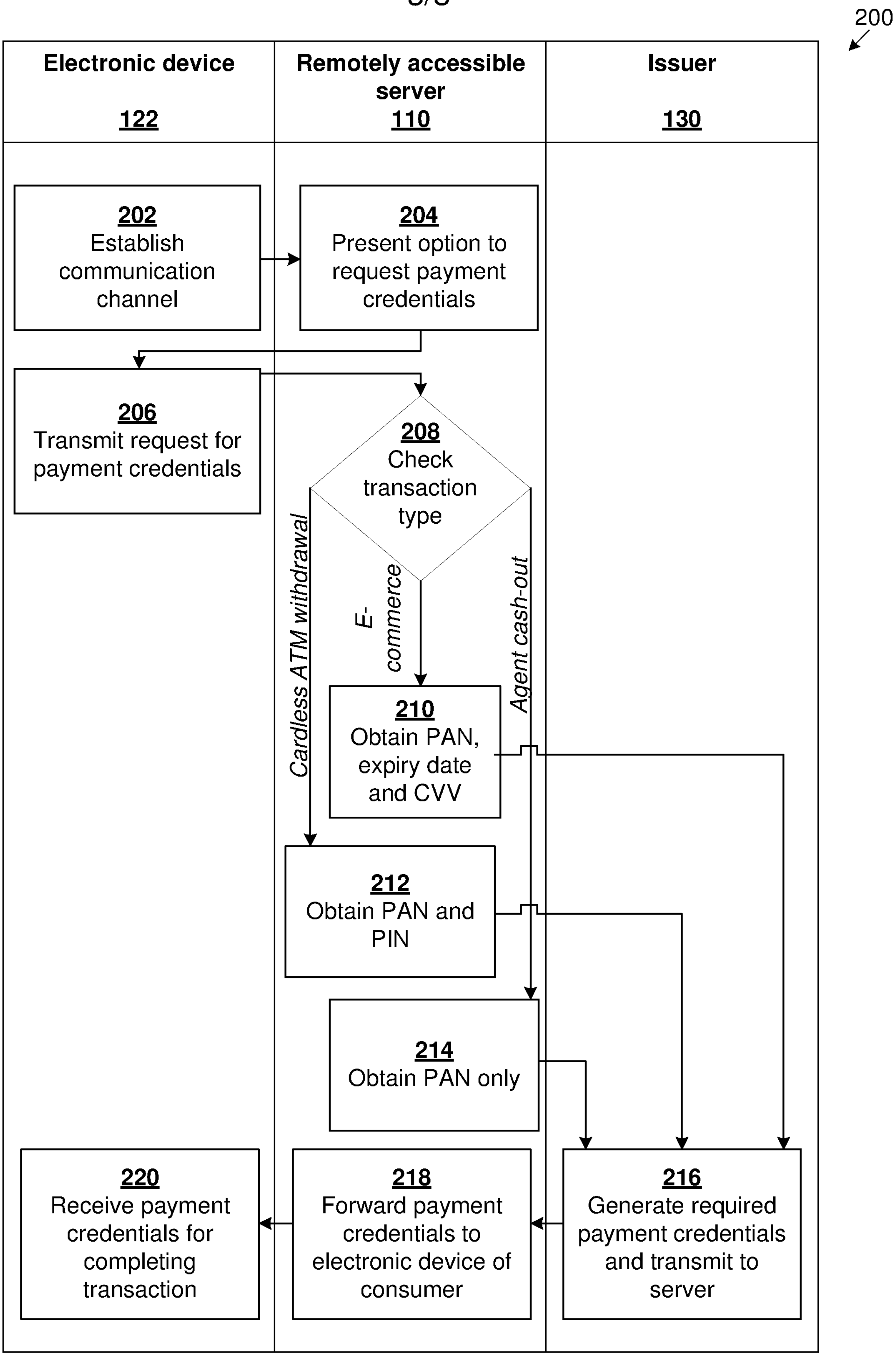

200
Electronic device
122
Remotely accessible server
110
Issuer
130
202
Establish communication channel
204
Present option to request payment credentials
206
Transmit request for payment credentials
208
Check transaction type
Cardless ATM withdrawal
E-commerce
Agent cash-out
210
Obtain PAN, expiry date and CVV
212
Obtain PAN and PIN
214
Obtain PAN only
216
Generate required payment credentials and transmit to server
218
Forward payment credentials to electronic device of consumer
220
Receive payment credentials for completing transaction

