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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
15 June 2017 (15.06.2017)

WIPO | PCT

(10) International Publication Number
WO 2017/100144 A1

(51) International Patent Classification:
G06Q 20/40 (2012.01) *G06Q 20/38* (2012.01)
G06Q 20/34 (2012.01)

(21) International Application Number:
PCT/US2016/065045

(22) International Filing Date:
6 December 2016 (06.12.2016)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
62/265,020 9 December 2015 (09.12.2015) US
15/007,837 27 January 2016 (27.01.2016) US

(71) Applicant: **MASTERCARD INTERNATIONAL INCORPORATED** [US/US]; 2000 Purchase Street, Purchase, NY 10577 (US).

(72) Inventors: **WARNER, Maribeth Sevigny**; 2000 Purchase Street, Purchase, NY 10577 (US). **KAULBACH, Pete**; 52 Kingsbury Way, Bedford, Nova Scotia, B4A 4M5 (CA). **DUNNELL, Robert C.**; 4259 Humphrey Street, Saint Louis, MO 63116 (US). **MCDONALD, Robert J.**; 2706 Cascade Lake Drive, Belleville, IL 62221 (US). **DONNELLY, Kathleen**; 91 Wyndview Court, Lake St. Louis, MO 63367 (US). **ROEWE, Thomas**; 3 Sundew Court, Belleville, IL 62221 (US). **JABR, Ghassan T.**; 3122 Bear View Court, Wentzville, MO 63385 (US). **HOCHHALTER, Michael**; 25 Auvergne Drive, Lake St. Louis, MO 63367 (US). **BALL, Russell W.**; 3976 Lockport Drive, Bridgeton, MO 63044 (US). **HOUSE, Winifred Elizabeth**; 26 Hampton Drive, Troy, MO 63379 (US). **RAO, Prasad Krishnamoorthy**; 105 Josephine Avenue, West Conshohocken, PA 19428 (US). **HANMER, Matthew**; 45 Park Avenue North Abington, Northampton, Northamptonshire NN3 2HT (GB). **KRYZA, Nora**; 12008 Jeffers Lane, Fenton, MI 48430 (US).

(74) Agent: **DOBBYN, Colm J**; Mastercard International Incorporated, 2000 Purchase Street, Purchase, NY 10577 (US).

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

[Continued on next page]

(54) Title: DYNAMIC SECURITY CODE AUTHORIZATION VERIFICATION SERVICE

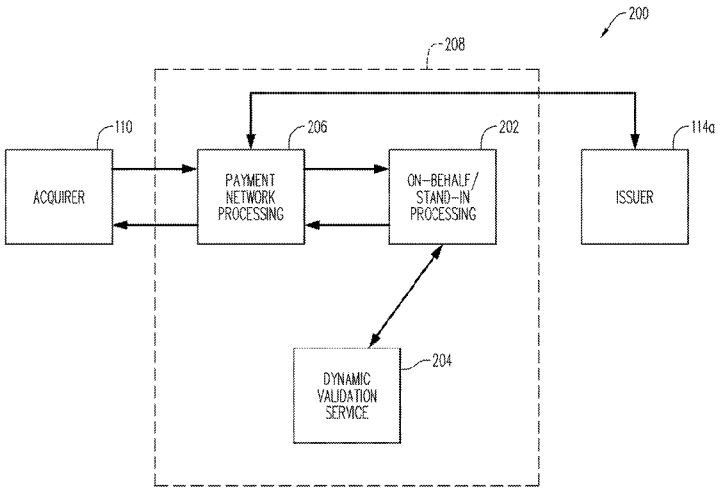


FIG. 2

(57) Abstract: A method includes receiving a request to verify a dynamic security code included in a transaction authorization request message. The transaction authorization request message was generated in connection with a payment account transaction. The method further includes performing a verification process with respect to the dynamic security code to generate a verification result. In addition, the transaction authorization request message may be modified by adding the verification result to the transaction authorization request message. Also, the modified transaction authorization request message may be transmitted to an issuer of a payment account designated for use in the payment account transaction.

WO 2017/100144 A1

TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

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

Published:

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

DYNAMIC SECURITY CODE AUTHORIZATION VERIFICATION SERVICE

CROSS-REFERENCE TO RELATED APPLICATIONS

This application claims priority to and the benefit of the filing date of U.S. Patent Application Serial Nos. 62/265,020, filed December 9, 2015 and 15/007,837, filed January 27, 2016, which are hereby incorporated by reference in their entireties.

BACKGROUND

Payment accounts are in widespread use for both in-store and online purchase transactions. FIG. 1 is a block diagram of a conventional payment system 100 as it may operate in connection with an online purchase transaction.

The system 100 includes an e-commerce server computer 102 that may be operated by or on behalf of an online merchant to permit online shopping transactions. For this purpose, as is well known, the e-commerce server computer 102 may host a shopping website, sometimes referred to as an "online store". A customer 103 who operates a customer device 104 may access the shopping website by communicating over the Internet 105 with the e-commerce server computer 102. As is very well-known to those who are skilled in the art, the customer device 104 may be, for example, a personal computer or notebook computer that runs a browser program, a tablet computer or smartphone that runs a mobile browser and/or a suitable app, etc. In entering payment information into a page served by the e-commerce server computer 102 to the customer device 104, the customer 103 may refer to a payment card 106 issued to the customer 103 in connection with the payment account to be used for the current online purchase transaction.

In connection with the online purchase transaction, the e-commerce server computer 102 may transmit a transaction authorization request message (sometimes simply referred to as an "authorization request") to the merchant's acquirer financial institution ("acquirer" or "transaction acquirer"), indicated by reference numeral 110. The acquirer 110 may route the authorization request via a payment network 112 to a server computer 114 operated by the issuer of the payment account that corresponds to the payment card 106 and the payment account number

provided by the customer as part of the checkout process for the online purchase transaction. Also, the authorization response generated by the issuer server computer 114 may be routed back to the acquirer 110 via the payment network 112. The acquirer 110 may confirm to the merchant (i.e., to the e-commerce server computer 102) that the transaction has been approved.

As is familiar to those who engage in online purchase transactions, during the checkout phase of the transaction the customer may enter payment related information such as the customer's name as it appears on the payment account, the PAN (primary account number) that identifies the payment account, and the current expiration date for the account. In addition, the customer may—in many cases—be prompted to enter a three or four digit security code that typically is printed on the rear face (on the signature slip) of the payment card. Common names for such a code include "CVC" (card verification code) and "CVV" (card verification value). All of these items of information may be included in the authorization request.

