Office de la Propriété Intellectuelle du Canada
Un organisme d'Industrie Canada

Canadian Intellectual Property Office
An agency of Industry Canada

CA 2655748 A1 2008/02/07

(21) 2 655 748

(12) DEMANDE DE BREVET CANADIEN
CANADIAN PATENT APPLICATION

(13) A1

(86) Date de dépôt PCT/PCT Filing Date: 2007/06/18
(87) Date publication PCT/PCT Publication Date: 2008/02/07
(85) Entrée phase nationale/National Entry: 2008/12/17
(86) N° demande PCT/PCT Application No.: US 2007/071479
(87) N° publication PCT/PCT Publication No.: 2008/016752
(30) Priorités/Priorities: 2006/06/19 (US60/815,059); 2006/06/20 (US60/815,430); 2007/01/09 (US60/884,089)

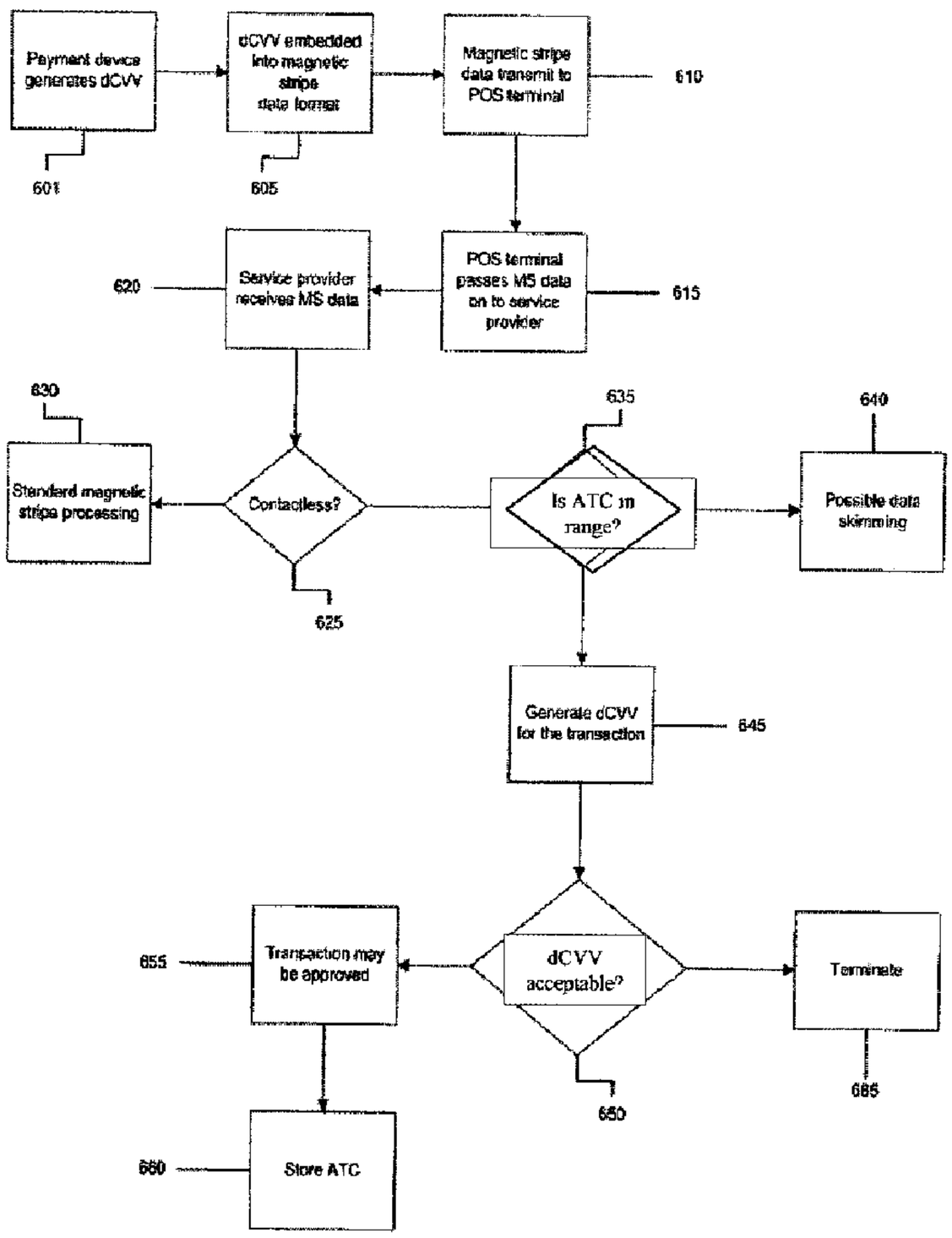
(51) Cl.Int./Int.Cl. *H04K 1/00* (2006.01)

(71) Demandeur/Applicant:
VISA U.S.A. INC., US

(72) Inventeurs/Inventors:
FAITH, PATRICK, US;
HAMMAD, AYMAN, US

(74) Agent: FETHERSTONHAUGH & CO.

(54) Titre : SYSTEME DE REDUCTION D'ERREURS DE VERIFICATION
(54) Title: VERIFICATION ERROR REDUCTION SYSTEM



(57) Abrégé/Abstract:
A method is disclosed. The method includes a) receiving a dynamic data element and a first verification value derived from the dynamic data element, wherein the first verification value is generated in response to a transaction conducted using a portable

CA 2655748 A1 2008/02/07

(21) 2 655 748

(13) A1

(57) Abrégé(suite)/Abstract(continued):
consumer device, b) determining if the dynamic data element is within a predetermined range, c) if the dynamic data element is within the predetermined range, generating a second verification value, d) determining if the second verification value matches the first verification value, or if the second verification value is otherwise acceptable, and e) initiating the approval the transaction if the second verification value matches the first verification value.

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
7 February 2008 (07.02.2008)

PCT

(10) International Publication Number
WO 2008/016752 A3

(51) International Patent Classification:
H04K 1/00 (2006.01)

(21) International Application Number:
PCT/US2007/071479

(22) International Filing Date: 18 June 2007 (18.06.2007)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

60/815,059	19 June 2006 (19.06.2006)	US
60/815,430	20 June 2006 (20.06.2006)	US
60/884,089	9 January 2007 (09.01.2007)	US

(71) Applicants *(for all designated States except US)*: **VISA INTERNATIONAL SERVICE ASSOCIATION** [US/US]; 900 Metro Center Boulevard, Foster City, California 94404 (US). **VISA U.S.A. INC.** [US/US]; P.O. Box 8999, San Francisco, California 94128 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **FAITH, Patrick** [US/US]; 2810 Jones Gate Court, Pleasanton, California 94566 (US). **HAMMAD, Ayman** [US/US]; 6048 Corte Montanas, Pleasanton, California 94566 (US).

(74) Agents: **JEWIK, Patrick R.** et al.; Townsend and Townsend and Crew LLP, Two Embarcadero Center, Eighth Floor, San Francisco, California 94111-3834 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, 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.

(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,

[Continued on next page]

(54) Title: VERIFICATION ERROR REDUCTION SYSTEM

(57) Abstract: A method is disclosed. The method includes a) receiving a dynamic data element and a first verification value derived from the dynamic data element, wherein the first verification value is generated in response to a transaction conducted using a portable consumer device, b) determining if the dynamic data element is within a predetermined range, c) if the dynamic data element is within the predetermined range, generating a second verification value, d) determining if the second verification value matches the first verification value, or if the second verification value is otherwise acceptable, and e) initiating the approval the transaction if the second verification value matches the first verification value.

