

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
2 October 2008 (02.10.2008)

PCT

(10) International Publication Number
WO 2008/118582 A1

(51) International Patent Classification:
H04L 9/00 (2006.01) *G06Q 30/00* (2006.01)

(74) Agents: GIBBY, Darin, J. et al.; Townsend and Townsend and Crew LLP, 1200 17th Street, Suite 2700, Denver, Colorado 80202 (US).

(21) International Application Number:
PCT/US2008/054683

(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, BR, BW, BY, BZ, CA, CH, 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, IS, JP, KE, KG, KM, 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, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(22) International Filing Date:
22 February 2008 (22.02.2008)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
11/677,960 22 February 2007 (22.02.2007) US

(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, NO, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

(71) Applicant (for all designated States except US): **FIRST DATA CORPORATION** [US/US]; 6200 S. Quebec St., Suite 270, Greenwood Village, Colorado 80111 (US).

(72) Inventor; and

(75) Inventor/Applicant (for US only): **ROYYURU, Vijay** [US/US]; 7010 Windswept Lane, Norristown, Pennsylvania 19403 (US).

Published:

— with international search report

(54) Title: PROCESSING OF FINANCIAL TRANSACTIONS USING DEBIT NETWORKS

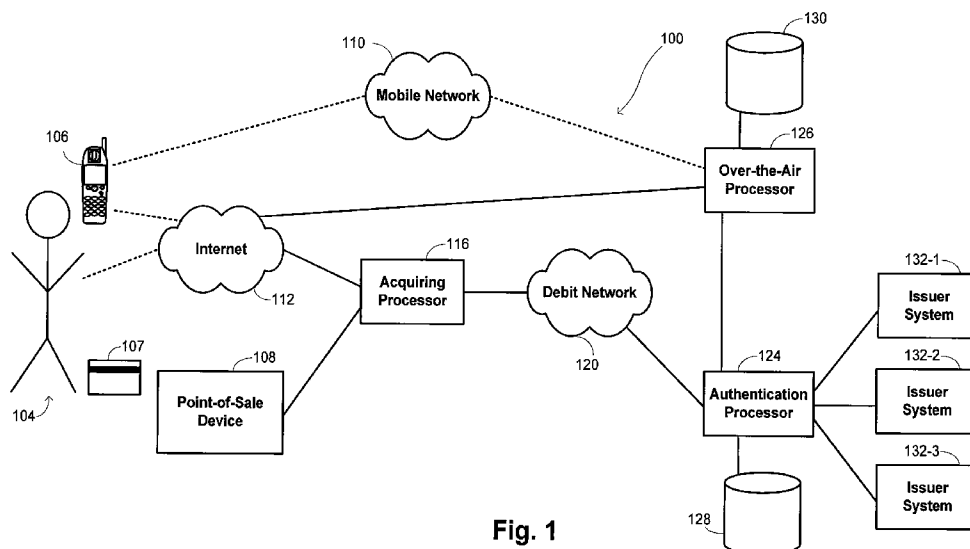


Fig. 1

(57) Abstract: Methods and systems are disclosed for executing financial transactions between customers and merchants. An identifier of a financial account is received from the customer at a merchant system. A one-time password is also received from the customer at the merchant system, with the customer having been provided with the one-time password by a mobile electronic device or contact less presentation instrument. A cryptogram is generated to include the identifier of the financial account encrypted using the one-time password. An authorization request is formulated at the merchant system. The authorization request includes the cryptogram and transaction information describing at least a portion of the financial transaction. The authorization request is transmitted from the merchant system to an authorization processor for authorization of the financial transaction.

PROCESSING OF FINANCIAL TRANSACTIONS USING DEBIT NETWORKS

5 CROSS REFERENCE TO RELATED APPLICATION

[0001] This application is related to commonly assigned, concurrently filed U.S. Pat. Appl. No. 11/677,967, filed February 22, 2007, entitled, "MANAGEMENT OF FINANCIAL TRANSACTIONS USING DEBIT NETWORKS," filed by Vijay Royyuru and Robert
10 Freisheim (Attorney Docket No. 20375-081000US), the entire disclosure of which is incorporated herein by reference for all purposes.

BACKGROUND OF THE INVENTION

15 [0002] This application relates generally to financial transactions. More specifically, this application relates to processing of financial transactions using debit networks.

[0003] In a modern commercial environment, there is an array of different financial products that consumers have available to them in executing financial transactions. Some of
20 the more prevalent forms of transactions may be characterized as credit transactions, debit transactions, and stored-value transactions. Each of these transactions differs in the manner in which access to funds is provided to the consumer. For example, credit transactions are supported by funds provided by a creditor to a customer. The principal example of such credit transactions are credit-card transactions in which the creditor issues a card to the
25 customer that the customer may use as a presentation instrument to identify a credit account. When the transaction is executed, funds are drawn against the credit account, which usually has a pre-established credit limit, to support the transaction.

[0004] The other major types of financial transactions also make use of presentation instruments. A stored-value transaction is one in which funds have been specifically set aside
30 and associated with a presentation instrument so that they may be used to support a transaction. In most cases, such stored-value instruments are anonymous in that the funds are

associated only with the instrument and not with any particular person. This has the advantage that such instruments may be easily transferred and they find wide utility as gift cards. This gift aspect is frequently reinforced by imposing restrictions on the merchant with whom transactions may be executed with the set-aside funds.

5 **[0005]** Debit transactions may also make use of a presentation instrument and are similar to stored-value transactions in that specifically identified funds are used to support the transactions. The source of funds for a debit transaction is specifically identified with a holder of the account that holds the funds and this account is usually a demand-deposit account maintained at a financial institution. As such, the funding of the account varies over
10 time as deposits and withdrawals are made from the account in response to receipt of wages, paying bills, etc. Debit accounts generally differ from stored-value accounts in that the account owner is provided with open-ended access, with all activity being based on the currently available funds level. Stored-value transactions might be considered to be a subset of debit transactions in which some money is set aside, but where there is no free access to
15 funds in the account. For instance, some stored-value accounts do not allow additional deposits, permitting only withdrawals to be made from the accounts in accordance with governing restrictions of the accounts.

[0006] The ability to transfer funds from a demand-deposit or other type of account in such a short time period is enabled by the use of one or more electronic networks provided as
20 part of a financial infrastructure. Communications routed over these networks permit decisions to be made in real time whether the criteria for executing a transaction — valid accounts are identified, there are sufficient funds in the supporting account, identity-verification protocols have been satisfied, etc. — are met. Such debit transactions are of particular interest to many merchants because they remove the element of trust that is
25 required of other transactions. The time lag of check transactions runs the risk that the check will be refused, forcing the merchant to expend time and effort in recovering funds due for a previously executed transaction. And while credit transactions usually involve some authorization process, there are mechanisms that may be used after the fact to prevent the payment from being made. From the perspective of merchants, debit transactions have the
30 advantage that funds are received substantially contemporaneously with execution of the transaction itself. If there are later disputes regarding the transaction, the merchant is in the superior position by having possession of the funds at that time.

[0007] There is accordingly a general need in the art for improved methods and systems of supporting debit transactions.

5

BRIEF SUMMARY OF THE INVENTION

[0008] Embodiments of the invention provide methods and systems for executing financial transactions between customers and merchants. In a first set of embodiments, an identifier of a financial account is received from the customer at a merchant system. A one-
10 time password is also received from the customer at the merchant system, with the customer having been provided with the one-time password by a mobile electronic device or a contactless presentation instrument. A cryptogram is generated, with the cryptogram comprising the identifier of the financial account encrypted using the one-time password. An authorization request is formulated at the merchant system. The authorization request
15 comprises the cryptogram and transaction information describing at least a portion of the financial transaction. The authorization request is transmitted from the merchant system to an authorization processor for authorization of the financial transaction.

[0009] In a second set of embodiments, an encrypted authorization request is received from a merchant system at an authorization processor, with the authorization request having
20 been encrypted by application of a one-time password provided to the customer by a debit presentation instrument. The authorization request is decrypted. A financial account is identified from the decrypted authorization request. Transaction information describing at least a portion of the financial transaction is determined from the decrypted authorization request. Authenticity of the transaction information is determined by validating the one-time
25 password. It is determined whether the identified financial account is capable of supporting the financial transaction based on the transaction information.