Referring again to FIG. 1, the payment network 112 may be, for example, the well-known Banknet® system operated by MasterCard International Incorporated, which is the assignee hereof.

The components of the system 100 as depicted in FIG. 1 are only those that are needed for processing a single transaction. Those who are skilled in the art will recognize that in the real world, online shopping and payment systems may process many purchase transactions (including simultaneous transactions) and may include a considerable number of payment account issuers and their computers, a considerable number of acquirers and their computers, and numerous merchants and their e-commerce servers. The system may also include a very large number of customers/online shoppers, who hold payment accounts that they use for their online shopping activities. It is also well known that elements of the system 100 (e.g., acquirers, the payment network, payment account issuers) may play similar roles in connection with in-store purchase transactions and in other types of transactions.

Resuming the above discussion of the security code printed on the card, it has been proposed, for purposes of deterring and/or preventing fraudulent transactions, to enhance the security code feature. For example, in U.S. Patent No. 8,919,643 and U.S. Patent publication no. 2012/0153028, it has been proposed that processing capability on the payment card (i.e., where the payment card is embodied as an IC card) be utilized to dynamically vary the security code, and to display the

current value of the dynamic security code on a display element included in the payment card. However, verification of dynamic security codes may place a significant burden on the card/account issuer, thereby making it unattractive or uneconomic to incorporate dynamic security codes in an issuer's payment account practices.

BRIEF DESCRIPTION OF THE DRAWINGS

Features and advantages of some embodiments of the present disclosure, and the manner in which the same are accomplished, will become more readily apparent upon consideration of the following detailed description of the disclosure taken in conjunction with the accompanying drawings, which illustrate preferred and exemplary embodiments and which are not necessarily drawn to scale, wherein:

FIG. 1 is a block diagram that illustrates a conventional system that handles online purchase transactions.

FIG. 2 is a block diagram of salient portions of a payment system according to some embodiments.

FIGS. 3 and 4 are block diagram representations of computers that may serve as components of the system shown in FIG. 2.

FIG. 5 is a flow chart that illustrates aspects of the present disclosure.

DETAILED DESCRIPTION

In general, and for the purpose of introducing concepts of embodiments of the present disclosure, a service may be provided to detect authorization requests that contain dynamic security codes. The service also incorporates verification of the dynamic security code included in the authorization request, and adding to the authorization request an indication of the result of the verification process. The authorization request, including the dynamic security code verification result, may then be routed to the account issuer for approval (if appropriate) of the authorization request.

FIG. 2 is a block diagram of salient portions of a payment system 200 provided according to some embodiments. The representation of the payment system 200 as shown in FIG. 2 assumes in addition that other aspects of the payment system (that were seen in FIG. 1) are also present but not shown in FIG. 2. For example, the

representation in FIG. 2 assumes that a merchant e-commerce server 102 (FIG. 1) has generated and sent to the transaction acquirer 110 (FIG. 2 and FIG. 1) an authorization request that corresponds to an online purchase transaction performed via the e-commerce website hosted by the e-commerce server. It will further be appreciated that, in such a circumstance, a customer 103 (FIG. 1) performed the online purchase transaction using a customer device 104 (FIG. 1) that accessed the e-commerce server and the merchant's website via the internet 105 (FIG. 1). It will further be assumed, for present purposes, that the customer visually referred to a payment card 106 (FIG. 1); a further assumption is that the payment card was of a commercially available type that is an IC (integrated circuit) card that generates and displays a time-varying dynamic security code. A further assumption is that the currently displayed value of the dynamic security code was read by the customer, entered by the customer as part of the payment information solicited by the e-commerce website, and included in the authorization request message generated by the e-commerce server and transmitted to the acquirer 110. A further assumption may be that the authorization request message is in a standard format for such messages and includes a PAN (primary account number) that identifies the payment account designated by the customer for use in the current purchase transaction.

In addition to the acquirer 110, the payment system 200 as shown in FIG. 2 includes a proxy computer 202 that performs on-behalf and/or stand-in processes—i.e., functions that might otherwise need to be performed by the account issuers. The payment system 200 further includes a dynamic validation service module 204 and a payment network processing computer 206. Dotted line box 208, which encompasses the proxy computer 202, the dynamic validation service module 204 and the payment network processing computer 206, is intended to imply that all three of the latter system components may be operated by the operator of a payment network, the main functions of which may be implemented by the payment network processing computer 206. Thus the payment network processing computer 206 may be seen as a modified analog of the payment network 112 referred to above in connection with FIG. 1.

Further details of the functionality provided by the proxy computer 202, the dynamic validation service module 204 and the payment network processing computer 206 will be described below. In terms of a brief overview, the payment network processing computer 206 may receive authorization requests from acquirers

(such as the acquirer 110 shown in FIG. 2). The payment network processing computer 206 may forward the authorization requests to the proxy computer 202, which may detect authorization requests that contain dynamic security codes, and forward those codes for validation by the dynamic validation service module 204. The dynamic validation service module 204 may perform a verification process with respect to the dynamic security codes and provide the results of the verification process to the proxy computer 202. The proxy computer 202 may append the verification process results to the authorization requests and transmit them to the payment network processing computer 206, which may route the authorization requests to account issuers, such as the issuer 114a shown in FIG. 2 (block 114a should also be understood to represent a computer operated by or for the issuer). Authorization responses from the issuers may be routed back to the acquirers via the payment network processing computer 206.

As was the case in the payment system depiction of FIG. 1, the system components shown in FIG. 2 are only those that may be required to handle a single transaction. For example, there may be a considerable number of transaction acquirers and account issuers in a practical embodiment of the payment system 200. The payment system 200, in a practical embodiment, may handle numerous transactions, including simultaneous transactions. Moreover, one or more components of the payment system 200 may handle in-store purchase transactions and/or other types of transactions in addition to online purchase transactions.

In some embodiments, any two or more of the proxy computer 202, the dynamic validation service module 204, and/or the payment network processing computer 206 may be constituted by components of an interrelated and/or integrated computer system and/or may be housed together in a single data center.

FIG. 3 is a block diagram representation of an embodiment of the dynamic validation service module 204.

In some embodiments, the dynamic validation service module 204 may be implemented using a software and/or hardware module solution that is commercially available from a supplier of the above-mentioned IC payment cards with dynamic security code features. In some embodiments, the dynamic validation service module 204 may be embodied in a hardware security module (HSM). In some embodiments the dynamic validation service module 204 may be constituted at least in part by typical server computer hardware, but may be controlled by software to

cause it to function as described herein. Suitable security measures may be applied to the dynamic validation service module 204.

