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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
13 April 2006 (13.04.2006)

PCT

(10) International Publication Number
WO 2006/039180 A2

(51) International Patent Classification: Not classified

(21) International Application Number: PCT/US2005/033986

(22) International Filing Date: 23 September 2005 (23.09.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

10/711,720	30 September 2004 (30.09.2004)	US
10/905,005	9 December 2004 (09.12.2004)	US

(71) Applicant (*for all designated States except US*): **AMERICAN EXPRESS MARKETING & DEVELOPMENT CORPORATION** [US/US]; World Financial Center, 200 Vesey Street, New York, NY 10285-4900 (US).

(72) Inventors; and

(75) Inventors/Applicants (*for US only*): **BISHOP, Fred** [US/US]; 5511 West Aster, Glendale, AZ 85304 (US). **SAUNDERS, Peter, D.** [US/US]; 3710 East Palisade Drive, Salt Lake City, UT 84109 (US).

(74) Agents: **WISCHHUSEN, Carl, B.** et al.; Fitzpatrick, Cella, Harper & Scinto, 30 Rockefeller Plaza, New York, NY 10112-3801 (US).

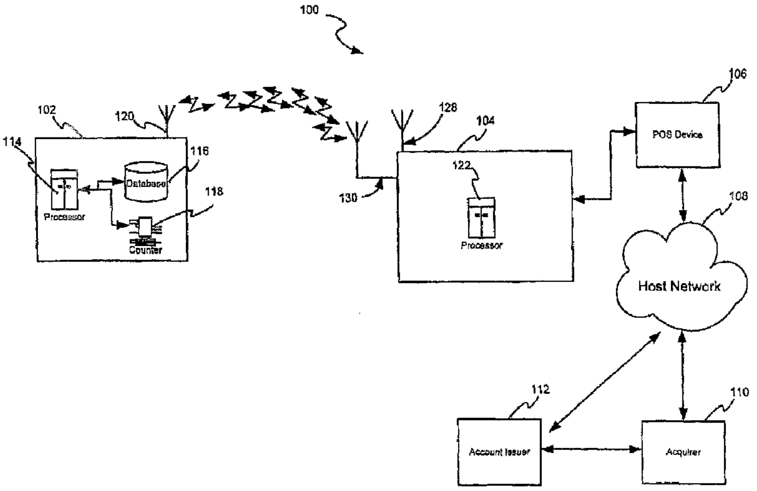
(81) Designated States (*unless otherwise indicated, for every kind of national protection available*): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, 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, 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, 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:
— *without international search report and to be republished upon receipt of that report*

[Continued on next page]

(54) **Title:** SYSTEM AND METHOD FOR AUTHENTICATING A RF TRANSACTION USING A RADIO FREQUENCY IDENTIFICATION DEVICE INCLUDING A TRANSACTIONS COUNTER



(57) **Abstract:** A system and method for securing a Radio Frequency (RF) transaction using a RF identification device (RFID) transaction device is provided. RFID transaction device includes a transactions counter for tallying the number of transactions attempted or completed with the RFID transactions device. Counter value is used to create a RFID device authentication tag for use in validating the RFID device. A RFID reader, interacting with the RFID device, provides a random number to the RFID device which may be used in the RFID device authentication tag creation and validation. RFID reader may also use counter value and random number to create a RFID reader authentication key useful for validating RFID reader. RFID transaction device may include an encryption key for creating RFID transaction device authentication tag. Likewise, RFID reader may include a RFID reader encryption key for creating RFID reader authentication tag.

WO 2006/039180 A2

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

Description

SYSTEM AND METHOD FOR AUTHENTICATING A RF TRANSACTION USING A RADIO FREQUENCY IDENTIFICATION DEVICE INCLUDING A TRANSACTIONS COUNTER

CROSS-REFERENCE TO RELATED APPLICATIONS

[Para 1] This invention is a continuation in part of and claims priority to U.S. Patent Application No. 10/711,720, titled "SYSTEMS AND METHODS FOR MANAGING MULTIPLE ACCOUNTS ON A RF TRANSACTION DEVICE USING SECONDARY IDENTIFICATION INDICIA," filed September 30, 2004. This invention is also a continuation-in-part of and claims priority to U.S. Patent Application No. 10/708,545, titled "SYSTEM AND METHOD FOR SECURING RF TRANSACTIONS USING A RADIO FREQUENCY IDENTIFICATION DEVICE INCLUDING A TRANSACTION COUNTER," filed March 10, 2004. Both the '720 and '545 applications claim priority to U.S. Provisional Application No. 60/507,803, filed September 30, 2003. This invention is also a continuation-in-part of and claims priority to U.S. Patent Application No. 10/340,352, entitled "SYSTEM AND METHOD FOR INCENTING PAYMENT USING RADIO FREQUENCY IDENTIFICATION IN CONTACT AND CONTACTLESS