[0010] In either set of embodiments, there may be a number of specific features. For example, the identifier may comprise an account number of the financial account. In other instances, it may comprise an identification number extracted from a presentation instrument,
30 with the identification number being translated to an account number of the financial account. The one-time password may comprise a two-factor one-time password. In certain cases, the one-time password is a second one-time password provided to the customer by the mobile

electronic device after passage of an expiry time after a first one-time password is provided to the customer by the mobile electronic device. In some cases, an intermediate authentication processor translates the identifier to a primary account number or card number that the authorization processor recognizes. In certain embodiments, a personal identification number is received from the customer at the merchant system, with the authorization request further comprising the personal identification number. Cryptographic keys used to generate the one-time password on the presentation instrument, and to validate the one-time password on the authentication processor, may either be generated on the presentation instrument and transferred to the authentication processor, or be generated on the authentication processor and transferred to the presentation instrument.

[0011] The merchant system may sometimes comprise an Internet web server and, at other times, comprises a merchant point-of-sale device. The mobile electronic device may comprise a cellular telephone. In some embodiments, the transaction information comprises a total cost for the financial transaction, or other descriptive data elements of the transaction such as location, terminal identifier, terminal sequence number, date, and/or time.

[0012] Methods of the invention may also be embodied by a computer-readable storage medium having a computer-readable program embodied therein for directing operation of a merchant system or of an authorization processor, either of which may include a communications system, a processor, and a storage device. The computer-readable program includes instructions for operating the respective devices to implement the methods as described above.

BRIEF DESCRIPTION OF THE DRAWINGS

[0013] A further understanding of the nature and advantages of the present invention may be realized by reference to the remaining portions of the specification and the drawings wherein like reference numerals are used throughout the several drawings to refer to similar components. In some instances, a sublabel is associated with a reference numeral and follows a hyphen to denote one of multiple similar components. When reference is made to a reference numeral without specification to an existing sublabel, it is intended to refer to all such multiple similar components.

[0014] Fig. 1 is a schematic illustration of a financial architecture within which embodiments of the invention may be executed;

[0015] Fig. 2 is a schematic illustration of a computational unit that may be included as parts of elements of the financial architecture of Fig. 1;

5 [0016] Fig. 3 is a flow diagram summarizing methods of providing cards suitable for use in contactless debit transactions to customers;

[0017] Fig. 4 is a flow diagram summarizing methods of enabling mobile electronic devices to be used by customers in debit transactions;

10 [0018] Fig. 5 is a flow diagram summarizing enrollment methods used in some embodiments of the invention;

[0019] Fig. 6 is a flow diagram summarizing methods of executing debit transactions using the cards provided with the method of Fig. 3;

[0020] Fig. 7 is a flow diagram summarizing methods of executing debit transactions using mobile electronic devices configured according to the method of Fig. 4; and

15 [0021] Fig. 8 is a flow diagram summarizing use of a federated authentication web service to execute transactions in accordance with certain embodiments of the invention.

DETAILED DESCRIPTION OF THE INVENTION

20 [0022] Embodiments of the invention provide a number of different techniques for executing debit transactions. Some of these embodiments involve the use of “contactless” transactions that make use of a presentation instrument. In many instances, such a presentation instrument may take a form that is conventional in appearance, such as in the form of a credit-card-sized card, or may take a less conventional form, examples of which
25 include key fobs or other kinds of instruments. Contactless transactions may be executed in some embodiments with a mobile electronic device. Transactions that are “contactless” are those that are executed with only wireless interaction between the presentation instrument and a merchant point-of-sale device. Conventional debit transactions involve contact between these elements because account information is conventionally stored on one or more
30 tracks of a magnetic stripe that is affixed to the presentation instrument. These tracks are

read by swiping the presentation instrument through a magnetic-stripe reader comprised by the point-of-sale device. While some forms of contactless transaction have been attempted in the past, these have involved such techniques as optically reading a bar code from a presentation instrument, often requiring that certain information conventionally stored on the magnetic-stripe tracks be stored instead in a database that forms part of the financial architecture, i.e. either locally to the point-of-sale device or at some other location in communication with the point-of-sale device. Other forms of contactless transactions have involved transmission of the same data from the presentation instrument to a the merchant point-of-sale device, as would have been transmitted for a magnetic-stripe card. There are also a number of security issues associated with such arrangements. Embodiments of the invention use a structure in which both the information-management and security issues are better addressed.

[0023] Other embodiments of the invention provide techniques for using mobile electronic devices in executing Internet-based transactions. Examples of mobile electronic devices that may be used in different embodiments include mobile telephones, personal digital assistants, and the like. In some instances, the description may refer by way of example to the use of mobile telephones, it being understood that such references are intended merely to be illustrative and not to be limiting.

[0024] These various embodiments may be implemented in a financial architecture like that shown in Fig. 1. In this illustration, the architecture 100 is structured generally around a debit network 120, but it should be recognized that this is a depiction of only a portion of a larger financial infrastructure within which the architecture may be embodied. Other financial networks used in implementing credit, stored-value, or other types of transactions may be provided in communication with some of the elements shown in this drawing, even if not explicitly indicated. The debit network 120 generally comprises a private electronic communications network that implements security protocols commensurate with the sensitive nature of the financial information that is routed through the network 120. Such security protocols and methods for their implementation are well known to those of skill in the art.

[0025] Interactions with the debit network 120 are provided through a variety of different kinds of processors that are interfaced with the network. For example, front-end interactions may take place through an acquiring processor 116 that is in communication with

the Internet 112 and/or point-of-sale devices 108 that are used in execution of the underlying financial transactions. The back-end interactions may take place with an authentication processor 124, the specific functionality of which is described in further detail for some embodiments below.

5 **[0026]** Other communications within the architecture 100 may take place through a mobile network 110 that is interfaced with an over-the-air processor. The authentication processor 124 and over-the-air processor 126 may each make use of data stored in respective databases 128 and 130.

10 **[0027]** Endpoints of the architecture 100, at least from the perspective of the kinds of transactions discussed herein, are a customer 104 who interacts with the Internet 112 and/or point-of-sale device 108 to interface with the front end and issuer systems 132 that are in communication with the authentication processor 124. The issuer systems 132 may act as authorization processors as described in specific detailed embodiments below. In some instances, the customer 104 may have supplementary interactions with the architecture
15 through a mobile electronic device 106 and/or may use a contactless presentation instrument 107 depending on specific implementations. These interactions proceed through the mobile network 110 that is accessible by the mobile electronic device and that is in communication with the over-the-air processor 128. Each of the issuer systems 132 is a computational system that is operated by an issuer of the presentation instrument or that manages the
20 account used to support the transaction. Such issuers are thus frequently financial institutions such as banks, credit unions, or the like, that maintain demand-deposit or other types of financial accounts that may be used to support debit transactions.

25 **[0028]** Fig. 2 provides a schematic illustration of a physical structure that may be used to implement different computational systems that may form part of the architecture 100 of Fig. 1. For example, the computational systems 200 shown in Fig. 2 might correspond to a structure used for the mobile electronic device 106, for the contactless presentation instrument 107, for the acquiring processor 116, for the authentication processor 124, for the over-the-air processor 126, and/or for any of the issuer systems 132 in different embodiments. Fig. 2 broadly illustrates how individual system elements may be
30 implemented in a separated or more integrated manner. The computational system 200 is shown comprised of hardware elements that are electrically coupled via bus 226, including a processor 202, an input device 204, an output device 206, one or more storage devices 208, a

computer-readable storage media reader 210a, a communications system 214, a processing acceleration unit 216 such as a DSP or special-purpose processor, and a memory 218. The computer-readable storage media reader 210a is further connected to a computer-readable storage medium 210b, the combination comprehensively representing remote, local, fixed, and/or removable storage devices plus storage media for temporarily and/or more permanently containing computer-readable information. The communications system 214 may comprise a wired, wireless, modem, and/or other type of interfacing connection and permits data to be exchanged within the architecture 100 to implement embodiments described herein.

[0029] The computational system 200 also comprises software elements, shown as being currently located within working memory 220, including an operating system 224 and other code 222, such as a program designed to implement methods of the invention. It will be apparent to those skilled in the art that substantial variations may be made in accordance with specific requirements. For example, customized hardware might also be used and/or particular elements might be implemented in hardware (perhaps including tamper-resistant storage media for secure storage of cryptographic keys), software (including portable software, such as applets), or both. Further, connection to other computing devices such as network input/output devices may be employed.

[0030] To participate in financial transaction methods of the invention, a customer 104 may first be enrolled. Such enrollment establishes sets of data that may be used and manipulated in implementing embodiments of the invention. Such data may be stored in the databases 128 and/or 130 as well as on the presentation instrument and/or mobile electronic device 106. A general overview of how enrollment may be accomplished in embodiments that use physical presentation instruments is provided with the flow diagram of Fig. 3, while a corresponding overview of how enrollment may be accomplished in embodiments that make use of mobile electronic devices is illustrated with the flow diagram of Fig. 4.