The dynamic validation service module 204 may include a processor 300 operatively coupled to a communication device 301, a storage device 304, an input device 306 and an output device 308. The communication device 301, the storage device 304, the input device 306 and the output device 308 may all be in communication with the processor 300.

The processor 300 may be constituted by one or more processors. The processor 300 may operate to execute processor-executable steps, contained in program instructions described below, so as to control the dynamic validation service module 204 to provide desired functionality.

Communication device 301 may be used to facilitate communication with, for example, other devices (such as the proxy computer 202 and the payment network processing computer 206). For example, communication device 301 may comprise numerous communication ports (not separately shown), to allow the dynamic validation service module 204 to receive and process numerous simultaneous dynamic security code validation requests.

Input device 306 may comprise one or more of any type of peripheral device typically used to input data into a computer. For example, the input device 306 may include a keyboard and a mouse. Output device 308 may comprise, for example, a display and/or a printer. (In some embodiments, input/output functions relative to the dynamic validation service module 204 may be handled via an associated computer such as the proxy computer 202.)

Storage device 304 may comprise any appropriate information storage device, including combinations of magnetic storage devices (e.g., hard disk drives), optical storage devices such as CDs and/or DVDs, and/or semiconductor memory devices such as Random Access Memory (RAM) devices and Read Only Memory (ROM) devices, as well as so-called flash memory. Any one or more of such information storage devices may be considered to be a computer-readable storage medium or a computer usable medium or a memory.

Storage device 304 stores one or more programs for controlling processor 300. The programs comprise program instructions (which may be referred to as computer readable program code means) that contain processor-executable process steps of the dynamic validation service module 204, executed by the

processor 300 to cause the dynamic validation service module 204 to function as described herein.

The programs may include one or more conventional operating systems (not shown) or kernels that control the processor 300 so as to manage and coordinate activities and sharing of resources in the dynamic validation service module 204, and to serve as a host for application programs (described below) that run on the dynamic validation service module 204.

The programs stored in the storage device 304 may also include a validation request handling program 310 that controls the processor 300 to enable the dynamic validation service module 204 to handle and process dynamic security code validation requests.

The storage device 304 may also store, and the dynamic validation service module 204 may also execute, other programs, which are not shown. For example, such programs may include a reporting application, which may respond to requests from system administrators for reports on the activities performed by the dynamic validation service module 204. The other programs may also include, e.g., device drivers, database management programs, etc.

The storage device 304 may also store an account database 312 that is referenced by the validation request handling program 310 in connection with performing a verification process with respect to dynamic security codes received by the dynamic validation service module 204 from the proxy computer 202.

FIG. 4 is a block diagram of an embodiment of the proxy computer 202.

In its hardware architecture and components, the proxy computer 202 may, for example, resemble the hardware architecture and components described above in connection with FIG. 3. However, the proxy computer 202 may be programmed differently from the dynamic validation service module 204 so as to provide different functionality.

Returning again to the hardware aspects of the proxy computer 202, it may include a processor 400, a communication device 401, a storage device 404, an input device 406 and an output device 408. The communication device 401, the storage device 404, the input device 406 and the output device 408 may all be in communication with the processor 400.

The above descriptions of the hardware components shown in FIG. 3 may, in some embodiments, also be applicable to the like-named components shown in FIG. 4.

Storage device 404 stores one or more programs for controlling processor 400. The programs comprise program instructions (which may be referred to as computer readable program code means) that contain processor-executable process steps of the proxy computer 202, executed by the processor 400 to cause the proxy computer 202 to function as described herein.

The programs may include one or more conventional operating systems (not shown) that control the processor 400 so as to manage and coordinate activities and sharing of resources in the proxy computer 202, and to serve as a host for application programs (described below) that run on the proxy computer 202.

The storage device 404 may store a transaction handling program 410 that handles receipt, processing and transmission of messages related to payment account transactions. The transaction handling program 410 may implement functionality of the proxy computer 202 as described herein and in accordance with some embodiments.

The storage device 404 may also store software 412 that serves as an interface between the proxy computer 202 and the dynamic validation service module 204.

The storage device 404 may also store, and the proxy computer 202 may also execute, other programs, which are not shown. For example, such programs may include a reporting application, which may respond to requests from system administrators for reports on the activities performed by the proxy computer 202. The other programs may also include, e.g., device drivers, database management programs, etc.

The storage device 404 may also store one or more databases (reference numeral 414) required for operation of the proxy computer 202.

The payment network processing computer 206 may have the same type of hardware architecture and/or components as the computing device described above in connection with FIG. 3. In addition, the payment network processing computer 206 may be programmed to perform conventional functions of a payment network as well as additional functions in accordance with aspects of the present disclosure and as described herein.

The issuer computer 114a may also have the same type of hardware architecture and/or components as described above in connection with FIG. 3, and may be programmed to provide functionality as described herein.

FIG. 5 is a flow chart that illustrates aspects of the present disclosure, including operations performed individually and/or cooperatively by the proxy computer 202, dynamic validation service module 204 and the payment network processing computer 206.

As indicated at 502 in FIG. 5, the payment network processing computer 206 may receive an authorization request message from an acquirer 110, and may forward the authorization request message to the proxy computer 202.

The processing by the proxy computer 202 may include a decision block 504. At the decision block 504, the proxy computer 202 may determine whether the authorization request received at 502 contains a dynamic security code. In some embodiments, for example, the proxy computer 202 may make this determination based on the PAN included in the authorization request. (It will be recalled that the PAN identifies the payment account designated by the customer for use in the transaction represented by the authorization request.) In particular, the proxy computer 202 may determine whether the PAN falls within one or more ranges of account numbers that have been indicated by the respective account issuers as being associated with payment accounts for which dynamic security code features were implemented (i.e., accounts for which the issued payment cards embody a dynamic security code feature). The determination may be made, for example, with reference to one or more of the databases 414 depicted in FIG. 4. If a negative determination is made at 504 (i.e., if it is determined that the authorization request does not include a dynamic security code), then block 506 may follow decision block 504 in the process of FIG. 5. Block 506 represents handling and processing the authorization request on the assumption that it contains a static rather than dynamic security code. This may result in the authorization request being handled and processed in a conventional manner.

Considering decision block 504 again, if a positive determination is made at that decision block (i.e., if the authorization request is determined to include a dynamic security code), then the process of FIG. 5 may advance from decision block 504 to block 508.

At block 508, the proxy computer 202 many generate and transmit a request for verification of the dynamic security code. The request may be transmitted from the proxy computer 202 to the dynamic validation service module 204 and may be received by the dynamic validation service module 204. The request may include, for example, the dynamic security code value to be verified and the PAN that was included in the authorization request received at 502.