FIG. 2

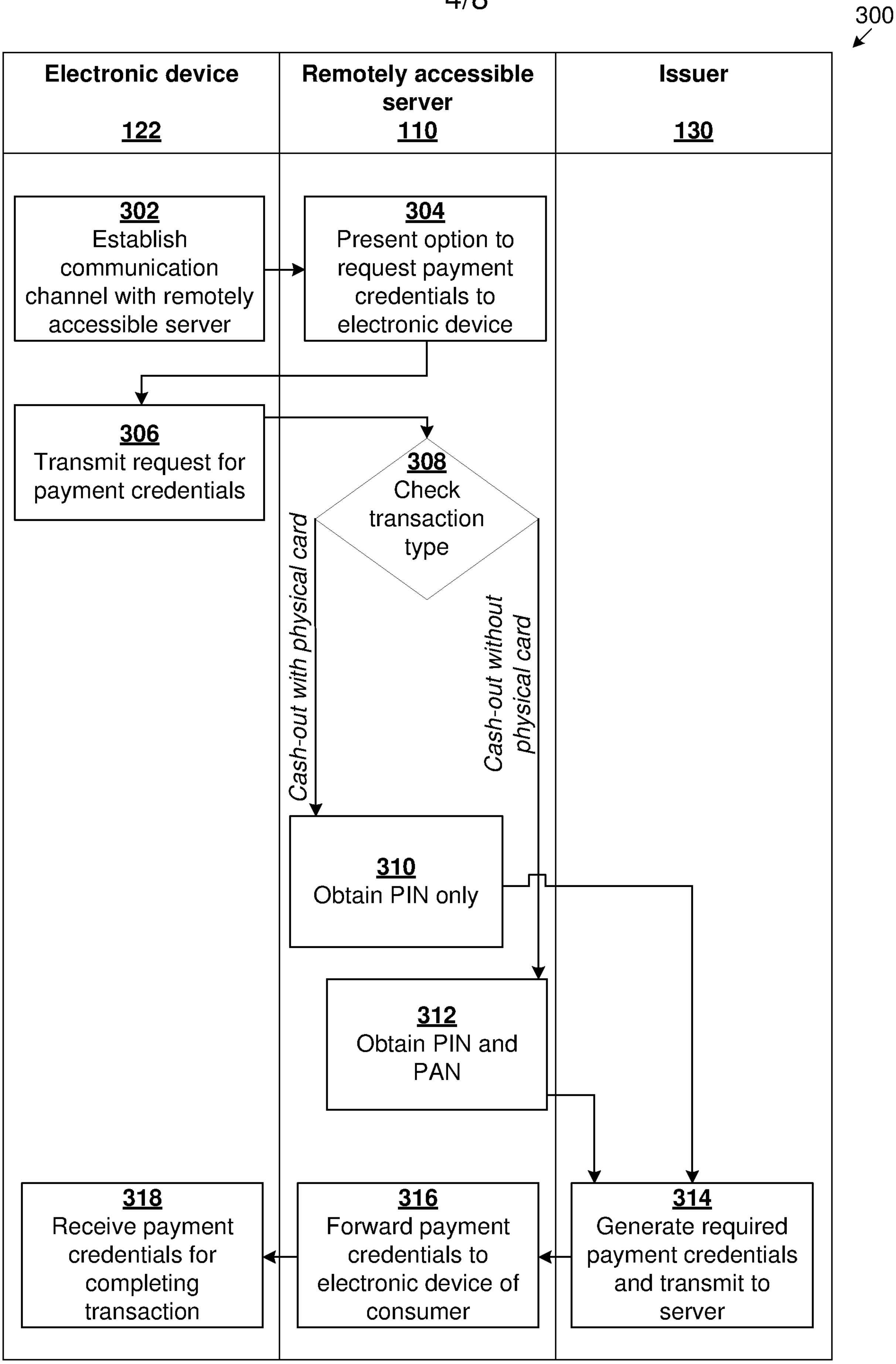