[0031] When contactless-card presentation instruments are issued by financial institutions, they are typically prepared using batch processes. Block 304 of Fig. 3 accordingly indicates that a production file is prepared by an issuer processor. Such a production file typically includes information defining the nature of the individual presentation instruments. For instance, when the presentation instruments comprise cards, the production file may include numbers to be embossed on the cards. It may also include

information identifying the individuals to be associated with each instrument, as well as identifying the financial account that will be used to support transactions executed with the instruments. A manufacturer of presentation instruments may also produce blank versions of the instruments at block 308. For example, when the presentation instruments comprise
5 cards, blank versions of the cards may be prepared by a card manufacturer that include a debit application that will be executed when performing debit transaction. Irrespective of their specific form, each of these instruments is equipped with structure that enables them to be used in contactless communications. For example, the instrument may have an embedded electromagnetic chip that receives and transmits electromagnetic signals at radio or other
10 frequencies. Once created, these instruments are delivered by the card manufacturer to the card producer at block 312.

[0032] Having received the production file and the blank cards, the card producer may engage in personalization processes at block 316 by writing information to the blank instruments in accordance with the specifications in the production file. This initial
15 personalization may include both direct physical alterations to the instrument, such as when cards are embossed with card numbers, and may additionally include writing data to storage maintained on the instrument itself. For instance, card numbers, cryptographic keys, account or identification numbers, and/or merchant loyalty identification numbers, in addition to other data, may additionally be stored as data on the card so that this information may be accessed
20 and transmitted as appropriate in implementing embodiments of the invention.

[0033] In addition to this personalization information, the card producer may implement certain encryption protocols that will be used in enhancing the security of transactions executed with the instruments. In one implementation, public-key-private-key encryption is used within a public-key infrastructure ("PKI"). Consistent with such an
25 infrastructure, at block 320 the card producer generates a PKI key pair for each card, referred to herein as the "card encryption key pair." The public key of the pair is transmitted by the card producer, together with an indication of the card number that it refers to, to the authentication processor 124 at block 324 and the private key of the pair is retained on the card. Having been so prepared, the instrument is ready for transmission to the customer at
30 block 328.

[0034] In addition to this use of the production file by the card producer in preparing the instruments, the production file may be provided to the authentication processor 124 at

block 132. The combination of the production file and the key information received from the card producer provides the authentication processor 124 with sufficient information to authenticate transactions as they are performed with the instruments. Both of these forms of information may be stored in database 128. The individual instruments may be activated
5 after receipt by customers at block 336 using a process defined by the issuer producer. In some instances, this activation is performed by interactions between the customer 104 and the authentication processor 124, such as may be achieved over the Internet, through the use of a voice-response unit, or the like. One purpose of this activation step is to reduce the risk of fraud by confirming receipt of the instrument by the correct customer 104. A comparison can
10 accordingly be made between information provided by the customer 104 during this activation with information extracted from the production file by the authentication processor 124.

[0035] In some instances, the presentation instruments may be created with certain redundancies of information. This is especially suitable, for example, in embodiments where
15 a card is to be equipped for both contactless and conventional transactions. Such multifunction cards may include an electromagnetic chip such as a radio-frequency identification chip to perform contactless transactions as well as a magnetic stripe or other mechanism that stores information that can be read by a device in contact with the card.

[0036] Some aspects of the enrollment shown in Fig. 4 for enrolling a mobile
20 electronic device 106 are similar to parts of the enrollment described in connection with Fig. 3. The method may begin, for example, with the customer visiting an Internet web site managed by the over-the-air processor 126 at block 404. This web site acts as a provisioning web site that may be used by the over-the-air processor 126 in effecting enrollment functions. The customer provides enrollment information at block 408. Such enrollment information
25 may comprise, for example, an identification number that generally corresponds to the card number of a debit card in more conventional debit transactions, in addition to the access number for the mobile device 106 to be enrolled.

[0037] This information is used by the over-the-air processor 126 at block 412 to enroll the identification number with the authentication processor 124 at block 412. An
30 exchange of verification information acts to confirm that the correct mobile device 106 is enrolled. One example of such an exchange shown in Fig. 4 involves the transmission of a short-message-service ("SMS") message to the mobile device 106 identified by the access

number provided at block 408. In one instance, the SMS message includes a provisioning URL that is used by the customer to confirm the verification information.

[0038] At block 424, the over-the-air processor 126 downloads a software debit application to the mobile device 106. The debit application resident on the mobile electronic device 106 generates a cryptographic key at block 428. This cryptographic key is a direct analogue of the key discussed in connection with Fig. 3 for the generation of presentation instruments. As indicated at block 432, the debit application transmits the cryptographic key using the mobile device to the over-the-air process 126. The over-the-air processor 126 then transmits it to the application processor 124 at block 436, resulting in the authentication processor 124 now having all the requisite information to process a transaction in the manner described below.

[0039] Fig. 5 is a flow diagram that summarizes a provisioning using the over-the-air processor 126 that may be used in some embodiments. Such provisioning permits enrollment to be accomplished by the customer using a combination of information provided over an Internet connection to a web site and information provided over a mobile network 110 from a mobile electronic device 106. The method begins at block 504 with the customer visiting the enrollment web site. Once connected to this site, the customer enters the identification number at block 508. Similar to the description of the processes of Fig. 4, such an identification number may correspond to a more conventional card number of a debit card.

[0040] In addition to this information, the customer enters the PIN on the mobile electronic device 106 using an interface for doing generated for display on the mobile electronic device. This information is transmitted from the mobile electronic device 106 over the mobile network 110 to the over-the-air processor 126 at block 516. The combination of information is provided to the authentication processor 124, with the over-the-air processor 126 transmitting the PIN to the authentication process 124 at block 520 and the enrollment web site transmitting the identification number to the authentication processor 124 at block 524. This combination of information is then used by the authentication processor 124 at block 528 to complete the enrollment of the mobile electronic device 106, permitting it subsequently to be used as a presentation instrument.

[0041] Figs. 6 and 7 are flow diagrams that illustrate methods that may be implemented to support debit transactions using the contactless presentation instruments or mobile electronic devices enrolled in accordance with Figs. 3 and 4. Fig. 6 provides an

illustration of methods for executing and supporting debit transactions made using a contactless card. Such transactions generally take place at a physical merchant location, with the drawing accordingly indicating that the method begins at block 604 with a customer selecting goods and/or services for purchase at the merchant location. If the transaction is not to be completed as a contactless transaction, the instrument may be swiped at block 648 to read information from a magnetic stripe or otherwise read with a device in contact with the instrument to proceed with a conventional form of transaction.

[0042] If the transaction is to be executed as a contactless transaction, the instrument is activated with a contactless mechanism at block 612. It is anticipated that such activation will normally be accomplished using an electromagnetic mechanism, although any contactless mechanism that may be implemented may be used in alternative embodiments.

[0043] The flow diagram also accounts for the fact that different kinds of transactions may be supported as contactless transactions. One distinction that may be made among transactions is the need to supply a personal identification number ("PIN") as evidence of authorization to use the presentation instrument. The PIN is a number that is preferably kept secret by the account owner so that that person is the only one authorized to use the instrument, but in practice PIN's are sometimes shared with family members or friends who are authorized by the account holder to execute transactions with the instrument. While the PIN offers a higher level of security for transactions, there are embodiments in which transactions will be permitted without verification of a PIN. These transactions are typically smaller transactions, so that a particular embodiment might permit transactions to be executed without a PIN when they are less than \$25 but require a PIN when the transaction size exceeds \$25. If the transaction is to be a PIN transaction as checked at block 616, the customer enters the PIN information with the point-of-sale device 108 at block 652.

[0044] To execute any transaction, whether it requires a PIN or not, account information is retrieved contactlessly from the presentation instrument by the point-of-sale device 108. The content of this information may vary in different embodiments, with it including or not including PIN information in accordance with the type of transaction being executed. The account information is signed digitally with the card key that is resident on the presentation instrument at block 620. This signed account information is transmitted at block 624 in a contactless way from the presentation instrument to the point-of-sale device 108. Merchant point-of-sale devices 108 may deliver transaction data elements to the contactless

presentation instrument during the contactless transaction session and such data elements may be included in derivation of the transaction digital signature.

[0045] With this information, the merchant point-of-sale device 108 has sufficient information to generate a transaction request at block 628 by combining the signed account information with transaction information. The transaction information usually specifies at least a total amount for the transaction and an account under the control of the merchant to which the transaction amount is to be transferred. In certain circumstances, the transaction information may include other information, such as the location at which the transaction is to be executed, the specific items comprised by the transaction, and the like. The resulting transaction request is transmitted by the merchant point-of-sale device 108 to the authentication processor 124, which is then equipped to parse the transaction request to extract the information needed to make an authentication decision. The customer-account information comprised by the transaction request may be resolved with the card public key at block 632, permitting the authentication processor 124 to identify the issuer and specific account to be used in supporting the transaction.