Following block 508 is block 510. Block 510 includes a dynamic security code verification process, which may be performed by the dynamic validation service module 204. In some embodiments, the verification process may involve duplicating the process performed in the payment card to generate the dynamic security code and comparing the result of the code generation process performed by the dynamic validation service module 204 with the received dynamic security code value to confirm that the two match. The verification process may be a cryptographic process and may involve use of one or more cryptographic keys. In some embodiments, the required inputs to the code generation process performed by the dynamic validation service module 204 may be available in the account database 312 depicted in FIG. 3, and may be indexed by the PAN for the relevant payment account. The required inputs may include one or more cryptographic keys that may be stored in the entry for the relevant account in the account database 312. The notional match for the received dynamic security code, with the former having been generated in the dynamic validation service module 204, may be referred to as a "parallel-generated dynamic security code", given that the generation process in the dynamic validation service module 204 is parallel to the code generation process performed in the payment card.

In some embodiments, the account issuer may select the time-frame and/or circumstances under which the payment cards generate new values of the dynamic security code. For example, in some embodiments, the payment cards for a given account issuer (or class of accounts) may generate a new code value every hour, or at some other regular interval. The corresponding data entry in the account database 312 may point to data that identifies the code regeneration pattern for the payment card in question and/or may point to a suitable algorithm/process to duplicate the card-based code generation. In some embodiments, to deal with issues of time drift, latency in receiving the authorization and/or validation requests, etc., the dynamic validation service module 204 may compare current, immediately preceding,

and/or immediately succeeding parallel-generated code values with the dynamic security code as received in the verification request received at 508. It will be understood that the immediately preceding parallel-generated code value may be adjacent the current parallel-generated code value in a sequence of parallel-generated code values for the relevant payment account, and similarly the current parallel-generated code value may be adjacent the succeeding parallel-generated code value in the sequence of parallel-generated code values for the relevant payment account.

In some embodiments, the software and/or hardware required to parallel-generate the dynamic security code in the dynamic validation service module 204 may be commercially available from, and may be obtained from, the supplier of the card blanks that incorporate the dynamic security code features, and which correspond to the payment account in question or the corresponding group of payment cards.

A number of different dynamic security code generation and verification algorithms may be commercially available for use in connection with the payment system 200.

The verification process may have a number of different outcomes, such as "successful", "invalid", "timed out", or "inconclusive". The last may occur, for example, if the PAN submitted with the verification request is not found in the account database 312. The dynamic validation service module 204 may pass the result of the verification process to the proxy computer 202.

Block 512 may follow block 510 in the process of FIG. 5. The process of block 512 may be performed by the proxy computer 202. At 512, the proxy computer 202 may add the result of the verification process (or an indicator therefor, which may also be considered the result) to the authorization request for the transaction for which dynamic security code verification was requested at 508. Then, at 514, the proxy computer 202 may transmit the authorization request to the payment network processing computer 206, which may route the authorization request—including the verification result—to the issuer 114a (FIG. 2). In some embodiments, the authorization request, as transmitted by the payment network processing computer 206 to the issuer, may also include a static security code that the issuer had previously assigned of record to the payment account in question. The proxy computer 202 may have inserted the static security code into the authorization request before transmitting it to the issuer. In some embodiments, the authorization request, as transmitted by the

payment network processing computer 206 to the issuer, may not include the dynamic security code value that was contained in the authorization request when it was received at 502. In some embodiments, the authorization request, as transmitted by the payment network processing computer 206 to the issuer, may include an indication that a dynamic security code verification has been performed with respect to the authorization request.

In some embodiments, the process of FIG. 5 may have a lapse of time (represented at 516) after block 514 while the issuer processes the authorization request. In some embodiments, the lapse of time may typically be rather brief. Thereafter, the payment network processing computer 206 may receive the authorization response from the issuer 114a, as indicated by block 518. Then—as indicated at block 520—the payment network processing computer 206 may route the authorization request to the acquirer 110 (FIG. 2). In some embodiments, it may be necessary or desirable for the dynamic verification results to be stripped from the authorization response before it is sent to the acquirer. If so, this may be done at the proxy computer 202 or the payment network processing computer 206.

One implication of the foregoing is that the issuer 114a may receive (from the payment network processing computer 206) an authorization request that is different from a conventional authorization request. The difference may lie in that, in accordance with the present disclosure, the authorization request may include a result of a dynamic security code verification process (the "verification result"). Accordingly, the issuer computer 114a may be programmed to consider the verification result in determining whether or not to approve the authorization request. It may well be the case that a "successful" verification result will increase the likelihood that the issuer 114a will approve the authorization request, and that an "invalid" verification result will decrease the likelihood that the issuer will approve the authorization request. For example, the issuer computer 114a may be programmed to approve high value transactions only if the verification result is "successful". In another example, the issuer computer 114a may be programmed to approve low value transactions (assuming the account is in good standing, etc.) even if the verification result is "invalid" or "inconclusive". It may be up to the issuer to decide how it will act in various kinds of situations on the basis of the various possible verification results.

In some embodiments, the proxy computer 202 may perform so-called "stand-in" services, in which the proxy computer 202 may decide to approve or decline the transaction—based on one or more rules pre-determined by the account issuer—in cases where no authorization response is received from the issuer. In some embodiments, the rule(s) may provide that the proxy computer 202 is to make the decision on the transaction based at least in part on the dynamic security code verification result generated with respect to the corresponding authorization request.

With a dynamic security code verification service as described herein, an account issuer's adoption of dynamic security code payment cards may be highly streamlined, since little change in infrastructure may be required for the issuer apart from a modest amount of programming of its computer that handles authorization requests. With this service, the issuer is immediately compatible with all online merchants and does not need to install platform-specific hardware or software. At the same time, the issuer may benefit by the improved protections against fraudulent transactions supported by use of dynamic security codes.

By the same token, merchants may not need to change their systems at all, or only to a limited extent, and may also benefit from reduced risk of fraudulent transactions. For cardholders also, little in the way of adaptation may be required, and enhanced security may be provided.

In embodiments described above, the proxy computer 202 may detect that an incoming authorization request includes a dynamic security code by comparing a PAN included in the authorization request with relevant ranges of account numbers. However, in alternative embodiments, one or more other processes may be employed to detect that the incoming authorization request includes a dynamic security code. For example, in some embodiments, the incoming authorization request may carry an indicator that shows that the security code contained within the authorization request is dynamic, and the proxy computer 202 may read the indicator.

In some embodiments, card-on-file transactions submitted by merchants may include a previously verified dynamic security code, and in such cases, and in some embodiments, the system 200 would not re-verify the dynamic security code.