TRANSACTIONS," filed January 10, 2003 (which itself claims priority to U.S. Provisional Patent Application No. 60/396,577, filed July 16, 2002), and is also a continuation-in-part and claims priority to U.S. Patent Application No. 10/192,488, entitled "SYSTEM AND METHOD FOR PAYMENT USING RADIO FREQUENCY IDENTIFICATION IN CONTACT AND CONTACTLESS TRANSACTIONS," filed on July 9, 2002 (which itself claims priority to U.S. Provisional Patent Application No. 60/304,216, filed July 10, 2001. All of the above-listed applications are incorporated herein by reference.

FIELD OF INVENTION

[Para 2] This invention generally relates to a system and method for securing a Radio Frequency (RF) transaction using a RF operable transaction device, and more particularly, to securing a RF transaction using a Radio Frequency Identification (RFID) device module including a transactions counter.

BACKGROUND OF INVENTION

[Para 3] Like barcode and voice data entry, RFID is a contactless information acquisition technology. RFID systems are wireless, and are usually extremely effective in hostile environments where conventional acquisition methods fail. RFID has established itself in a wide range of markets, such as, for example, the high-speed reading of railway containers, tracking moving objects such as livestock or automobiles, and retail inventory applications. As such, RFID technology has become a primary focus in automated data collection, identification and analysis systems worldwide.

[Para 4] Of late, companies are increasingly embodying RFID data acquisition technology in portable devices are identifiable by hand. For example, RFID modules are being placed in a fob or tag for use in completing financial transactions. A typical fob includes a RF transponder and is ordinarily a self-contained device which may be contained on any portable form factor. In some instances, a battery may be included with the fob to power the transponder, in which case the internal circuitry of the fob (including the transponder) may draw its operating power from the battery power source. Alternatively, the fob may exist independent of an internal power source. In this instance the internal circuitry of the fob (including the transponder) may gain its operating power directly from an RF interrogation signal provided by a RF reader. U.S. Patent No. 5,053,774, issued to Schuermann, describes a typical transponder RF interrogation system which may be found in the prior art. The Schuermann patent describes in general the powering technology surrounding conventional transponder structures. U.S. Patent No. 4,739,328 discusses a method by which a conventional transponder may respond to a RF interrogation signal. Other typical modulation techniques which may be used include, for example, ISO/IEC 14443 and the like.

[Para 5] In the conventional fob powering technologies used, the fob is typically activated upon presenting the fob in an interrogation signal. In this regard, the fob may be activated irrespective of whether the user desires such activation. These are called "passive" RFID devices. Alternatively, the fob may have an internal power source such that interrogation by the reader to activate the fob is not required. These RFID devices are termed "active" RFID devices.

[Para 6] One of the more visible uses of the RFID technology is found in the introduction of Exxon/Mobil's Speedpass® and Shell's EasyPay® products. These products use transponders placed in a fob or tag which enables automatic identification of the user when the fob is presented at a Point-of-Sale (POS) device. Fob identification data is typically passed to a third-party server database, where the identification data is referenced to a customer (*e.g.*, user) credit or debit account. In an exemplary processing method, the server seeks authorization for the transaction by passing the transaction and account data to an authorizing entity, such as for example an "acquirer" or account issuer. Once the server receives authorization from the authorizing entity, the authorizing entity sends clearance to the point-of-sale device for completion of the transaction.

[Para 7] Minimizing fraud transactions in the RFID environment is typically important to account issuer to lessen the loss associated with fraudulent RFID transaction device usage. One conventional method for securing RFID transactions involves requiring the device user to provide a secondary form of identification during transaction completion. For example, RFID transaction device user may be asked to enter a personal identification number (PIN) into a keypad. The PIN may then be verified against a number associated with the user or RFID transaction device, where the associated number is stored in an account issuer database. If the PIN number provided by the device user matches the associated number, then the transaction may be cleared for completion.