[0046] With such a resolution, the decision-making process implemented by the authentication processor 124 may be relatively simple. A check is made by the at block 636 to validate the cryptogram included in the encrypted authorization request transaction. If this authentication check fails, a transaction denial code is returned to the merchant point-of-sale device 108 at block 656 so that the merchant can refuse the transaction or request some other financial support for it from the customer 104.

[0047] Upon successful completion of the authentication check at the authentication processor, the authorization request transaction is forwarded to an authorization processor 132 to determine whether there are sufficient funds in the identified account to cover the transaction amount. If there are sufficient funds in the identified account, as checked at block 641, a transaction authorization code is returned by the authentication processor 124 at block to the merchant point-of-sale device 108, indicating to the merchant that the transaction may be completed at block 644. Funds are debited in real time from the customer account and transferred to the control of the merchant by depositing them into the merchant account identified with the transaction request. If there are insufficient funds, a transaction denial code may be returned by the authentication processor 124 to the merchant point-of-sale device 108 at block 642.

[0048] In other embodiments, the authorization decision may be more complex than simply considering whether the total transaction amount exceeds the funds available in the customer account. For example, some implementations include item-level restrictions that the funds may be applied to so that the customer is restricted in use of those funds to purchasing only certain approved items. Alternatively, the customer account might be restricted so that its funds can only be applied to transactions executed at certain approved merchants. In each of these and in other circumstances, the decision-making processes applied by the authentication processor 124 may consider the data received as part of the transaction request on this more detailed level to determine whether to authorize the transaction.

[0049] A number of aspects of transactions executed using a mobile electronic device as summarized with the flow diagram of Fig. 7 are similar to execution of a contactless transaction. Block 704 indicates that the customer 104 selects goods and/or services to purchase from a merchant at block 704. These goods and services may be purchased at a merchant location or may be purchased remotely such as over the Internet 112, the different transaction types resulting in different processing described below.

[0050] A check is accordingly made of the transaction mode at block 708. If the transaction occurs at a merchant location, a check may be made whether to execute the transaction as a PIN or non-PIN transaction. This is indicated at block 712. Often such a decision hinges some characteristic of the transaction like its total size. If the transaction is to be a PIN transaction, the customer may enter the PIN using a keypad comprised by the mobile electronic device 106. This may be included as part of the account information that is digitally signed and transmitted from the mobile device 106 to the merchant point-of-sale device 108 at block 720. This digital signing is similar to the signing performed with contactless cards in Fig. 6 by performing an encryption using the cryptographic key, but is performed by the mobile electronic device 106.

[0051] The signed account information is used by the merchant point-of-sale device 108 in generating a transaction request that is then transmitted to the authentication processor at block 724. In addition to the signed account information, the transaction request may include details of the transaction, usually including at least a transaction amount but perhaps sometimes additionally including such information as item-level identifications of the specific goods and services that form part of the transaction.

[0052] When an Internet-based transaction is to be performed, the customer may enter the PIN using the keypad on the mobile device at block 730 and the mobile device 106 may load a one-time password at block 728. In some embodiments, the one-time password comprises a two-factor one-time password. Conventionally, a number of different factors may be used to provide security for authentication. For instance, such factors may include something that the customer has, something that the customer knows, and something that the customer is. A two-factor one-time password is based on two such factors. In a particular implementation, the two factors are something that the customer has, such as possession of the presentation instrument, and something that the customer knows, such as the PIN. The customer enters the identification number for his account at block 732 with the password read from the mobile device. This provides sufficient information for the merchant operating the web site to generate an authorization request at block 736. The authorization request is transmitted by the merchant web server to the authentication processor 124 at block 740, permitting the authentication processor 124 to use the one-time password to validate the authorization request at block 744.

[0053] Subsequent processing of the transaction is similar to conventional processing, irrespective of whether the authorization request is received from a point-of-sale device 106 or from a merchant web server. The authentication processor resolves the account information from the authorization request at block 748 by applying decryption techniques. If the digital signature fails to pass validation as checked at block 752, then a transaction denial code is returned by the authentication processor 124 at block 754. If the digital signature passes validation, the transaction request is forwarded to the authorization processor 132 at block 756, permitting a check to be made at block 758 whether there are sufficient funds in the identified account. If not, a transaction denial code is returned by the authorization processor 132 at block 760. If both the digital signature pass and there are sufficient funds in the account, the transaction is completed at block 762.

[0054] Fig. 8 is a flow diagram that summarizes methods of executing certain Internet-based transactions. These methods may be implemented using merchants that provide web sites that participate in the program, sometimes referred to herein as implementing “federated authentication.” When a customer enters one of these participating web sites, as indicated at block 804, he or she may enter conventional identification information to log into the web site at block 808. Such conventional identification information will frequently take the form of a userid, but may use other forms of

identification known in the art. To complete the customer's authentication, the customer enters the PIN for the presentation instrument on the mobile electronic device at block 812, with the device responding to correct entry of the PIN by displaying a one-time password at block 816. As in other embodiments of the invention, the one-time password sometimes
5 comprises a two-factor one-time password. This password is used by the customer to complete the log in to the participating web site at block 820, permitting the customer to enter into and complete a transaction at block 824.

[0055] In some embodiments, the security information that is used in the methods described in connection with either Fig. 7 or Fig. 8 may vary over time. That is, when a two-
10 factor one-time password is generated, it may have a limited time of validity. In such embodiments, the customer 104 must generally provide the password within the limited time to validate the transaction. After the time period has expired, a new one-time password is generated that must be received in order to validate the transaction within a separate time period. Such a feature further enhances the overall security of the transaction methods.

15
[0056] Thus, having described several embodiments, it will be recognized by those of skill in the art that various modifications, alternative constructions, and equivalents may be used without departing from the spirit of the invention. Accordingly, the above description should not be taken as limiting the scope of the invention, which is defined in the following
20 claims.

WHAT IS CLAIMED IS:

1 1. A method of executing a financial transaction between a customer and
2 a merchant, the method comprising:
3 receiving an identifier of a financial account from the customer at a merchant
4 system;
5 receiving a one-time password from the customer at the merchant system,
6 wherein the customer is provided with the one-time password by a mobile electronic device
7 or by a contactless presentation instrument;
8 generating a cryptogram comprising the identifier of the financial account
9 encrypted using the one-time password;
10 formulating an authorization request at the merchant system, the authorization
11 request comprising the cryptogram and transaction information describing at least a portion
12 of the financial transaction; and
13 transmitting the authorization request from the merchant system to an
14 authorization processor for authorization of the financial transaction.

1 2. The method recited in claim 1 wherein the identifier comprises an
2 account number of the financial account.

1 3. The method recited in claim 1 wherein the identifier comprises an
2 identification number extracted from a presentation instrument, the method further
3 comprising translating the identification number to an account number of the financial
4 account.

1 4. The method recited in claim 1 wherein the one-time password
2 comprises a two-factor one-time password.

1 5. The method recited in claim 1 wherein the one-time password is a
2 second one-time password provided to the customer by the mobile electronic device or
3 contactless presentation instrument after passage of an expiry time after a first one-time
4 password is provided to the customer by the mobile electronic device or contactless
5 presentation instrument.

1 6. The method recited in claim 1 wherein the merchant system comprises
2 an Internet web server.

1 7. The method recited in claim 1 wherein the merchant system comprises
2 a merchant point-of-sale device.

1 8. The method recited in claim 1 further comprising receiving a personal
2 identification number from the customer at the merchant system, wherein the authorization
3 request further comprises the personal identification number.

1 9. The method recited in claim 1 wherein the mobile electronic device or
2 contactless presentation instrument comprises a cellular telephone.

1 10. The method recited in claim 1 wherein the transaction information
2 comprises data selected from the group consisting of a total cost for the financial transaction,
3 a location, a point-of-sale-device identifier, a point-of-sale-device sequence number, a date,
4 and a time.

1 11. The method recited in claim 1 wherein the financial account comprises
2 an account selected from the group consisting of a debit account, a credit account, and a
3 stored-value account.