As used herein and in the appended claims, the term "computer" should be understood to encompass a single computer or two or more computers in communication with each other.

As used herein and in the appended claims, the term "processor" should be understood to encompass a single processor or two or more processors in communication with each other.

As used herein and in the appended claims, the term "memory" should be understood to encompass a single memory or storage device or two or more memories or storage devices.

As used herein and in the appended claims, a "server" includes a computer device or system that responds to numerous requests for service from other devices.

The flow charts and descriptions thereof herein should not be understood to prescribe a fixed order of performing the method steps described therein. Rather the method steps may be performed in any order that is practicable, including simultaneous performance of steps.

As used herein and in the appended claims, the term "payment card system account" includes a credit card account, a deposit account that the account holder may access using a debit card, a prepaid card account, or any other type of account from which payment transactions may be consummated. The terms "payment card system account" and "payment card account" and "payment account" are used interchangeably herein. The term "payment card account number" includes a number that identifies a payment card system account or a number carried by a payment card, or a number that is used to route a transaction in a payment system that handles debit card and/or credit card transactions. The term "payment card" includes a credit card, debit card, prepaid card, or other type of payment instrument, whether an actual physical card or virtual.

As used herein and in the appended claims, the term "payment card system" refers to a system for handling purchase transactions and related transactions. An example of such a system is the one operated by MasterCard International Incorporated, the assignee of the present disclosure. In some embodiments, the term "payment card system" may be limited to systems in which member financial institutions issue payment card accounts to individuals, businesses and/or other organizations.

Although the present disclosure has been described in connection with specific exemplary embodiments, it should be understood that various changes, substitutions, and alterations apparent to those skilled in the art can be made to the disclosed embodiments without departing from the spirit and scope of the disclosure as set forth in the appended claims.

WHAT IS CLAIMED IS:

1. A method comprising:

receiving a request to verify a dynamic security code included in a transaction authorization request message, the transaction authorization request message generated in connection with a payment account transaction;

performing a verification process with respect to the dynamic security code to generate a verification result;

modifying the transaction authorization request message by adding the verification result to the transaction authorization request message; and

transmitting the modified transaction authorization request message to an issuer of a payment account designated for use in the payment account transaction.

2. The method of claim 1, wherein receiving said request to verify includes receiving said dynamic security code and a PAN (primary account number) that identifies the designated payment account.

3. The method of claim 1, wherein the transmitting modified transaction authorization request message includes transmitting a static security code associated with the designated payment account.

4. The method of claim 3, wherein the transmitted modified transaction authorization request message does not include the dynamic security code.

5. The method of claim 1, wherein the dynamic security code consists of a three or four digit number.

6. The method of claim 1, wherein the verification process includes comparing the dynamic security code with a parallel-generated current dynamic security code and a parallel-generated previous dynamic security code, said parallel-generated current dynamic security code and said parallel-generated previous dynamic security code adjacent to each other in a sequence of parallel-generated dynamic security codes parallel-generated for the designated payment account.

7. The method of claim 1, further comprising:

making a determination as to approving or declining the payment account transaction based at least in part on said verification result.

8. The method of claim 7, wherein the determination as to approving or declining is made in a case where the issuer fails to respond to the transmitting step.

9. The method of claim 8, wherein the determination is made based at least in part on at least one rule pre-defined by the issuer prior to the payment account transaction.

10. The method of claim 1, further comprising:

receiving a transaction authorization response message from the issuer in response to the transmitted modified transaction authorization request message.

11. The method of claim 10, further comprising:

transmitting the transaction authorization response message to a transaction acquirer, the transmitted transaction authorization response message not including the verification result.

12. A method comprising:

receiving a transaction authorization request message in a computer operated by an operator of a payment network;

detecting, in said computer, that the received transaction authorization request message includes a dynamic security code; and

in response to a result of the detecting step, transmitting a request to verify the dynamic security code.

13. The method of claim 12, wherein the detecting is based on an account number range that corresponds to a payment account number included in the received transaction authorization request message.

14. The method of claim 12, wherein the dynamic security code consists of a three or four digit number.

15. An apparatus comprising:

a processor; and

a memory in communication with the processor and storing program instructions, the processor operative with the program instructions to perform functions as follows:

receiving a request to verify a dynamic security code included in a transaction authorization request message, the transaction authorization request message generated in connection with a payment account transaction;

performing a verification process with respect to the dynamic security code to generate a verification result;

modifying the transaction authorization request message by adding the verification result to the transaction authorization request message; and

transmitting the modified transaction authorization request message to an issuer of a payment account designated for use in the payment account transaction.

16. The apparatus of claim 15, wherein receiving said request to verify includes receiving said dynamic security code and a PAN (primary account number) that identifies the designated payment account.

17. The apparatus of claim 15, wherein the transmitting modified transaction authorization request message includes transmitting a static security code associated with the designated payment account.

18. The apparatus of claim 17, wherein the transmitted modified transaction authorization request message does not include the dynamic security code.

19. The apparatus of claim 15, wherein the dynamic security code consists of a three or four digit number.

20. The apparatus of claim 15, wherein the verification process includes comparing the dynamic security code with a parallel-generated current dynamic security code and a parallel-generated previous dynamic security code, said parallel-generated current dynamic security code and said parallel-generated previous dynamic security code adjacent to each other in a sequence of parallel-generated dynamic security codes parallel-generated for the designated payment account.