[Para 8] One problem with the conventional method of securing an RFID transaction is that the time for completing the transaction is increased. The increased time is typically due to the RFID device user delaying the transaction to provide the alternate identification. The increased time for completing a transaction defeats one of the real advantages of RFID transaction device, which is to permit expedient completion of a transaction since the account information may be passed to a reader without merchant involvement.

[Para 9] As such, a need exists for a method of securing a RFID transaction which does not increase the time needed to complete a transaction, and wherein the method may be used without device user intervention.

SUMMARY OF INVENTION

[Para 10] The invention includes a system and method for securing RFID transactions which addresses the problems found in conventional transaction securing methods. The securing method includes verifying a RFID transaction device counter, which may generate an indicia corresponding to the number of transactions conducted using a particular RFID transaction device. The method involves variously validating a RFID device authentication tag and a RFID reader authentication tag.

[Para 11] The invention discloses a system and method for verifying a RFID transaction device and RFID reader operable with a RF transaction system. An exemplary method involves presenting a RFID transaction system to a RFID reader, receiving a random number from RFID reader, creating a RFID transaction device authentication tag using the random number and a counter value, providing the random number, counter value, and RFID transaction device authentication tag to a RFID reader, creating a RFID reader authentication tag using counter random number, and RFID authentication tag, and providing RFID reader and RFID transaction device for authentication.

[Para 12] Under a second embodiment, the invention involves verifying RFID transaction device only. In another embodiment, the invention involves verifying RFID reader without verifying RFID transaction device.

[Para 13] These features and other advantages of the system and method, as well as the structure and operation of various exemplary embodiments of the system and method, are described below.

BRIEF DESCRIPTION OF THE DRAWINGS

[Para 14]

The accompanying drawings, wherein like numerals depict like elements, illustrate exemplary embodiments of the present invention, and together with the description, serve to explain the principles of the invention. In the drawings:

[Para 15] Figure 1 illustrates an exemplary RFID-based system depicting exemplary components for use in RFID transaction completion in accordance with the present invention;

[Para 16] Figure 2 illustrates an exemplary method for securing a RFID transaction using a counter-generated indicia in accordance with the present invention;

[Para 17] Figure 3 depicts a flow diagram of an exemplary RFID transaction device and RFID reader authentication flow chart useful with this invention;

[Para 18] Figure 4 depicts a flow diagram of an exemplary RFID transaction device authentication flow diagram useful with this invention; and

[Para 19] Figure 5 depicts a flow diagram of an exemplary RFID reader authentication flow diagram useful with this invention.

DETAILED DESCRIPTION

[Para 20]

The present invention may be described herein in terms of functional block components, screen shots, optional selections and various processing steps. Such functional blocks may be realized by any number of hardware and/or software components configured to perform to specified functions. For example, the present invention may employ various integrated circuit components (*e.g.*, memory elements, processing elements, logic elements, look-up tables, and the like), which may carry out a variety of functions under the control of one or more microprocessors or other control devices. Similarly, the software elements of the present invention may be implemented with any programming or scripting language such as C, C++, Java, COBOL, assembler, PERL, extensible markup language (XML), JavaCard and MULTOS with the various algorithms being implemented with any combination of data structures, objects, processes, routines or other programming elements. Further, it should be noted that the present invention may employ any number of conventional techniques for data transmission, signaling, data processing, network control, and the like. For a basic introduction on cryptography, review a text written by Bruce Schneier entitled "Applied Cryptography: Protocols, Algorithms, and Source Code in C," published by John Wiley & Sons (second edition, 1996), herein incorporated by reference.

[Para 21] In addition, many applications of the present invention could be formulated. The exemplary network disclosed herein may include any system for exchanging data or transacting business, such as the Internet, an intranet, an extranet, WAN, LAN, satellite communications, and/or the like. It is noted that the network may be implemented as other types of networks, such as an interactive television network (ITN).

[Para 22] Further still, the terms "Internet" or "network" may refer to the Internet, any replacement, competitor or successor to the Internet, or any public or private inter-network, intranet or extranet that is based upon open or proprietary protocols. Specific information related to the protocols, standards, and application software utilized in connection with the Internet may not be discussed herein. For further information regarding such details, see, for example, Dilip Naik, Internet Standards and Protocols (1998); Java 2 Complete, various authors, (Sybex 1999); Deborah Ray and Eric Ray, Mastering HTML 4.0 (1997); Loshin, TCP/IP Clearly Explained (1997). All of these texts are hereby incorporated by reference.