1 12. A method of executing a financial transaction between a customer and
2 a merchant, the method comprising:

3 receiving an encrypted authorization request from a merchant system at an
4 authorization processor, wherein the authorization request was encrypted by application of a
5 one-time password provided to the merchant by a presentation instrument;

6 decrypting the authorization request;

7 identifying a financial account from the decrypted authorization request;

8 determining transaction information describing at least a portion of the
9 financial transaction from the decrypted authorization request;

10 determining authenticity of the transaction information by validating the one-
11 time password; and

12 determining whether the identified financial account is capable of supporting
13 the financial transaction based on the transaction information.

1 13. The method recited in claim 12 further comprising delivering a loyalty
2 customer identification number from the presentation instrument to the merchant.

1 14. The method recited in claim 12 wherein the identifier comprises an
2 account number of the financial account.

1 15. The method recited in claim 12 wherein the one-time password
2 comprises a two-factor one-time password.

1 16. The method recited in claim 12 wherein the merchant system
2 comprises an Internet web server.

1 17. The method recited in claim 12 wherein the merchant system
2 comprises a merchant point-of-sale device.

1 18. The method recited in claim 12 further comprising verifying
2 authenticity of the one-time password by validating the personal identification number
3 associated with the identified financial account.

1 19. The method recited in claim 12 wherein the debit presentation
2 instrument comprises a cellular telephone.

1 20. The method recited in claim 12 wherein the transaction information
2 comprises data selected from the group consisting of a total cost for the financial transaction,
3 a location, a point-of-sale-device identifier, a point-of-sale-device sequence number, a date,
4 and a time.

1 21. The method recited in claim 12 wherein the financial account
2 comprises an account selected from the group consisting of a debit account, a credit account,
3 and a stored-value account.

1 22. A computer-readable storage medium having a computer-readable
2 program embodied therein for directing operation of a merchant system, mobile electronic
3 device, or a contactless presentation instrument to execute a financial transaction between a
4 customer and a merchant, the merchant system, mobile electronic device, or contactless
5 presentation instrument including a communications system, a processor, and a storage
6 device, wherein the computer-readable program includes:

7 instructions for receiving an identifier of a financial account from the
8 customer at the merchant system;

9 instructions for receiving a one-time password from the customer at the
10 merchant system, wherein the customer is provided with the one-time password by a mobile
11 electronic device or contactless presentation instrument;

12 instructions for generating a cryptogram comprising the identifier of the
13 financial account encrypted using the one-time password;

14 instructions for formulating an authorization request at the merchant system,
15 the authorization request comprising the cryptogram and transaction information describing
16 at least a portion of the financial transaction; and

17 instructions for transmitting the authorization request from the merchant
18 system to an authorization processor for authorization of the financial transaction.

1 23. The system recited in claim 22 wherein the identifier comprises an
2 account number of the financial account.

1 24. The system recited in claim 22 wherein;
2 the identifier comprises an identification number extracted from a presentation
3 instrument; and
4 the computer-readable program further includes instructions for translating the
5 identification number to an account number of the financial account.

1 25. The system recited in claim 22 wherein the one-time password
2 comprises a two-factor one-time password.

1 26. The system recited in claim 22 wherein the one-time password is a
2 second one-time password provided to the customer by the mobile electronic device or
3 contactless presentation instrument after passage of an expiry time after a first one-time
4 password is provided to the customer by the mobile electronic device or contactless
5 presentation instrument.

1 27. The system recited in claim 22 wherein the merchant system comprises
2 an Internet web server.

1 28. The system recited in claim 22 wherein the merchant system comprises
2 a merchant point-of-sale device.

1 29. The system recited in claim 22 wherein:

2 the computer-readable program further includes instructions for receiving a
3 personal identification number from the customer at the merchant system; and
4 the authorization request further comprises the personal identification number.

1 30. The system recited in claim 22 wherein the mobile electronic device or
2 contactless presentation instrument comprises a cellular telephone.

1 31. The system recited in claim 22 wherein the transaction information
2 comprises data selected from the group consisting of a total cost for the financial transaction,
3 a location, a point-of-sale-device identifier, a point-of-sale-device sequence number, a date,
4 and a time.

1 32. The system recited in claim 22 wherein cryptographic keys used to
2 generate the one-time password on the presentation instrument are generated on the
3 presentation instrument and transmitted to an authentication processor or are generated on the
4 authentication processor and transmitted to the presentation instrument.

1 33. The system recited in claim 22 wherein the debit presentation
2 instrument does not divulge the one-time password until the merchant system has been
3 validated using a mutual authentication scheme.

1 34. The system recited in claim 22 wherein the financial account
2 comprises an account selected from the group consisting of a debit account, a credit account,
3 and a stored-value account.

1 35. A computer-readable storage medium having a computer-readable
2 program embodied therein for directing operation of an authorization processor to execute a
3 financial transaction between a customer and a merchant, the authorization processor
4 including a communications system, a processor, and a storage device, wherein the computer-
5 readable program includes:

6 instructions for receiving an encrypted authorization request from a merchant
7 system at the authorization processor, wherein the authorization request was encrypted by
8 application of a one-time password provided to the customer by a presentation instrument;

9 instructions for decrypting the authorization request;

10 instructions for identifying a financial account from the decrypted
11 authorization request;

12 instructions for determining transaction information describing at least a
13 portion of the financial transaction from the decrypted authorization request;
14 instructions for determining authenticity of the transaction information by
15 validating the one-time password; and
16 instructions for determining whether the identified financial account is capable
17 of supporting the financial transaction based on the transaction information.

1 36. The system recited in claim 35 wherein the computer-readable
2 program further includes instructions for delivering a loyalty customer identification number
3 from the presentation instrument to the merchant.

1 37. The system recited in claim 35 wherein the identifier comprises an
2 account number of the financial account.

1 38. The system recited in claim 35 wherein the one-time password
2 comprises a two-factor one-time password.

1 39. The system recited in claim 35 wherein the merchant system comprises
2 an Internet web server.

1 40. The system recited in claim 35 wherein the merchant system comprises
2 a merchant point-of-sale device.

1 41. The system recited in claim 35 wherein the computer-readable
2 program further includes instructions for verifying authenticity of the one-time password by
3 validating the personal identification number associated with the identified financial account.

1 42. The system recited in claim 35 wherein the debit presentation
2 instrument comprises a cellular telephone.

1 43. The system recited in claim 35 wherein the transaction information
2 comprises data selected from the group consisting of a total cost for the financial transaction,
3 a location, a point-of-sale-device identifier, a point-of-sale-device sequence number, a date,
4 and a time.

1 44. The system recited in claim 35 wherein cryptographic keys used to
2 generate the one-time password on the presentation instrument are generated on the

3 presentation instrument and transmitted to an authentication processor or are generated on the
4 authentication processor and transmitted to the presentation instrument.

1 45. The system recited in claim 35 wherein the financial account
2 comprises an account selected from the group consisting of a debit account, a credit account,
3 and a stored-value account.