WO 2008/016752 A3

WO 2008/016752 A3

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, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

(88) Date of publication of the international search report:
17 April 2008

VERIFICATION ERROR REDUCTION SYSTEM

CROSS-REFERENCES TO RELATED APPLICATIONS

[0001] This application claims the benefit of the filing dates of U.S. Provisional Patent Application Nos. 60/815,059 filed June 19, 2006, 60/815,430 filed June 20, 2006, and 60/884,089 filed January 9, 2007, which are hereby incorporated by reference, as if set forth in full in this document, for all purposes.

BACKGROUND

[0002] As methods and devices for engaging in financial transactions have increased, old problems such as fraud and counterfeiting persist.

[0003] One of the primary sources of fraud, which is prevalent in the credit card industry is skimming. Skimming refers to the electronic copying of a card's magnetic stripe data to create counterfeit cards.

[0004] Skimming is predominantly a phenomenon afflicting magnetic stripe based transactions. This is because the magnetic stripe, which is placed on the back of a transaction card and stores a variety of data on three separate tracks, is a passive medium. In other words, the digital content of the magnetic stripe can be perfectly copied, without any difference between the copy and the original.

[0005] One of the primary means by which skimming can be prevented is for the consumer to closely monitor the whereabouts of his transaction card. This may allow the consumer to prevent the card from being swiped through inappropriate devices. However, as contactless cards evolve, the classic skimming problem comes along with it. In fact, in a wireless environment the opportunity to skim magnetic stripe data is more prevalent. In a wireless environment, a potential skimmer need not physically possess the card to be skimmed nor have access to any of the physical equipment (e.g. POS terminal, communication lines, etc.) which is required for skimming in a wire based environment. A skimmer can, without the knowledge of the consumer or merchant, intercept the wireless transaction and copy the data being transmitted from the card to POS terminal.

[0006] To address the above problems, some have proposed using a dCVV or a dynamic card verification value. The dCVV can be generated using an algorithm which uses at least a counter and input data such as an account number, expiration date, and other information. The counter can increase by one each time a transaction is conducted. The dCVV can be independently generated by either a portable consumer device or POS terminal at the front end of a transaction and can be sent to a back end computer. The counter may be sent from the merchant to the back end computer so that it knows the current counter value associated with the portable consumer device. In other cases, the counter may simply be present at the back end computer. In the latter case, the counter increments every time the back end computer sees a transaction. The back end computer, using a similar algorithm to the one that generated the dCVV at the front end, the counter value, and input data, can independently generate a second dCVV. If the received dCVV and the generated dCVV match, the transaction can be considered authentic. If the dCVVs do not match, this may indicate that the transaction is fraudulent.

[0007] Although the above-described dCVV process is useful, there may, however, be a number of instances where the counter value transmitted from a portable consumer device and received at the back end server does not match the corresponding counter value at the back end computer. For example, sometimes, a merchant might not forward transaction data to the issuer in a timely manner. If this occurs, it is possible that future transactions conducted by the consumer could be inadvertently rejected. For instance, if the portable consumer device used by the consumer has a counter in it to count the number of transactions conducted, and if the counter in the back end computer does not keep a corresponding transaction count (e.g., because of the delayed receipt of transaction data from one or more merchants, chargebacks), some of the consumer's transactions may be inadvertently rejected. This is undesirable.

[0008] Embodiments of the invention address these and other problems, individually and collectively.

BRIEF SUMMARY

[0009] Embodiments of the present invention describes verification error reduction systems and methods for dynamically verifying the authenticity of a payment service

deployed on a portable consumer device, such as an integrated circuit credit card, each time the payment service is utilized in a transaction.

[0010] One embodiment of the invention is directed to a method comprising: a) receiving a dynamic data element and a first verification value derived from the dynamic data element (e.g., a counter), wherein the first verification value (a dCVV) is generated in response to a transaction conducted using a portable consumer device; b) determining if the dynamic data element is within a predetermined range; c) if the dynamic data element is within the predetermined range, generating a second verification value; d) determining if the second verification value matches the first verification value, or if the second verification value is otherwise acceptable; and e) initiating the approval the transaction if the second verification value matches the first verification value, or if the second verification value is otherwise acceptable.

[0011] Another embodiment of the invention is directed to a computer readable medium comprising: code for receiving a dynamic data element and a first verification value derived from the dynamic data element, wherein the first verification value is generated in response to a transaction conducted using a portable consumer device; code for determining if the dynamic data element is within a predetermined range; code for generating a second verification value if the dynamic data element is within the predetermined range; code for determining of the second verification value matches the first verification value, or if the second verification value is otherwise acceptable; and code for initiating the approval of the transaction if the second verification value matches the first verification value, or if the second verification value is otherwise acceptable.

[0012] Other embodiments of the invention are directed to server computers and systems.

BRIEF DESCRIPTION OF THE DRAWINGS

[0013] FIG. 1 depicts a method of creating an encrypted data block for use in an embodiment of the present invention.

[0014] FIG. 2 depicts a method for generating unique derived keys from data residing on a portable consumer device.

[0015] FIG. 3 depicts a method for extracting portions of an encrypted data block for creating a dynamic card verification value according to the present invention.

[0016] FIG. 4 depicts an exemplary record format for use in an embodiment of the present invention.

[0017] FIG. 5 depicts an alternative exemplary format for use in an embodiment of the present invention.

[0018] FIG. 6 is a flowchart of a preferred method of utilizing a dynamically created verification value to authenticate a transaction.

[0019] FIG. 7 is a flowchart of an alternate method of utilizing a dynamically created verification value to authenticate a transaction.

DETAILED DESCRIPTION

[0020] Before the present methods are described, it is to be understood that this invention is not limited to the particular methodologies, devices or protocols described, as these may vary. It is also to be understood that the terminology used in the description is for the purpose of describing the particular versions or embodiments only, and is not intended to limit the scope of the present invention which may be limited only by the appended claims. In particular, although the present invention is described in conjunction with financial transactions, it may be appreciated that the present invention may find use in any electronic exchange of data.

[0021] It is also noted that as used herein and in the appended claims, the singular forms "a", "an", and "the" include plural reference unless the context clearly dictates otherwise. Thus, for example, reference to a "key" is a reference to one or more keys and equivalents thereof known to those skilled in the art, and so forth.

[0022] Generally, embodiments of the invention provide improved methods and systems for dynamically generating a card verification value for each transaction and for utilizing such value to verify that the payment service is authentic and has not been skimmed. The dynamically generated Card Verification Value (referred to herein as the "dCVV") is generated on the portable consumer device, embedded into the payment data, and transmitted to a point of sale terminal. In an alternate

embodiment, payment data is received from a portable consumer device, a verification value is generated by a point of sale terminal, and the verification value is embedded into the payment data.

[0023] In an embodiment, data received by the point of sale terminal is interpreted as simply payment data (e.g. standard magnetic stripe Track 1 and/or Track 2 data without an embedded dCVV) by the point of sale terminal. The point of sale terminal passes on the received data to a payment network which, in turn, passes the data on to the service provider. If the service provider determines the transaction is one for which a dCVV is required, the service provider independently generates a verification value. If the verification value generated by the service provider does not match the dCVV received from the portable consumer device, the transaction is identified as potentially fraudulent and disapproved.

[0024] In an alternate embodiment, data is received by the point of sale terminal and is used by the point of sale terminal to generate a verification value. The point of sale terminal passes on the received data to a payment network which, in turn, passes the data on to the service provider. The service provider independently generates a verification value. If the verification value generated by the service provider does not match the dCVV received from the point of sale terminal, the transaction is identified as potentially fraudulent and disapproved.