[Para 23] By communicating, a signal may travel to/from one component to another. The components may be directly connected to each other or may be connected through one or more other devices or components. The various coupling components for the devices can include but are not limited to the Internet, a wireless network, a conventional wire cable, an optical cable or connection through air, water, or any other medium that conducts signals, and any other coupling device or medium.

[Para 24] Where required, the system user may interact with the system via any input device such as, a keypad, keyboard, mouse, kiosk, personal digital assistant, handheld computer (*e.g.*, Palm Pilot®, Blueberry®), cellular phone and/or the like). Similarly, the invention could be used in conjunction with any type of personal computer, network computer, work station, minicomputer, mainframe, or the like running any operating system such as any version of Windows, Windows NT, Windows 2000, Windows 98, Windows 95, MacOS, OS/2, BeOS, Linux, UNIX, Solaris or the like. Moreover, although the invention may frequently be described as being implemented with TCP/IP communications protocol, it should be understood that the invention could also be implemented using SNA, IPX, Appletalk, IPte, NetBIOS, OSI or any number of communications protocols. Moreover, the system contemplates the use, sale, or distribution of any goods, services or information over any network having similar functionality described herein.

[Para 25] A variety of conventional communications media and protocols may be used for data links providing physical connections between the various system components. For example, the data links may be an Internet Service Provider (ISP) configured to facilitate communications over a local loop as is typically used in connection with standard modem communication, cable modem, dish networks, ISDN, Digital Subscriber Lines (DSL), or any wireless communication media. In addition, the merchant system including the POS device 106 and host network 108 may reside on a local area network which interfaces to a remote network (not shown) for remote authorization of an intended transaction. POS 106 may communicate with the remote network via a leased line, such as a T1, D3 line, or the like. Such communications lines are described in a variety of texts, such as, “Understanding Data Communications,” by Gilbert Held, which is incorporated herein by reference.

[Para 26] A transaction device identifier, as used herein, may include any identifier for a transaction device which may be correlated to a user transaction account (*e.g.*, credit, charge debit, checking, savings, reward, loyalty, or the like) maintained by a transaction account provider (*e.g.*, payment authorization center). A typical transaction account identifier (*e.g.*, account number) may be correlated to a credit or debit account, loyalty account, or rewards account maintained and serviced by such entities as American Express, Visa and/or MasterCard, or the like.

[Para 27] To facilitate understanding, the present invention may be described with respect to a credit account. However, it should be noted that the invention is not so limited and other accounts permitting an exchange of goods and services for an account data value is contemplated to be within the scope of the present invention.

[Para 28] A transaction device identifier may be, for example, a sixteen-digit credit card number, although each credit provider has its own numbering system, such as the fifteen-digit numbering system used by American Express. Each company's credit card numbers comply with that company's standardized format such that the company using a sixteen-digit format will generally use four spaced sets of numbers, as represented by the number "0000 0000 0000 0000". In a typical example, the first five to seven digits are reserved for processing purposes and identify the issuing bank, card type and, etc. In this example, the last sixteenth digit is used as a sum check for the sixteen-digit number. The intermediary eight-to-ten digits are used to uniquely identify the customer. The account number stored as Track 1 and Track 2 data as defined in ISO/IEC 7813, and further may be made unique to RFID transaction device.

[Para 29] In one exemplary embodiment, transaction device identifier may include a unique RFID transaction device serial number and user identification number, as well as specific application applets. Transaction device identifier may be stored on a transaction device database located on transaction device. Transaction device database may be configured to store multiple account numbers issued to RFID transaction device user by the same or different account providing institutions. In addition, where the device identifier corresponds to a loyalty or rewards account, RFID transaction device database may be configured to store the attendant loyalty or rewards points data.

[Para 30] The merchant database locations maintained on database 116 by server 110 are provided a distinct merchant identifier. Database discussed herein may be a graphical, hierarchical, relational, object-oriented or other database, and may be maintained on a local drive of a server or on a separate computer coupled to the server via a local area or other network (not shown). In one embodiment, databases disclosed are a collection of ASCII or other text files stored on a local drive of server. Database information is suitably retrieved from the database and provided to transaction processing systems upon request via a server application, as described more fully below.