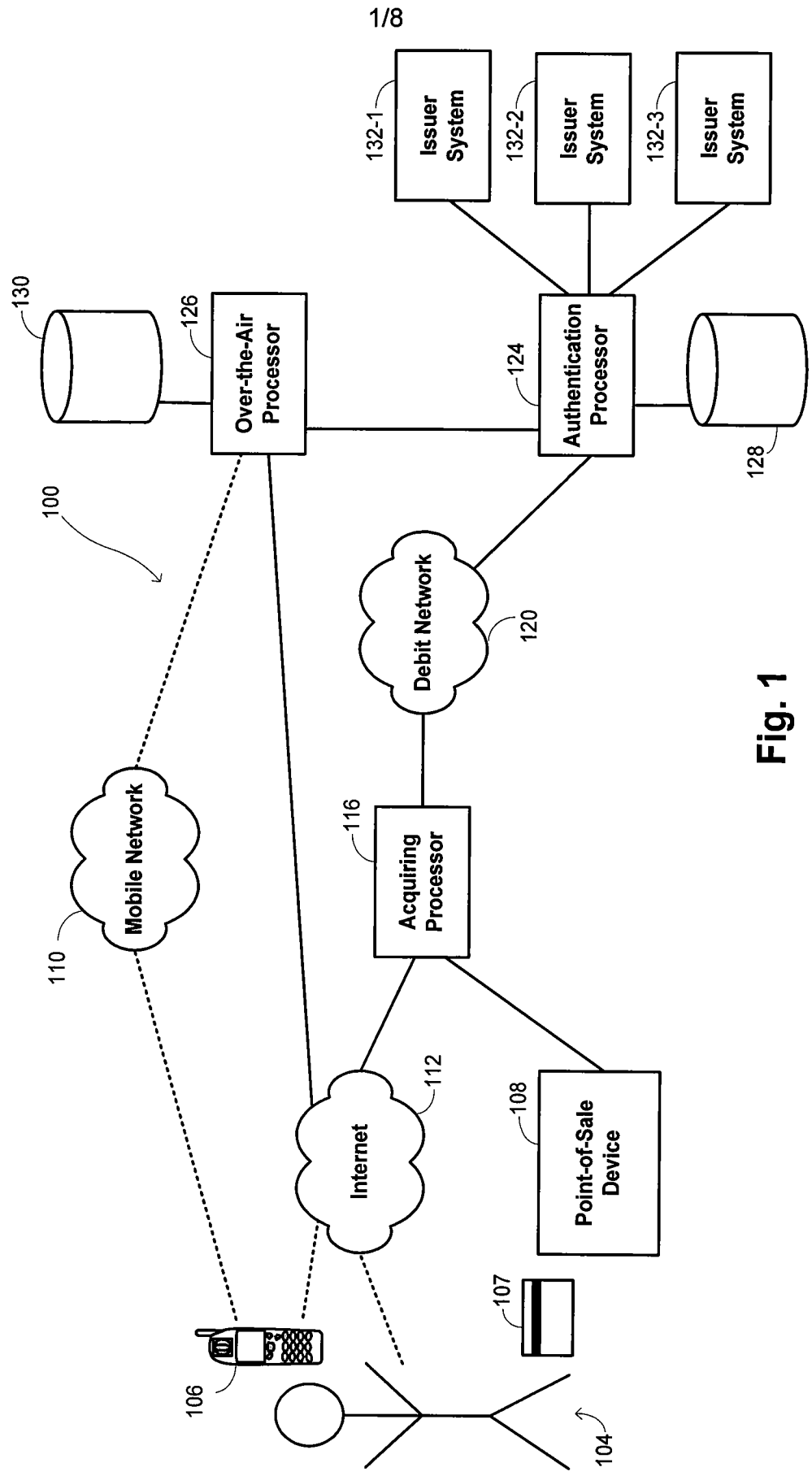
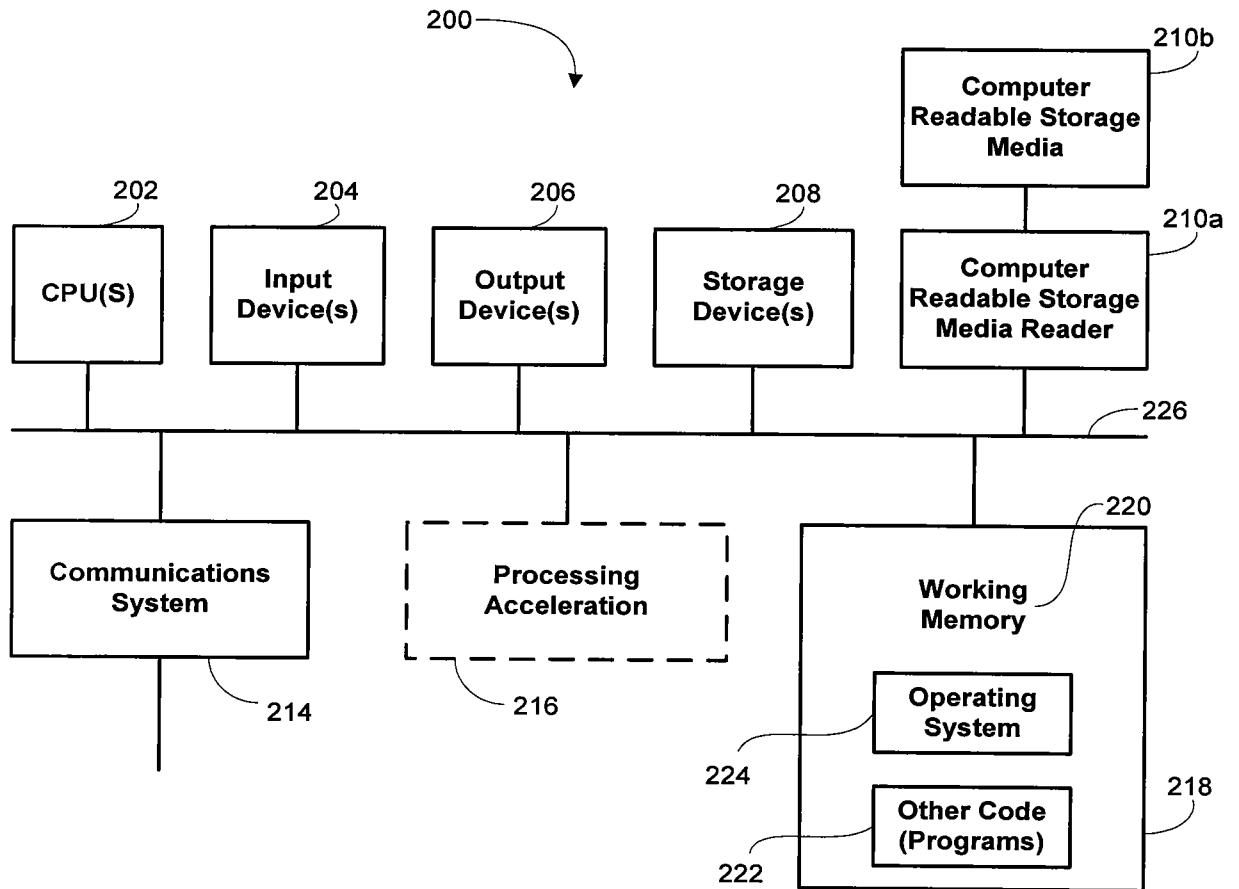