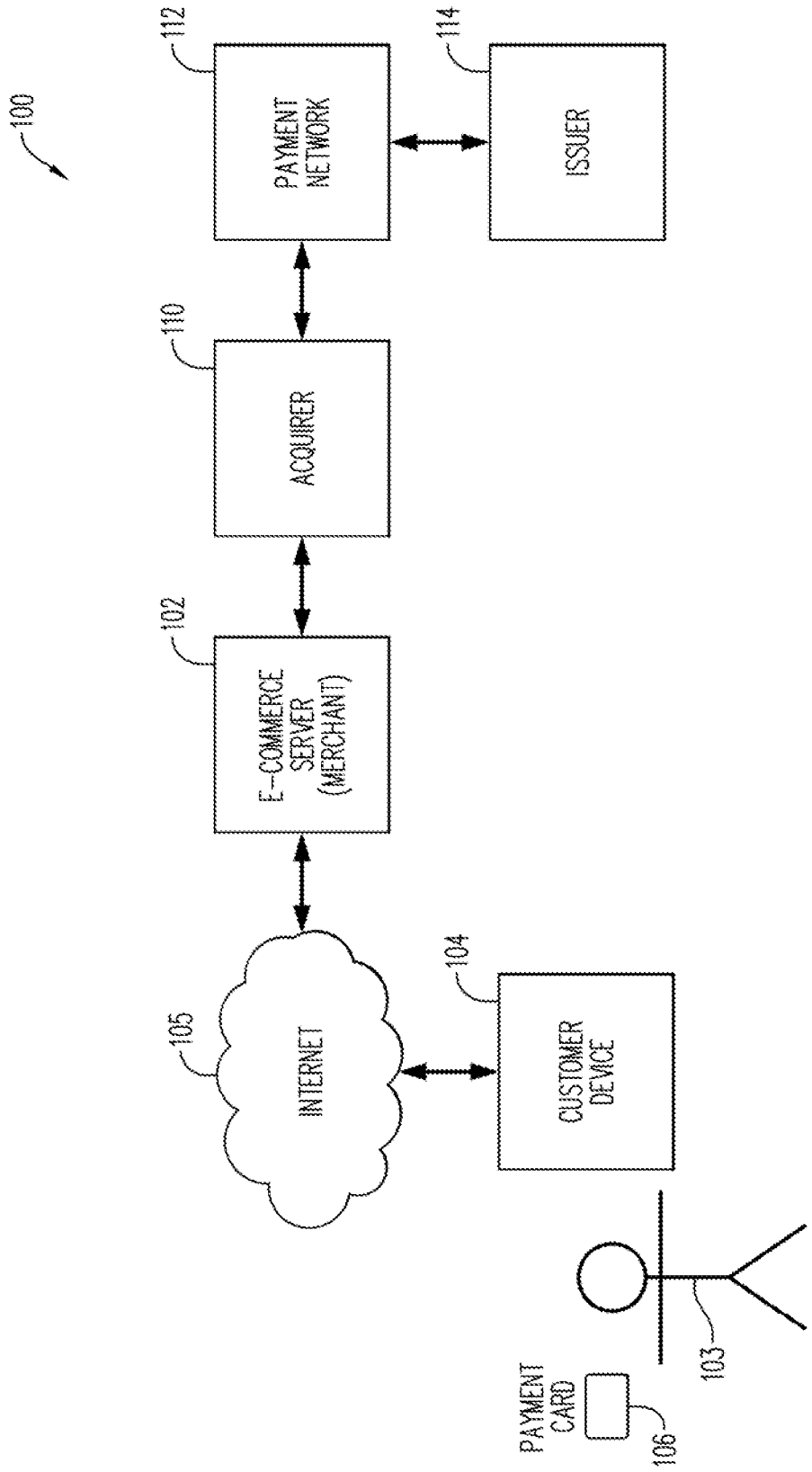


FIG. 1
(PRIOR ART)

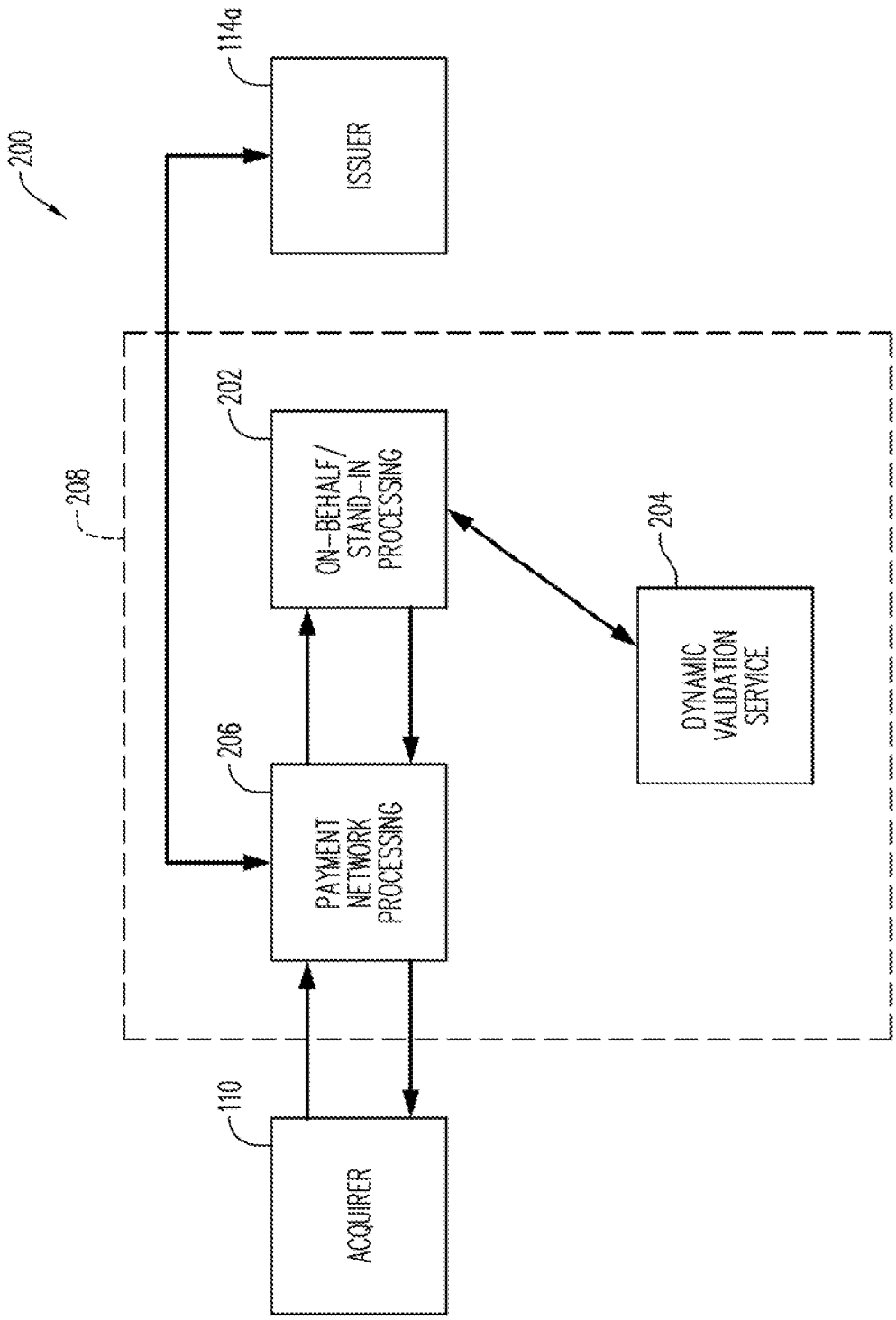

200
114a
ISSUER
208
202
ON-BEHALF / STAND-IN PROCESSING
204
DYNAMIC VALIDATION SERVICE
206
PAYMENT NETWORK PROCESSING
110
ACQUIRER