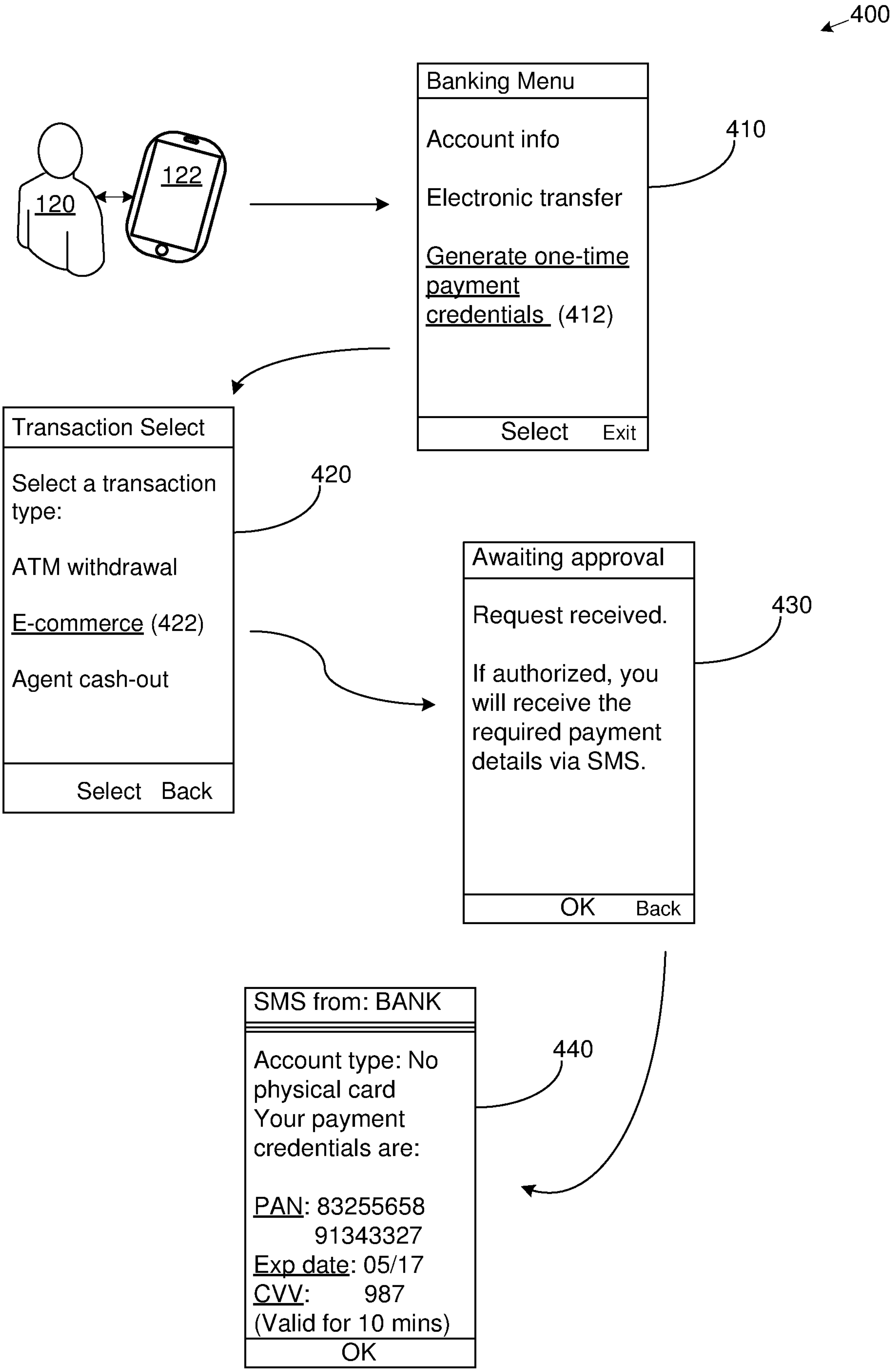