Fig. 1

2/8

**Fig. 2**

3/8

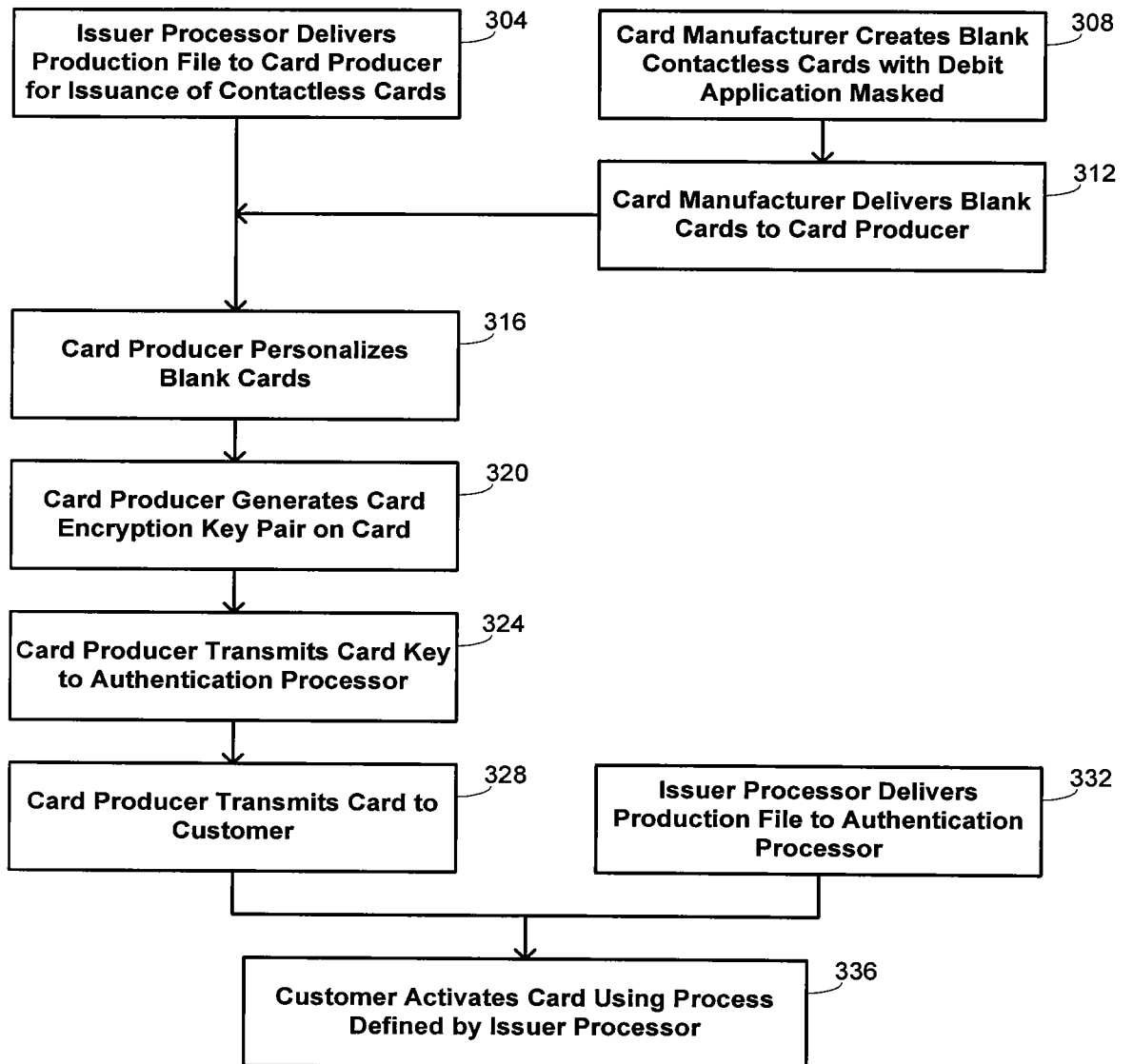
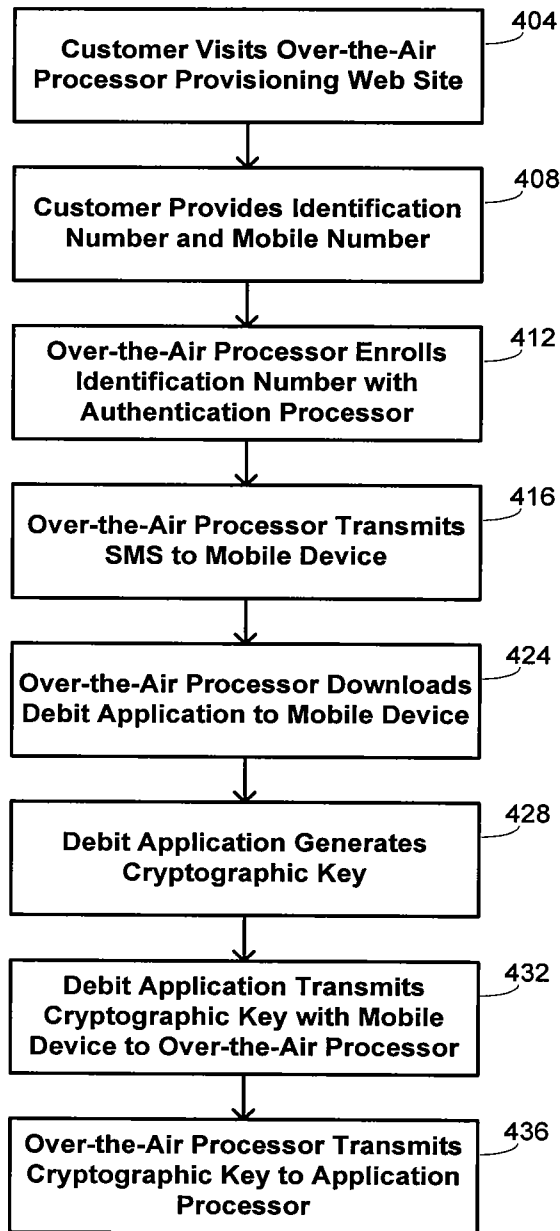
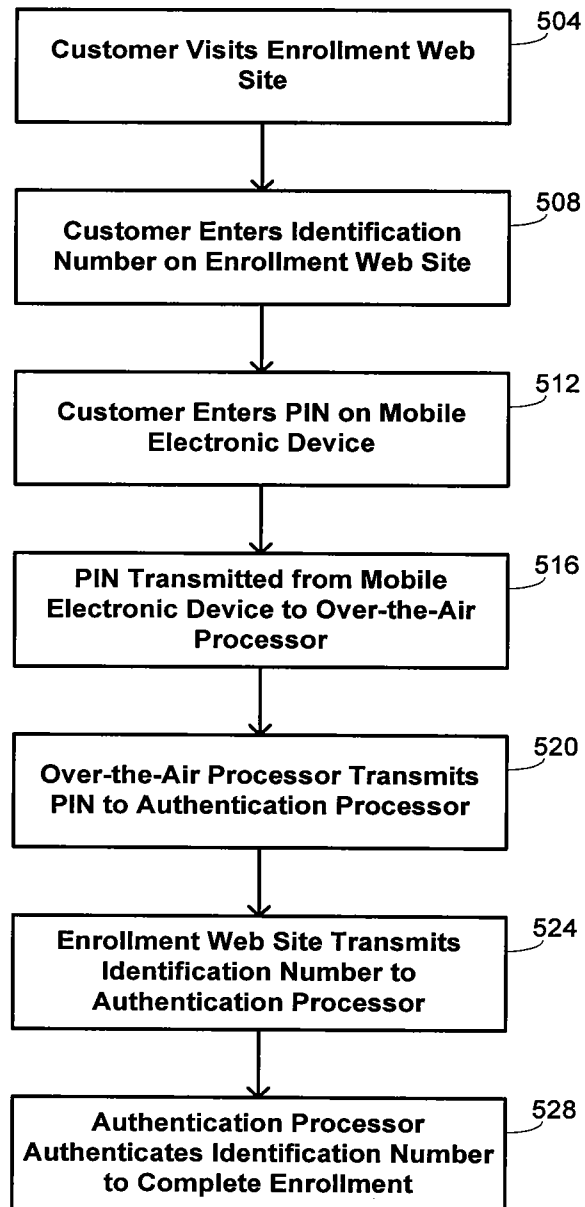