FIG. 2

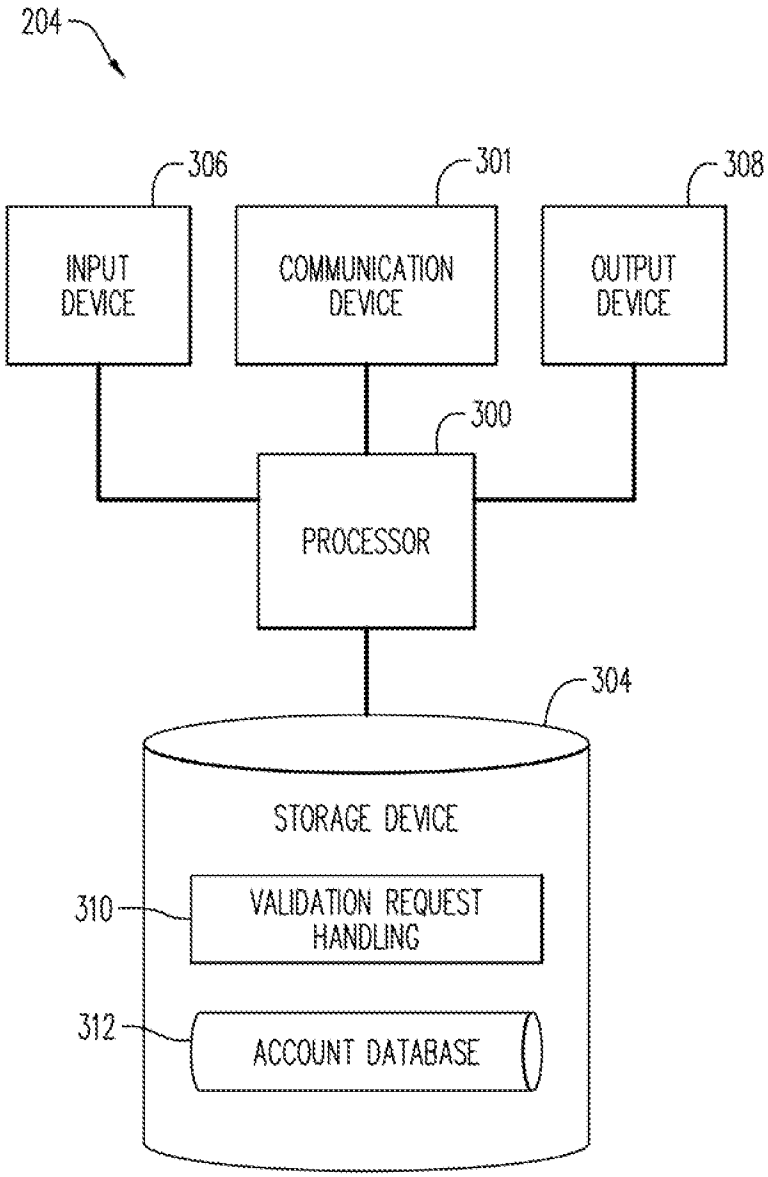

204
306
301
308
INPUT DEVICE
COMMUNICATION DEVICE
OUTPUT DEVICE
300
PROCESSOR
304
STORAGE DEVICE
310
VALIDATION REQUEST HANDLING
312
ACCOUNT DATABASE

FIG. 3

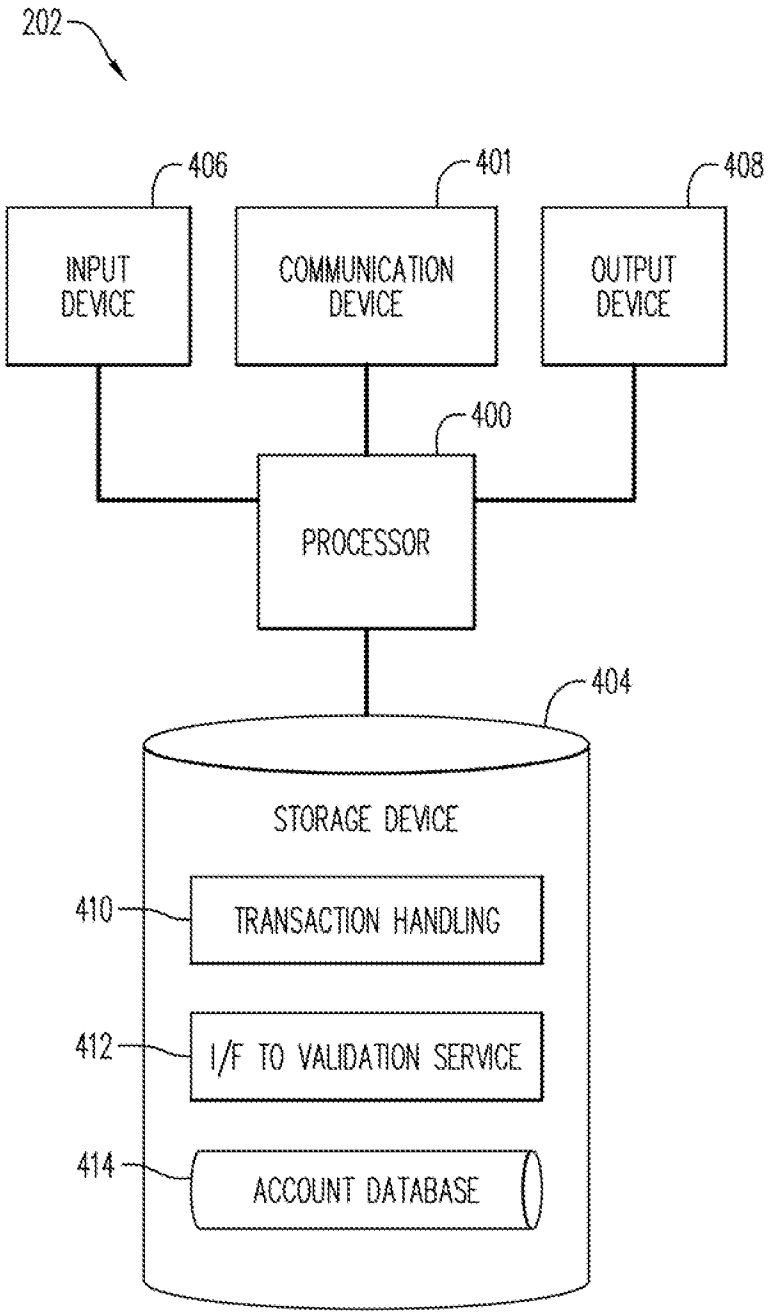

202
406
401
408
INPUT DEVICE
COMMUNICATION DEVICE
OUTPUT DEVICE
400
PROCESSOR
404
STORAGE DEVICE
410
TRANSACTION HANDLING
412
I/F TO VALIDATION SERVICE
414
ACCOUNT DATABASE