[0025] As explained above, in some instances, a dynamic data element such as a counter (or other type of data element that can change) can be received at a back end computer along with a dCVV generated by a portable consumer device. The back end computer can determine if the counter is within a predetermined range. If it is, then the back end computer can independently generate another dCVV. If the received dCVV and the generated dCVV match, then the transaction can be considered authentic.

[0026] The back end computer can comprise a processor, and a computer readable medium comprising code for performing any of the functions described herein. For example, the back end computer may comprise a computer readable medium comprising code for receiving a dynamic data element and a first verification value derived from the dynamic data element, wherein the first verification value is generated in response to a transaction conducted using a portable consumer device,

code for determining if the dynamic data element is within a predetermined range, code for generating a second verification value if the dynamic data element is within the predetermined range, code for determining if the second verification value matches the first verification value, and code for initiating the approval of the transaction if the second verification value matches the first verification value.

[0027] The range of counter values at the back end computer provides some tolerance, in case the counter at the back end computer does not match the counter that it receives from a POS terminal. In preferred embodiments, the range of counter values is less than about 10, or between about 2 and about 10. If the counter received from the POS terminal and the counter at the back end server are within, for example, 10 or even 5 or less, the transaction may be considered authentic even if the dCVVs do not match.

[0028] Advantageously, in embodiments of the invention, fewer transactions will be rejected as being non-authentic due to non-matching counter values. Note that although counter values are described in detail, other types of values and ranges could be used. For example, the dynamic data element could be a time of day and the range could be a range of days.

[0029] For purposes of this application, the term "portable consumer device" can include any device comprising a microprocessor which may be used in a transaction or data exchange as described herein. Without limiting the generality of the foregoing, "portable consumer device" can include an integrated circuit card (also commonly known as a smartcard), a memory card, a cellular telephone, a personal digital assistant, a mobile electronic device, or a computer.

[0030] For purposes of this application, "contactless" or "wireless" can include any communications method or protocol, including proprietary protocols, in which data are exchanged between two devices without the need for the devices to be physically coupled. Without limiting the generality of the foregoing, "contactless" or "wireless" can include data transmissions by laser, radio frequency, infrared communications, Bluetooth, or wireless local area network.

[0031] For purposes of this application, the term "payment service" can include any application deployed on a portable consumer device which causes the exchange of

data between the portable consumer device and any other device or location. It should be appreciated that "payment service" is not limited to financial applications.

[0032] For purposes of this application, "payment data" can include, with respect to financial applications those data elements used by the payment service to execute a transaction, and with respect to non-financial transactions any necessary data elements exclusive of the present invention. For example, when the payment service is a magnetic stripe credit card transaction, "payment data" would comprise Track 1 and/or Track 2 data, as that is understood by one of ordinary skill in the credit card industry, such as the primary account number, expiration date, service codes, and discretionary data. "Payment data" may also comprise a unique card identification number or a unique identification number for a service provider.

[0033] In an embodiment of the invention, the payment data may reside in memory located in the portable consumer device. The portable consumer device may also maintain an application transaction counter (ATC), which may be a value of any suitable length. The ATC may initially be set by the service provider to a predetermined value. Thereafter, the ATC may be incremented with each transaction. Alternately, the ATC may be decremented from its initial predetermined value with each transaction. In addition, the service provider which deployed the payment service may maintain a corresponding ATC accessible to the service provider's computer. As discussed in more detail below, this corresponding ATC is used to identify payment services which may have been skimmed. In an alternate embodiment, a cryptogram, digital signature, or hash value based on transaction data may be used in place of or in conjunction with the ATC.

[0034] Each time the payment service is initiated, a dCVV is generated on the portable consumer device for authentication purposes. FIG. 1 depicts the method of generating a dCVV for each transaction according to the present invention. Initially, a numeric string of predetermined length is created. This numeric string is created by overlaying 101 the ATC 102 over the corresponding leftmost digits of the account number for the payment service or PAN 104. This numeric string is concatenated on the right with the expiration date for the payment service and the service code to produce a concatenated value 106. If necessary, padding characters 108 are concatenated 110 on the right of the concatenated value 106 to form a numeric

string 112 with a predetermined fixed length. In one embodiment, this numeric string 112 is 128-bits in length, although a numeric string of any length may be used. The padding characters 108 may consist of a stream of 0's, 1's, or any other numeric value that is known both to the portable consumer device and the service provider. The numeric string 112 is bisected into two blocks of equal length, Block A 116 and Block B 118. Block A 116 is then encrypted 121 with a first encryption key 120. The result of the encryption step 121 is Block C 122 of length equal to Block A 116. Block C 122 is then exclusively OR'ed (XOR) 123 with Block B 118 resulting in Block D 124. Block D 124 is then encrypted 125 with a second encryption key 126 to produce Block E 128. Block E 128 is then decrypted 129 using a decryption key 130 to produce Block F 132. Block F 132 is then encrypted 133 using a fourth encryption key 134 to produce Block G 136.

[0035] It will be apparent to one of ordinary still in the art that the first encryption key 120, the second encryption key 126, the third encryption key 130 and the fourth encryption key 134 may take any preselected value. In an embodiment of the present invention, the first encryption key 120, the second encryption key 126, and the fourth encryption key 134 are equivalent and of a different value from the third encryption key 130. Other permutations of the encryption key values utilized in the methodology of FIG.1 are within the scope of the present invention.

[0036] In one embodiment, the first encryption key 120, the second encryption key 126, the third encryption key 130, and the fourth encryption key 134 take the value of unique keys derived from data existing on the portable consumer device. Upon deployment, each payment service is personalized by the service provider with a master derivation key. The master derived key may be deployed with payment services in batches (i.e. multiple payment services receive the same master derived key) or individually. Each portable consumer device may be personalized with the functionality to derive keys unique to the payment service.

[0037] FIG. 2 shows the methodology for deriving two unique keys which are utilized in the preferred embodiment. The account number 201, the account sequence number 202, the inverse of the account number 203, and the inverse of the account sequence number 204 are concatenated together to create a concatenated value 210. If necessary, the concatenated value 210 may be padded

with zeroes, or some other value 211 and may accommodate additional discretionary data comprising one or more data elements, to create a string of a predetermined fixed length. In one embodiment, the concatenated value 210 may be 128 bits in length, although the concatenated value is not limited to being this length and may accommodate additional discretionary data comprising one or more data elements. The concatenated value 210 is then encrypted 220 using the master derivation key 221 as the encryption key for each encryption stage. The encryption utilized may include any type of encryption methodology. For example, this encryption step may utilize Triple-DES encryption. The value resulting from the encryption step 220 is a unique derived key or UDK 230 for the application identified by the account number. Two additional keys, UDKA 240 and UDKB 241, are derived from the UDK. The derivation of UDKA 240 and UDKB 241 from the UDK 230 may take any form, including assigning the value of the leftmost half of the UDK 230 to UDKA 240, and assigning the value of the rightmost half of the UDK 230 to UDKB 241. Alternatively, the UDKA 240 may be derived by selecting alternating or other predetermined bit sequences from the UDK 230 while the remaining bits are assigned to UDKB 241. Furthermore, there is no requirement that UDKA 240 and UDKB 241 are of equal length.

[0038] FIG. 3 describes the further processing required to generate the dCVV. Each nibble (4-bit grouping) of the value stored in Block G 136 is subjected to two separate iterative processes to evaluate the value of each nibble. As shown in FIG. 3, beginning with the most significant (i.e. left most) digit of Block G 136 and examining each sequential nibble, if a nibble contains a value ranging from zero to nine, inclusive, that value is extracted 301 and placed in a new numeric string 305, referred to herein as a holding string, by concatenating the extracted value to the right of the previously extracted value, if any. The result may be that the holding string contains a series of values ranging from zero to nine, inclusive, which appear from left to right in the holding string in the same sequence in which they appear in Block G 136.