Fig. 3

4/8

**Fig. 4**

5/8

**Fig. 5**

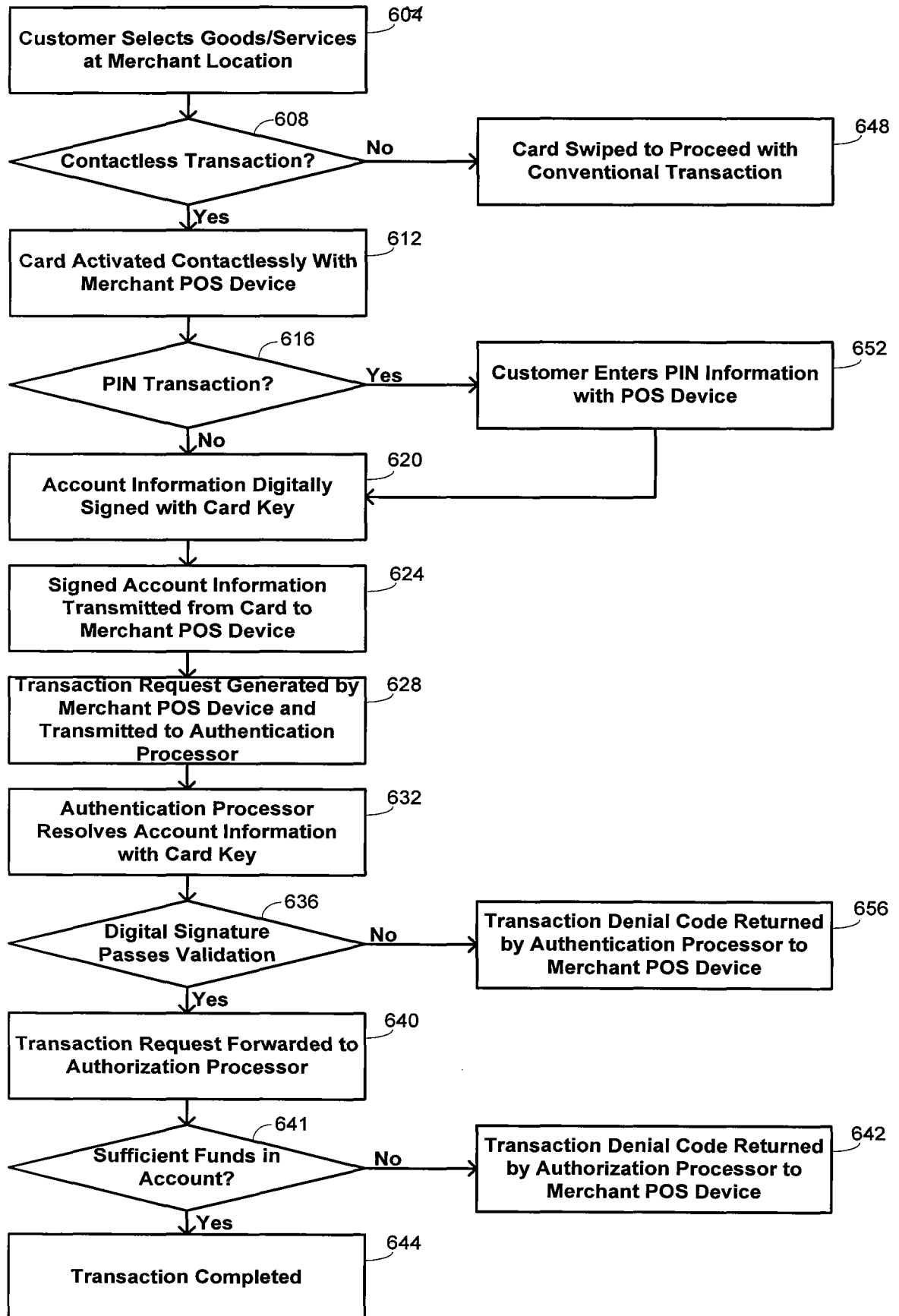


Fig. 6

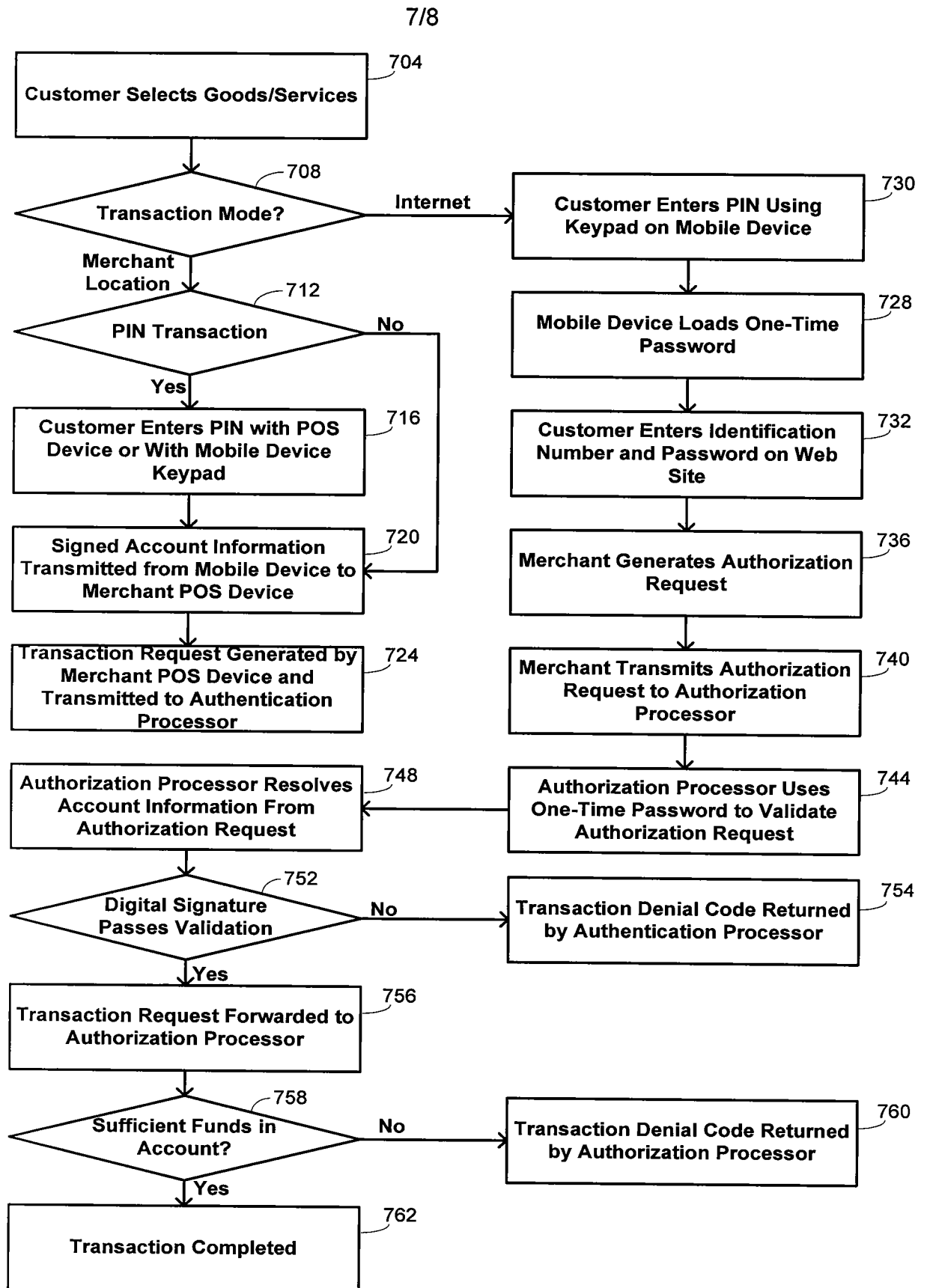
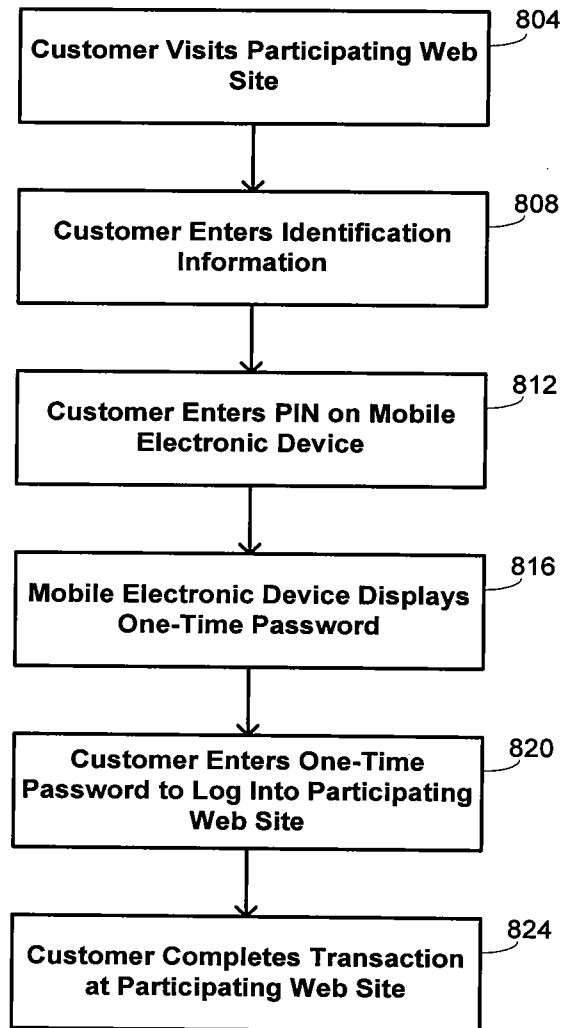


Fig. 7

8/8

**Fig. 8**

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US 08/54683

A. CLASSIFICATION OF SUBJECT MATTER

IPC(8) - H04L 9/00, G06Q 30/00 (2008.04)

USPC - 705/67

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)

USPC - 705/67

IPC(8) - H04L 9/00, G06Q 30/00 (2008.04)

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

USPC - 705/50, 64, 72, 75, 76; 700/1, 90

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

PubWEST (USPT, PGPB, EPAB, JPAB); DIALOG PRO (Engineering) & Google; financial transaction, customer, merchant, identifier, financial account, merchant system, one-time password, mobile electronic device, contactless presentation instrument, cryptogram, authorization request, transaction information, portion, authorization...

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2004/0064351 A1 (Mikurak) 01 April 2004 (01.04.2004), entire document, especially Fig 12, 15; para [0005], [0025], [0226], [0249], [0259], [0289], [0293], [0330], [0374], [0406], [0468], [0484], [0492], [0505], [0521], [0530], [0581], [0750], [0754], [0793], [0876], [0880], [0922], [0961], [0986], [0989], [1011], [1024]-[1025], [1041], [1105], [1130], [1170], [1273], [1305], [1313], [1344], [1351], [1421], [1468]-[1469], [1576], [1644], [1709], [1818], [1825], [2075], [2085], [2088], [2097], [2099], [2124], [2126], [2140], [2162]-[2163], [2192], [2196], [2198], [2215], [2219]-[2220], [2225], [2533], [2535], [2545], [2549]-[2550], [2610], [2614], [2770]-[2771], [2823], [2991], [2995], [3033], [3210], [3214], [3225], [3232] and [3236].	1-45
Y	US 2007/0037552 A1 (Lee et al). 15 February 2007 (15.02.2007), entire document, especially Abstract, Fig 3 and para [0008] and [0219].	1-45

☐ Further documents are listed in the continuation of Box C.

* 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

26 May 2008 (26.05.2008)

Date of mailing of the international search report

27 JUN 2008

Name and mailing address of the ISA/US

Mail Stop PCT, Attn: ISA/US, Commissioner for Patents

P.O. Box 1450, Alexandria, Virginia 22313-1450

Facsimile No. 571-273-3201

Authorized officer:

Lee W. Young

PCT Helpdesk: 571-272-4300

PCT OSP: 571-272-7774