300
Electronic device
122
Remotely accessible server
110
Issuer
130
302
Establish communication channel with remotely accessible server
304
Present option to request payment credentials to electronic device
306
Transmit request for payment credentials
308
Check transaction type
Cash-out with physical card
Cash-out without physical card
310
Obtain PIN only
312
Obtain PIN and PAN
318
Receive payment credentials for completing transaction
316
Forward payment credentials to electronic device of consumer
314
Generate required payment credentials and transmit to server

FIG. 3



Banking Menu

Account info

Electronic transfer

Generate one-time payment credentials (412)

Select Exit

Transaction Select

Select a transaction type:

ATM withdrawal

E-commerce (422)

Agent cash-out

Select Back

Awaiting approval

Request received.

If authorized, you will receive the required payment details via SMS.

OK Back

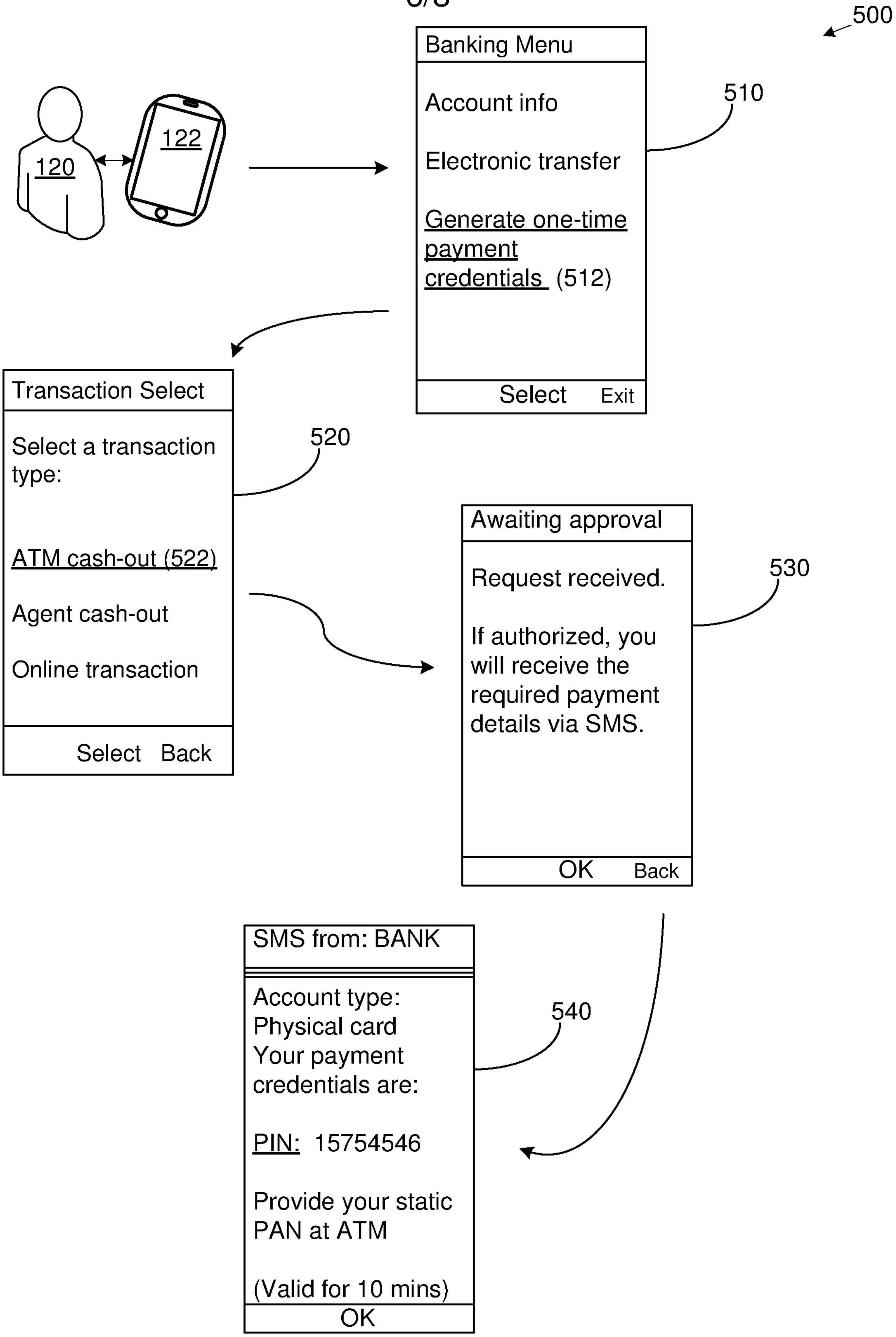
SMS from: BANK

Account type: No physical card
Your payment credentials are:

PAN: 83255658
91343327
Exp date: 05/17
CVV: 987
(Valid for 10 mins)

OK

FIG. 4



Request received.

If authorized, you will receive the required payment details via SMS.