FIG. 4

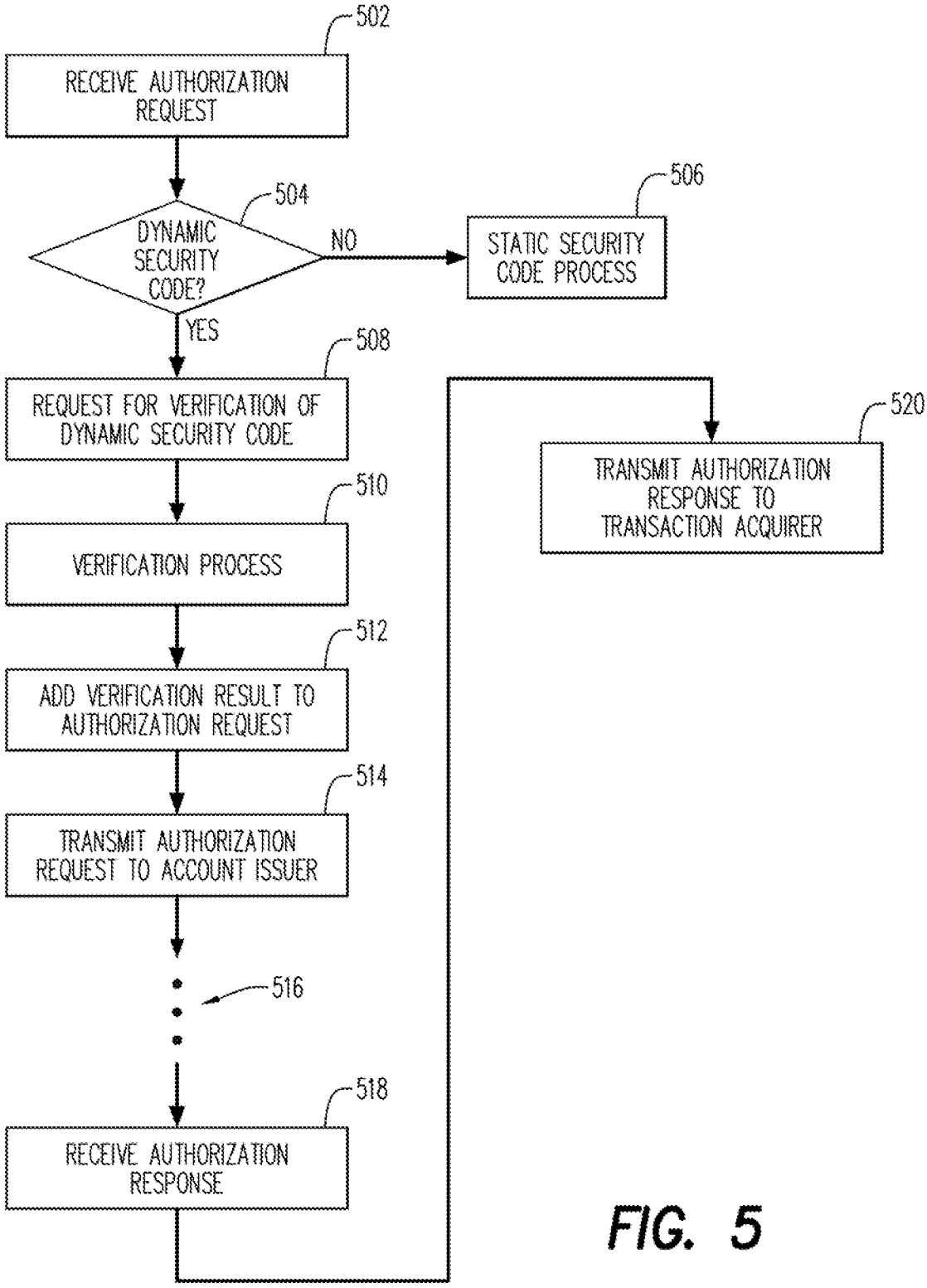

502
RECEIVE AUTHORIZATION REQUEST
504
DYNAMIC SECURITY CODE?
NO
506
STATIC SECURITY CODE PROCESS
YES
508
REQUEST FOR VERIFICATION OF DYNAMIC SECURITY CODE
510
VERIFICATION PROCESS
512
ADD VERIFICATION RESULT TO AUTHORIZATION REQUEST
514
TRANSMIT AUTHORIZATION REQUEST TO ACCOUNT ISSUER
516
518
RECEIVE AUTHORIZATION RESPONSE
520
TRANSMIT AUTHORIZATION RESPONSE TO TRANSACTION ACQUIRER

FIG. 5

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2016/065045

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06Q20/40 G06Q20/34 G06Q20/38
ADD.

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

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

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2015/161612 A1 (PARENTO STEPHEN [US] ET AL) 11 June 2015 (2015-06-11) paragraph [0047] - paragraph [0078]; claims 1,3,5; figures 5-8	1-20
X	US 2011/040640 A1 (ERIKSON GLADE RAYMOND [US]) 17 February 2011 (2011-02-17) paragraph [0068] - paragraph [0074]; claims 1,3; figures 3, 4A, 4B	5,14,19
X	US 2012/084207 A1 (HORVATH KRIS M [US] ET AL) 5 April 2012 (2012-04-05) paragraph [0103] - paragraph [0114]; figures 11-13	8,9

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

☒ See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
14 March 2017	23/03/2017

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Blackley, William

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2016/065045

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2015161612 A1	11-06-2015	AU 2014360348 A1	30-06-2016
		EP 3077973 A1	12-10-2016
		US 2015161612 A1	11-06-2015
		WO 2015085100 A1	11-06-2015
US 2011040640 A1	17-02-2011	US 2009063345 A1	05-03-2009
		US 2011040640 A1	17-02-2011
		US 2012066080 A1	15-03-2012
		US 2012221472 A1	30-08-2012
		WO 2009032523 A1	12-03-2009
US 2012084207 A1	05-04-2012	US 2008306850 A1	11-12-2008
		US 2011022481 A1	27-01-2011
		US 2012084207 A1	05-04-2012
		US 2012116977 A1	10-05-2012
		WO 2008151229 A1	11-12-2008