[0039] A second evaluation is then performed again beginning with the most significant digit of Block G 136 and examining each sequential nibble. If a nibble contains a hexadecimal value ranging from ten (A) to fifteen (F), inclusive, that value is extracted 310. The extracted value is then decimalized by subtracting the

hexadecimal value A from the extracted value resulting in a decimalized value ranging from zero to five 315. This decimalized value is then concatenated on the right to the right most value of the holding string 320.

[0040] Once all nibbles in Block G have been twice examined as described, the three most-significant (i.e. left-most) nibbles of the holding string are extracted 325. This 3-digit value is the dCVV for the transaction. Other numbers of bits may be extracted from the twice-examined nibble string to generate the dCVV for a transaction. Furthermore, different nibbles, such as the rightmost nibbles, may be used as the dCVV for a transaction. The three leftmost nibbles, however, represent a preferred embodiment.

[0041] Once generated, the dCVV is embedded into the payment data transmitted from the portable consumer device to the point of sale terminal. The data received by the point of sale terminal may appear to the point of sale terminal as standard payment data. In other words, the point of sale terminal may not be able to determine if a dCVV is embedded and where such dCVV may be located. There is no indication to the point of sale terminal that a dCVV is embedded into the data received from the portable consumer device.

[0042] FIG. 4 depicts an exemplary record format for transmitting payment data, with the dCVV embedded therein, from the portable consumer device to the point of sale terminal. The record format of FIG. 4 is created by concatenating a primary account number 401 for the payment service, with an expiration date 402, and a service code 403. In one embodiment, the primary account number 401 is 16 digits long, the expiration date 402 is four digits long, and the service code 403 is three digits long. However, the primary account number 401, the expiration date 402, and the service code 403 are not limited to being these lengths. Next, in a field typically reserved for other uses, a value is placed as an indicator 705 that a dCVV has been embedded in this record. The value of this indicator is known by the service provider which deployed the application on the portable consumer device. Next, the ATC 410 is placed in the field which may typically be reserved for PIN verification data. Finally, the dCVV 415 is concatenated on the right of the record. The remainder of the record may comprise additional discretionary data.

[0043] Alternately, FIG. 5 depicts a second exemplary format for transmitting payment information with the dCVV embedded thereon from the portable consumer device to the point of sale terminal. The format in FIG. 5 is created by concatenating a primary account number 501 for the payment service, with an expiration date 502, a service code 503, a PVKI 504, and a field for PIN verification data 505. In one embodiment, the primary account number 501 is sixteen digits long, the expiration date 502 is four digits long, the service code 503 is three digits long, the PVKI 504 is one digit long, and the PIN verification data 505 is four digits long. However, the primary account number 501, the expiration date 502, the service code 503, the PVKI 504, and the PIN verification data 505 are not limited to being these lengths. Next, in a single data field 510 each of the dynamically created CVV, the ATC and the indicator to be used by the service provider to identify that a dynamic CVV has been embedded are stored in sequence. The remainder of the record may comprise additional discretionary data.

[0044] An aspect of the present invention is that the system of utilizing the dynamically created CVV allows the service provider to make a determination of the authenticity of the payment service being utilized. This authentication step is not left to merchants, individual point of sale terminals, or other third parties or devices. FIG. 6 shows how the dCVV is used in a contactless environment to permit the service provider to evaluate the authenticity of the payment application deployed on the portable consumer device to make a determination of whether the payment application has been skimmed. Although shown in the embodiment of a contactless environment in FIG. 6, the present invention is not limited to such an environment and may be used for any transaction where magnetic stripe Track 1 and/or Track 2 data is exchanged using any method or means for communicating such data.

[0045] As shown in FIG. 6, the portable consumer device generates the dCVV 601, using the methodology described above. The dCVV is embedded into the payment data 605. In this respect, the exemplary record formats shown in FIG. 4 or FIG. 5 may be utilized. The payment data with the embedded dCVV is transmitted by data communication to the point of sale terminal 610. The point of sale terminal recognizes the received data as in the standard format of payment data and passes the data stream on to the service provider computer 615, likely via a payment network (not shown). The service provider computer receives 620 the payment data

with the embedded dCVV and interrogates the appropriate indicator to determine if the transaction was a contactless transaction or not 625. If the service provider computer determines that the transaction was not a contactless transaction, the transaction is processed in its normal manner 630. If the service provider computer determines that the transaction was contactless, the service provider computer compares the ATC received from the portable consumer device to the corresponding ATC on the service provider computer to determine if the received ATC is the expected next ATC 635, and/or is within an allowable range. If the ATC received from the portable consumer device is not the expected next ATC or within the allowable range, the payment service deployed on the portable consumer device has potentially been skimmed 640. If the expected next ATC and/or an ATC that is within the allowable range is received, the service provider computer may independently re-generate the dCVV for the given transaction 645 utilizing a similar or analogous process as described above. If the service provider generated dCVV matches the dCVV received from the portable consumer device 650, or if the dCVV is one that can be generated using an ATC within the allowable range, the service provider deems the payment application to be authentic 655. The service provider computer then replaces the ATC which was previously stored on the service provider computer with the generated ATC received from the portable consumer device 660 for subsequent authentications. If the service provider generated dCVV does not match the dCVV, or is not one which is derived from an ATC within the allowable range, the transaction is potentially fraudulent and is terminated 665.

[0046] The methodology of FIG. 6 discussed in conjunction with contactless transactions, is not limited thereto. For example, the methodology may be utilized with respect to transactions above a certain threshold value. In such an instance, the service provider, upon deploying the application, would configure the application to generate a dCVV for transactions above the threshold. The indicator interrogated in Step 625 would then be set for transactions above the threshold value. Similarly, the methodology may be utilized with respect to any other transaction criteria including, but not limited to, geographic location, use patterns, or any other criteria.

[0047] In an alternate embodiment, the portable consumer device transmits payment data to a point of sale terminal such as a credit card terminal 701. The point of sale terminal receives the data and computes a verification value for the

transaction 705. The verification value may be computed in a number of different ways including, without limitation, using a unique transaction number provided by the point of sale terminal, a timestamp, or a transaction amount added to a timestamp. The point of sale terminal may then embed and/or append the verification value and additional data to the payment data 710. The additional data may be required for the service provider computer to verify the transaction. The point of sale terminal then passes the data stream on to the service provider computer 715, likely via a payment network (not shown). The service provider computer receives the payment data with the verification value 720. The service provider computer may optionally compare at least a portion of the additional data embedded or appended by the point of sale terminal to corresponding data stored on the service provider computer to determine if the received data is proper 725, and/or is within a predetermined range. If the received data from the point of sale terminal is improper, the transaction data may potentially have been skimmed 730. If proper data, the service provider computer may independently re-generate the verification value for the given transaction utilizing the same process as used by the point of sale terminal 735. If the service provider generated verification value matches the verification value received from the point of sale terminal 740, of if the generated verification value is otherwise acceptable (e.g., the verification value is generated using dynamic data elements that are within acceptable ranges), the service provider deems the payment application to be authentic 745. The service provider computer may then optionally update the additional data which was previously stored on the service provider computer with the additional data received from the portable consumer device for subsequent authentications 750. If the service provider generated verification value does not match the verification value received from the point of sale terminal, or is otherwise not acceptable, the transaction is potentially fraudulent and is terminated 755.