Account type: Physical card
Your payment credentials are:

PIN: 15754546

Provide your static PAN at ATM

(Valid for 10 mins)

FIG. 5

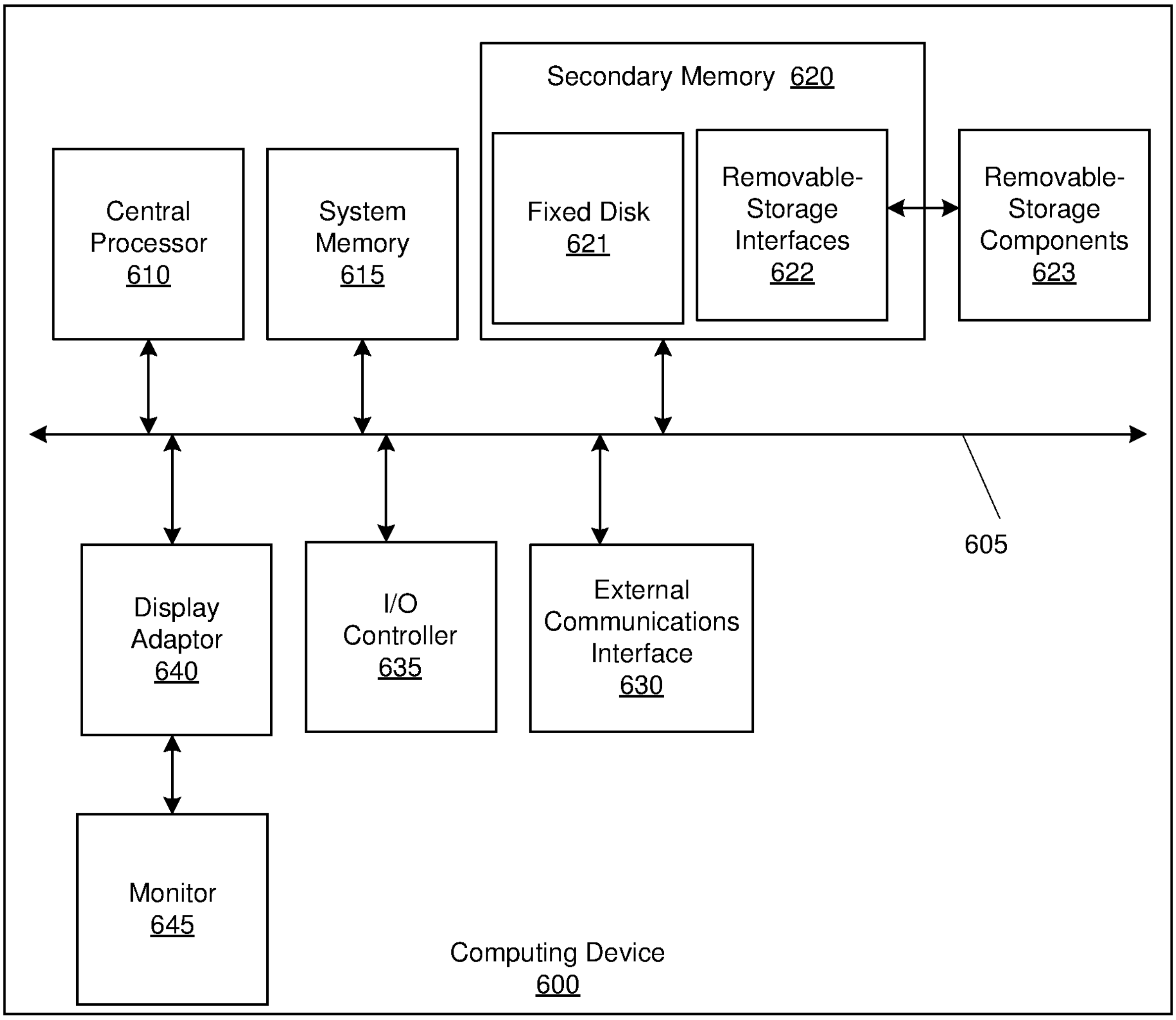

Secondary Memory 620
Central Processor 610
System Memory 615
Fixed Disk 621
Removable-Storage Interfaces 622
Removable-Storage Components 623
605
Display Adaptor 640
I/O Controller 635
External Communications Interface 630
Monitor 645
Computing Device 600