[0048] The foregoing is considered as illustrative only of the principles of the invention. Further, since numerous modifications and changes may readily occur to those skilled in the art, it is not desired to limit the invention to the exact construction and operation shown and described, and accordingly, all suitable modifications and equivalents may be resorted to, falling within the scope of the invention.

WHAT IS CLAIMED IS:

1. A method comprising:

a) receiving a dynamic data element and a first verification value derived from the dynamic data element, wherein the first verification value is generated in response to a transaction conducted using a portable consumer device;

b) determining if the dynamic data element is within a predetermined range;

c) generating a second verification value;

d) determining if the second verification value matches the first verification value, or if the second verification value is otherwise acceptable; and

e) initiating the approval the transaction if the second verification value matches the first verification value, or if the second verification value is otherwise acceptable.

2. The method of claim 1 wherein the dynamic data element is a counter value and wherein the predetermined range is a predetermined counter range.

3. The method of claim 2 wherein the predetermined counter range is between 2 and 10.

4. The method of claim 1 wherein the portable consumer device is a card.

5. The method of claim 1 wherein the portable consumer device is a phone.

6. The method of claim 1 a)-d) are performed by a service provider computer.

7. The method of claim 1 wherein initiating the approval includes approving the transaction or sending a message to an issuer who subsequently approves the transaction.

8. The method of claim 1 wherein the transaction is a purchase transaction.

9. The method of claim 1 wherein the predetermined range is less than 5.

10. The method of claim 1 wherein the verification value is 4 digits or less.

11. A computer readable medium comprising:
code for receiving a dynamic data element and a first verification value derived from the dynamic data element, wherein the first verification value is generated in response to a transaction conducted using a portable consumer device;
code for determining if the dynamic data element is within a predetermined range;
code for generating a second verification value;
code for determining of the second verification value matches the first verification value, or if the second verification value is otherwise acceptable; and
code for initiating the approval of the transaction if the second verification value matches the first verification value, or if the second verification value is otherwise acceptable.

12. The computer readable medium of claim 11 wherein the dynamic data element is a counter value and wherein the predetermined range is a predetermined counter range.

13. The computer readable medium of claim 12 wherein the predetermined counter range is between 2 and 10.

14. The computer readable medium of claim 11 wherein the portable consumer device is a card.

15. A computer comprising the computer readable medium of claim 11.

16. The computer of claim 15 wherein the dynamic data element is a counter value.

17. The computer apparatus of claim 15 wherein the predetermined counter range is between 2 and 10.

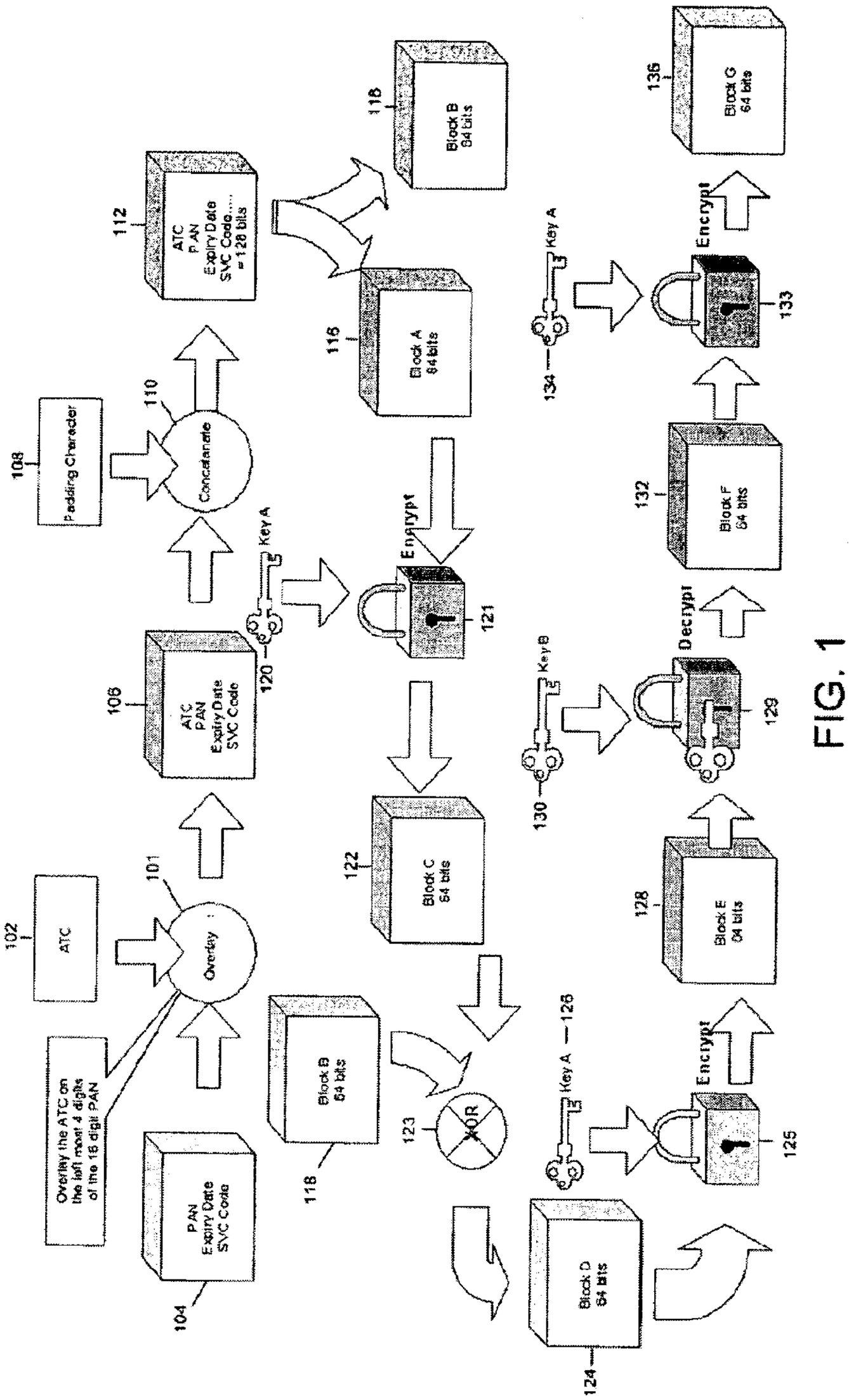

ATC
PAN
Expiry Date
SVC Code
106
Padding Character
108
Concatenate
110
ATC
PAN
Expiry Date
SVC Code.....
= 128 bits
112
Block A
64 bits
116
Block B
64 bits
118
Key A
120
Encrypt
121
Block C
64 bits
122
XOR
123
Block D
64 bits
124
Key B
126
Decrypt
129
Block E
64 bits
128
Key B
130
Encrypt
Block F
64 bits
132
Key A
134
Encrypt
133
Block G
64 bits
136
ATC
102
Overlay
101
Overlay the ATC on the left most 4 digits of the 16 digit PAN
PAN
Expiry Date
SVC Code
104
Block B
64 bits
118
Key A
126
Encrypt
125

FIG. 1

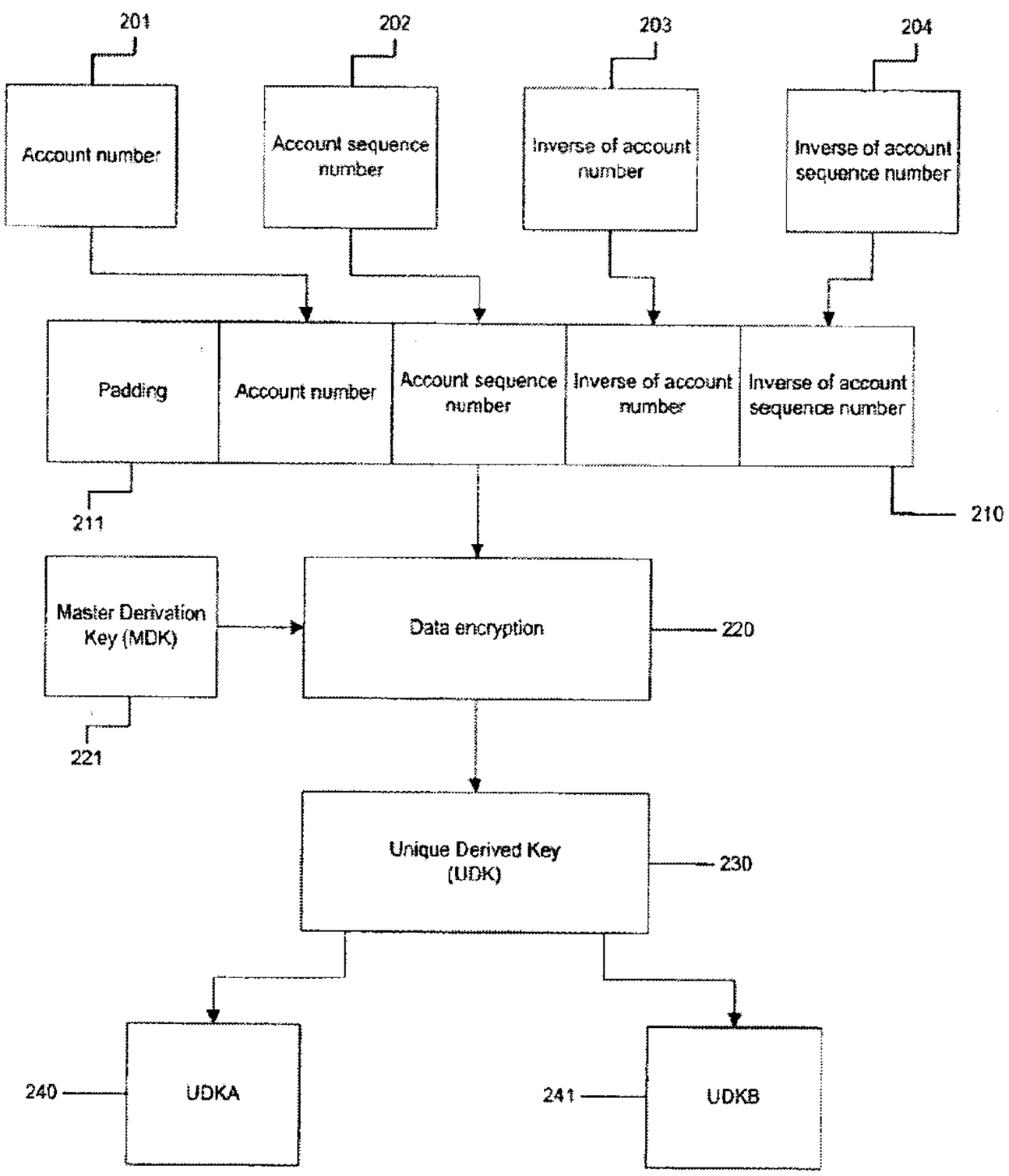

201
202
203
204
Account number
Account sequence number
Inverse of account number
Inverse of account sequence number
Padding
Account number
Account sequence number
Inverse of account number
Inverse of account sequence number
211
210
Master Derivation Key (MDK)
Data encryption
220
221
Unique Derived Key (UDK)
230
240
UDKA
241
UDKB

FIG. 2

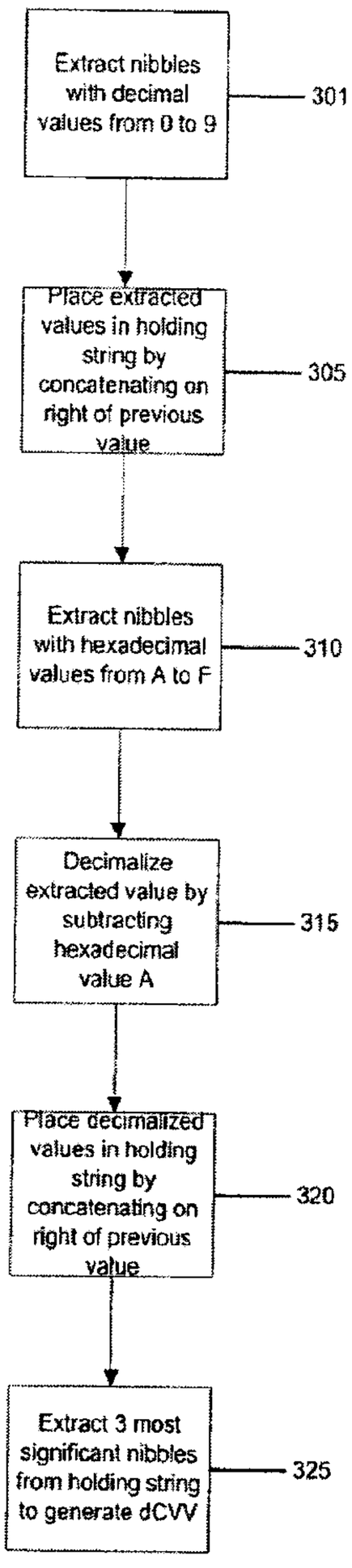

Extract nibbles with decimal values from 0 to 9
301
Place extracted values in holding string by concatenating on right of previous value
305
Extract nibbles with hexadecimal values from A to F
310
Decimalize extracted value by subtracting hexadecimal value A
315
Place decimalized values in holding string by concatenating on right of previous value
320
Extract 3 most significant nibbles from holding string to generate dCVV
325