FIG. 6

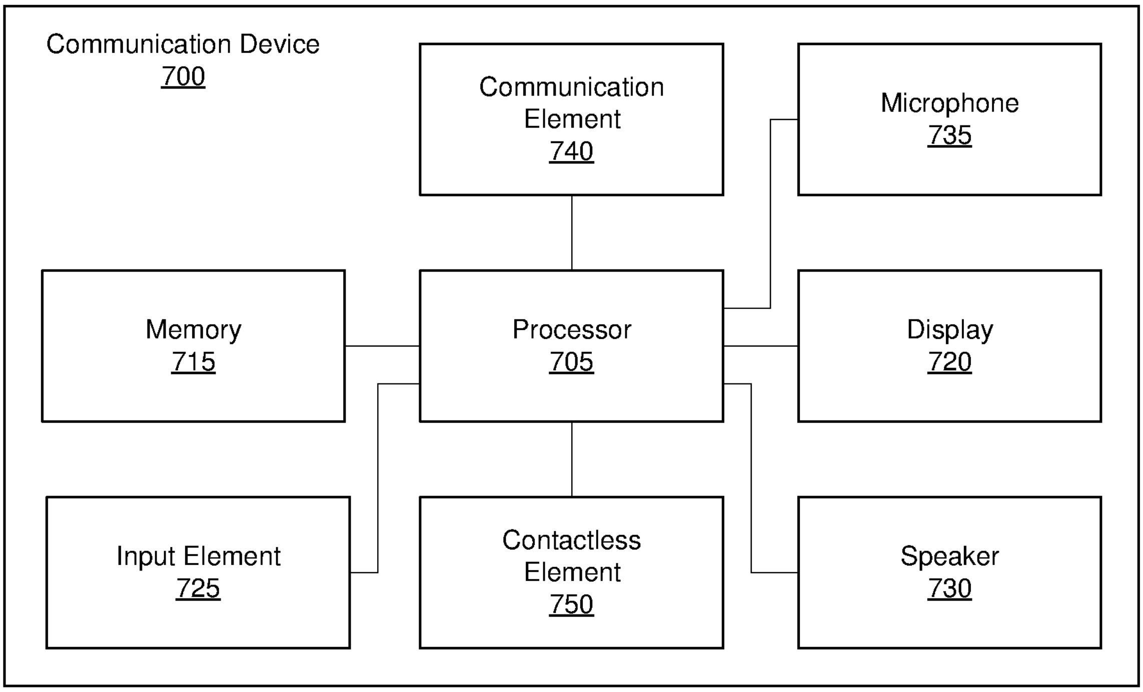

Communication Device
700
Communication Element
740
Microphone
735
Memory
715
Processor
705
Display
720
Input Element
725
Contactless Element
750
Speaker
730

FIG. 7

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IB2014/063339

A. CLASSIFICATION OF SUBJECT MATTER

G06Q 20/40(2012.01)i, G06Q 20/12(2012.01)i, G06Q 20/32(2012.01)i

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 20/40; G06K 7/10; G06Q 20/38; G06Q 40/00; G06Q 20/16; G06Q 20/00; G06K 9/18; G06Q 20/12; G06Q 20/32

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Korean utility models and applications for utility models
Japanese utility models and applications for utility models

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
eKOMPASS(KIPO internal) & keywords: transaction type, payment credential, request

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2012-0084200 A1 (MICHEL TRIANA) 05 April 2012 See paragraphs [0055]-[0061]; and figure 4.	1-24
Y	US 2010-0082444 A1 (GLORIA LIN et al.) 01 April 2010 See paragraphs [0097]-[0103], [0147]; claim 1; and figures 4, 11.	1-24
A	US 2009-0037333 A1 (DANIEL IAN FLITCROFT et al.) 05 February 2009 See paragraphs [0107]-[0114]; and figure 4.	1-24
A	KR 10-2012-0125443 A (BIZMODELINE CO., LTD.) 15 November 2012 See paragraphs [0033]-[0045]; and figures 1-2.	1-24
A	KR 10-2012-0105296 A (KOREA INFORMATION & COMMUNICATIONS CO., LTD.) 25 September 2012 See paragraphs [0054]-[0063]; and figures 1-2.	1-24