FIG. 3

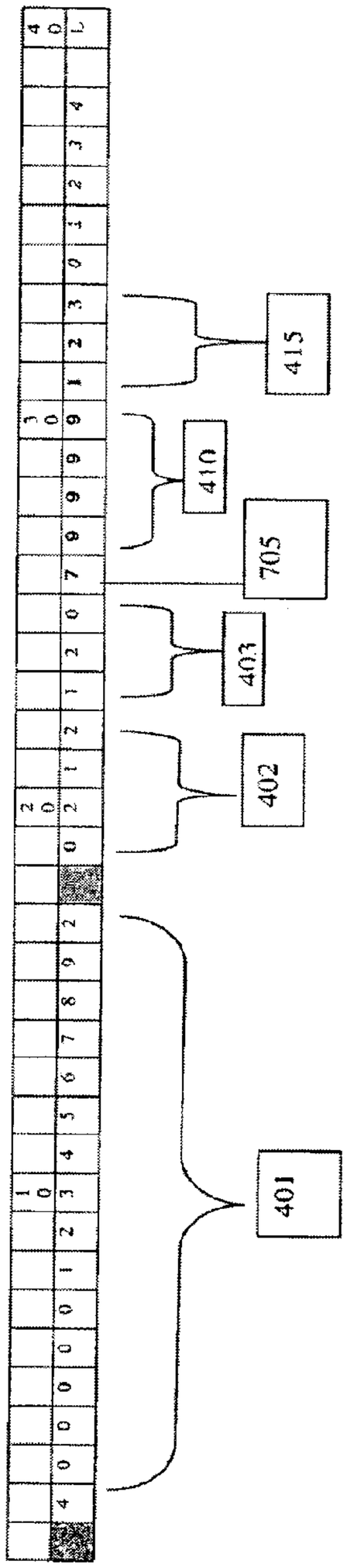


FIG. 4

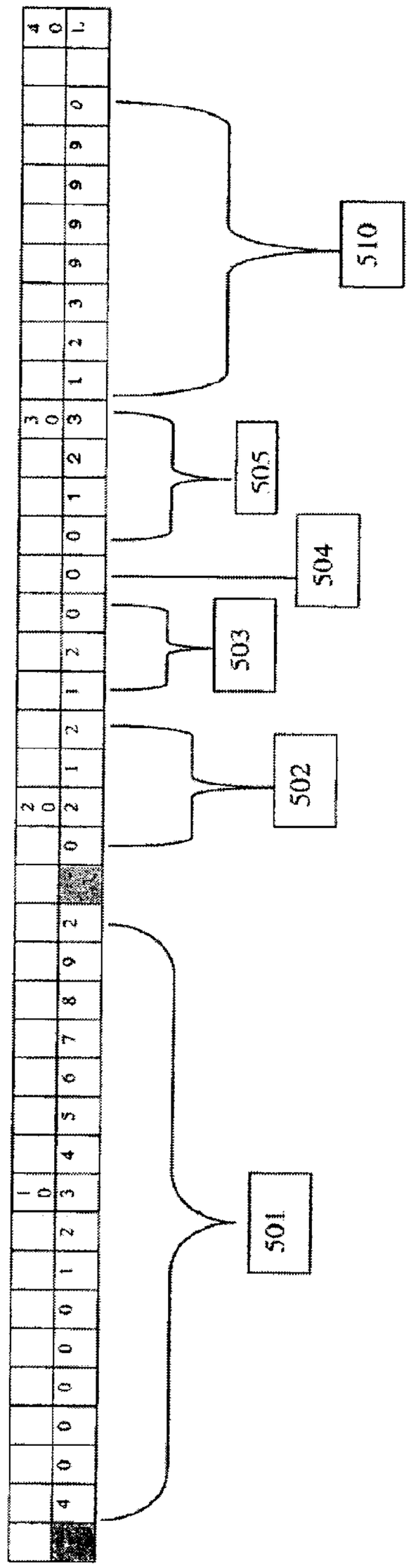


FIG. 5

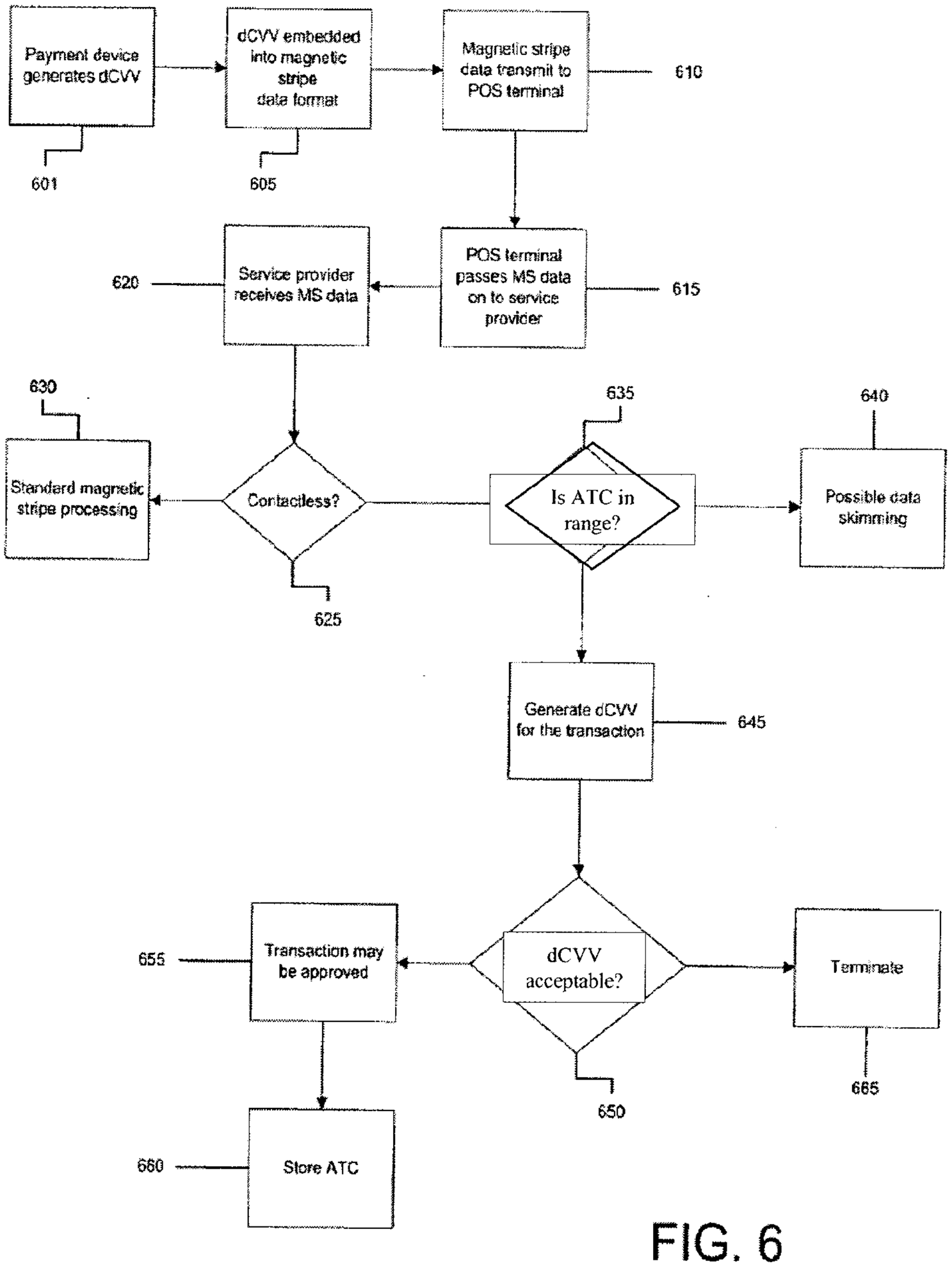

Payment device generates dCVV
601
dCVV embedded into magnetic stripe data format
605
Magnetic stripe data transmit to POS terminal
610
POS terminal passes MS data on to service provider
615
Service provider receives MS data
620
630
Standard magnetic stripe processing
Contactless?
625
635
Is ATC in range?
640
Possible data skimming
Generate dCVV for the transaction
645
dCVV acceptable?
650
655
Transaction may be approved
Terminate
665
660
Store ATC

FIG. 6

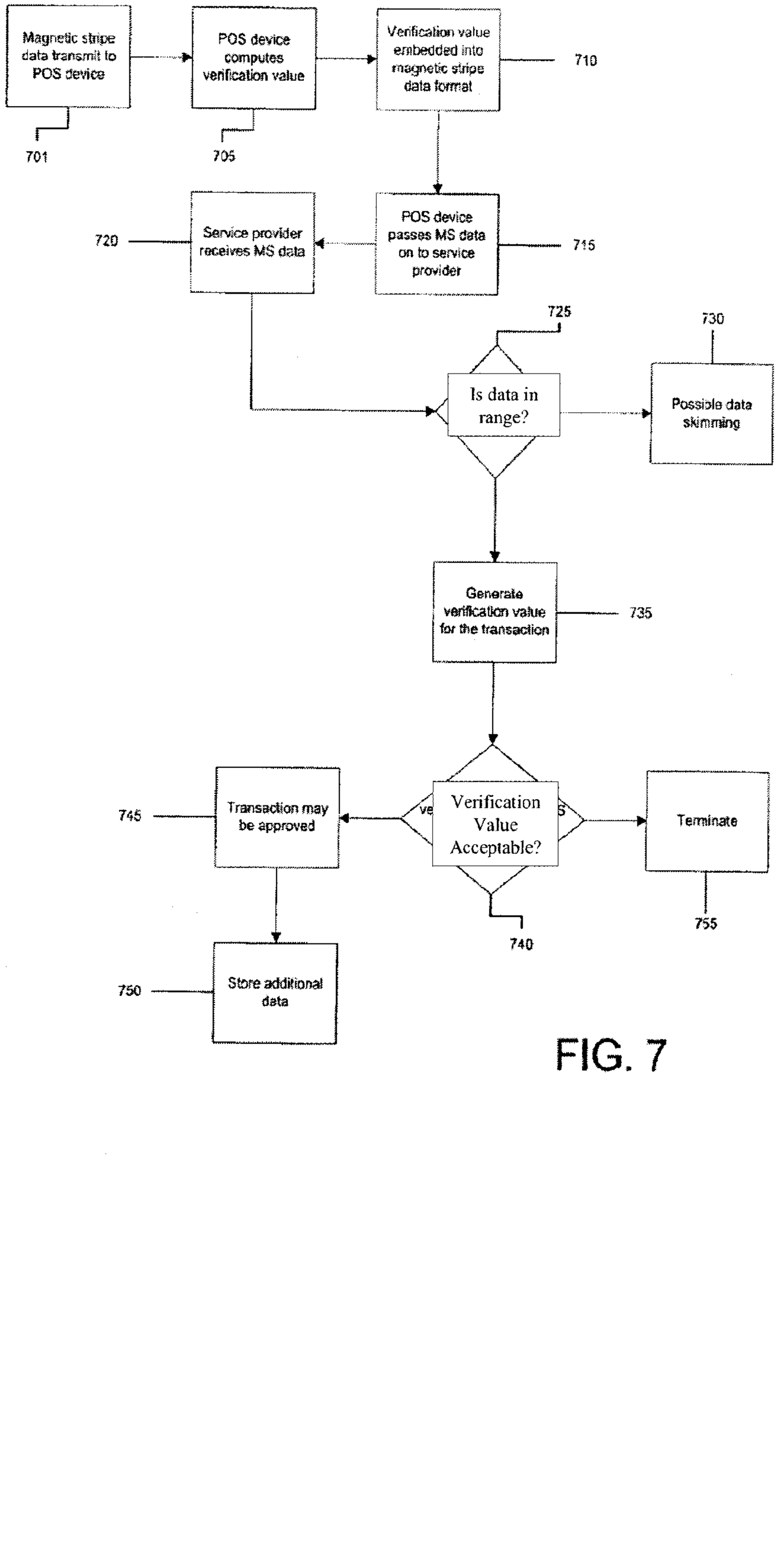
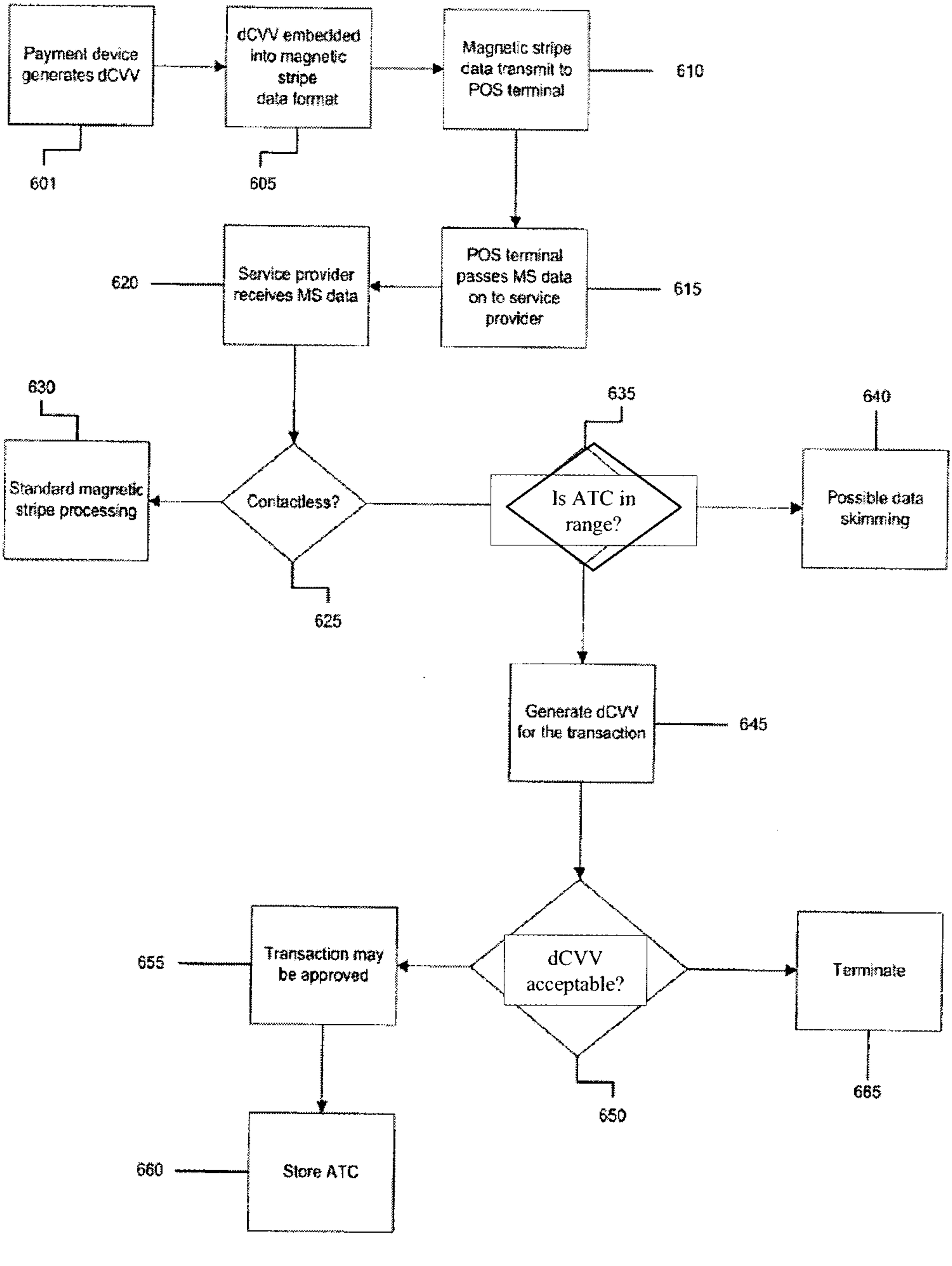

Magnetic stripe data transmit to POS device
701
POS device computes verification value
705
Verification value embedded into magnetic stripe data format
710
POS device passes MS data on to service provider
715
Service provider receives MS data
720
725
Is data in range?
730
Possible data skimming
Generate verification value for the transaction
735
Verification Value Acceptable?
740
Transaction may be approved
745
Store additional data
750
Terminate
755

FIG. 7


Payment device generates dCVV
601
dCVV embedded into magnetic stripe data format
605
Magnetic stripe data transmit to POS terminal
610
POS terminal passes MS data on to service provider
615
Service provider receives MS data
620
630
Standard magnetic stripe processing
Contactless?
625
635
Is ATC in range?
640
Possible data skimming
Generate dCVV for the transaction
645
655
Transaction may be approved
dCVV acceptable?
650
Terminate
665
660
Store ATC