□ 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 18 December 2014 (18.12.2014)	Date of mailing of the international search report **18 December 2014 (18.12.2014)**
Name and mailing address of the ISA/KR International Application Division Korean Intellectual Property Office 189 Cheongsa-ro, Seo-gu, Daejeon Metropolitan City, 302-701, Republic of Korea Facsimile No. +82-42-472-7140	Authorized officer PARK, Hye Lyun Telephone No. +82-42-481-3463

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2012-0084200 A1	05/04/2012	None	
US 2010-0082444 A1	01/04/2010	None	
US 2009-0037333 A1	05/02/2009	AT 202647 T	15/07/2001
		AU 1999-30506 A1	18/10/1999
		AU 1999-30506 B2	06/06/2002
		AU 2000-25694 A1	04/09/2000
		AU 2000-38334 A1	14/11/2000
		AU 3050699 A	18/10/1999
		BR 9909065 A	05/12/2000
		CA 2322356 A1	30/09/1999
		CA 2322356 C	04/12/2001
		CA 2362033 A1	30/09/1999
		CA 2362033 C	30/12/2003
		CA 2363003 A1	24/08/2000
		CA 2366517 A1	19/10/2000
		CA 2366517 C	07/11/2006
		CN 1292131 A	18/04/2001
		CN 1347540 A	01/05/2002
		CN 1355910 A	26/06/2002
		DE 1029311 T1	19/04/2001
		DE 69900169 D1	02/08/2001
		DE 69900169 T2	07/03/2002
		DE 69900169 T3	29/06/2006
		DK 1029311 T3	22/10/2001
		EA 003027 B1	26/12/2002
		EP 1029311 A1	23/08/2000
		EP 1029311 B1	27/06/2001
		EP 1029311 B2	31/08/2005
		EP 1115095 A2	11/07/2001
		EP 1115095 A3	20/03/2002
		EP 1153375 A1	14/11/2001
		EP 1179206 A1	13/02/2002
		EP 1729267 A2	06/12/2006
		EP 1729267 A3	27/12/2006
		ES 2154625 T1	16/04/2001
		ES 2154625 T3	01/02/2002
		ES 2154625 T5	16/03/2006
		GR 3036728 T3	31/12/2001
		HK 1030472 A1	07/12/2001
		HU 0102408 A2	28/11/2001
		HU 0102408 A3	28/05/2003
		IE 990240 A1	20/10/1999
		IL 137456 A	19/03/2001
		IL 137456 D0	24/07/2001
		IL 141060 D0	10/02/2002
		JP 2002-508550 A	19/03/2002
		JP 2002-537619 A	05/11/2002

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
		JP 2002-541601 A	03/12/2002
		KR 10-2001-0040411 A	15/05/2001
		KR 10-2001-0102261 A	15/11/2001
		KR 10-2001-0110740 A	13/12/2001
		KR 10-2003-0051863 A	25/06/2003
		NO 20004657 A	16/11/2000
		NO 20004657 D0	19/09/2000
		NO 323708 B1	25/06/2007
		NZ 506636 A	26/11/2002
		PL 343253 A1	30/07/2001
		PT 1029311 E	28/12/2001
		SG 115360 A1	28/10/2005
		TR 200002758 T2	23/07/2001
		TW 440800 A	16/06/2001
		TW 440800 B	16/06/2001
		US 2003-0028481 A1	06/02/2003
		US 2009-0012897 A1	08/01/2009
		US 2009-0070260 A1	12/03/2009
		US 2009-0134217 A1	28/05/2009
		US 2013-0204781 A1	08/08/2013
		US 2014-0122340 A1	01/05/2014
		US 2014-0236831 A1	21/08/2014
		US 6636833 B1	21/10/2003
		US 7136835 B1	14/11/2006
		US 7433845 B1	07/10/2008
		US 7567934 B2	28/07/2009
		US 7571142 B1	04/08/2009
		US 7593896 B1	22/09/2009
		US 7895122 B2	22/02/2011
		US 8676707 B2	18/03/2014
		US 8756150 B2	17/06/2014
		WO 1999-049424 A1	30/09/1999
		WO 2000-049586 A1	24/08/2000
		WO 2000-062259 A1	19/10/2000
KR 10-2012-0125443 A	15/11/2012	KR 10-2004-0075159 A	27/08/2004
		KR 10-2011-0131156 A	06/12/2011
		KR 10-2012-0040690 A	27/04/2012
		KR 10-2014-0014046 A	05/02/2014
KR 10-2012-0105296 A	25/09/2012	None	