[Para 31] In addition to the above, transaction device identifier may be associated with any secondary form of identification configured to allow the consumer to interact or communicate with a payment system. For example, transaction device identifier may be associated with, for example, an authorization/access code, personal identification number (PIN), Internet code, digital certificate, biometric data, and/or other secondary identification data used to verify a transaction device user identity.

[Para 32] It should be further noted that conventional components of RFID transaction devices may not be discussed herein for brevity. For instance, one skilled in the art will appreciate that RFID transaction device and RFID reader disclosed herein include traditional transponders, antennas, protocol sequence controllers, modulators/demodulators and the like, necessary for proper RFID data transmission. As such, those components are contemplated to be included in the scope of the invention.

[Para 33] It should be noted that the transfer of information in accordance with this invention, may be done in a format recognizable by a merchant system or account issuer. In that regard, by way of example, the information may be transmitted in magnetic stripe or multi-track magnetic stripe format. Because of the proliferation of devices using magnetic stripe format, the standards for coding information in magnetic stripe format were standardized by the International Standards Organization (ISO).

[Para 34] Typically, magnetic stripe information is formatted in three tracks. Certain industry information must be maintained on certain portion of the tracks, while other portions of the tracks may have open data fields. The contents of each track and the formatting of the information provided to each track is controlled by ISO standard ISO/IEC 7811. For example, the information must typically be encoded in binary. Track 1 is usually encoded with user information (name) in alphanumeric format. Track 2 is typically comprised of discretionary and non-discretionary data fields. In one example, the non-discretionary field may comprise 19 characters and the discretionary field may comprise 13 characters. Track 3 is typically reserved for financial transactions and includes enciphered versions of the user's personal identification number, country code, currently units amount authorized per cycle, subsidiary accounts, and restrictions.

[Para 35] As such, where information is provided in accordance with this invention, it may be provided in magnetic stripe format track. For example, counter values, authentication tags and encrypted identifiers, described herein, may be forwarded encoded in all or a portion of a data stream representing data encoded in, for example, track 2 or track 3 format.

[Para 36] Further still, various components may be described herein in terms of their "validity." In this context, a "valid" component is one which is authorized for use in completing a transaction request in accordance with the present invention. Contrarily, an "invalid" component is one which is not authorized for transaction completion. In addition, an invalid component may be one which is not recognized as being permitted for use on the secure RF system described herein.

[Para 37] Figure 1 illustrates an exemplary secure RFID transaction system 100 in accordance with the present invention, wherein exemplary components for use in completing a RF transaction are depicted. In general, system 100 may include a RFID transaction device 102 in RF communication with a RFID reader 104 for transmitting data there between. RFID reader 104 may be in further communication with a merchant point-of-sale (POS) device 106 for providing to POS 106 data received from RFID transaction device 102. POS 106 may be in further communication with an acquirer 110 or an account issuer 112 via host network 108 for transmitting a transaction request, including information received from RFID reader 104, and receiving authorization concerning transaction completion.

[Para 38] Although the point-of-interaction device (POS) is described herein with respect to a merchant point-of-sale (POS) device, the invention is not to be so limited. Indeed, a merchant POS device is used herein by way of example, and the point-of-interaction device may be any device capable of receiving transaction device account data. In this regard, the POS may be any point-of-interaction device enabling the user to complete a transaction using a transaction device 102. POS device 106 may receive RFID transaction device 102 information and provide the information to host network 108 for processing.

[Para 39] As used herein, an “acquirer” may be a third-party entity including various databases and processors for facilitating the routing of the transaction request to an appropriate account issuer 112. Acquirer 110 may route the request to account issuer in accordance with a routing number provided by RFID transaction device 102. The “routing number” in this context may be a unique network address or any similar device for locating an account issuer 112 on host network 108. Traditional means of routing the payment request in accordance with the routing number are well understood. As such, the process for using a routing number to provide the payment request will not be discussed herein for brevity.

[Para 40]

Additionally, account issuer 112 (“account provider” or “issuer system”) may be any entity which provides a transaction account for facilitating completion of a transaction request. The transaction account may be any credit, debit, loyalty, direct debit, checking, or savings, or the like. The term “issuer” or “account provider” may refer to any entity facilitating payment of a transaction using a transaction device, and which includes systems permitting payment using at least one of a preloaded and non-preloaded transaction device. Typical issuers may be American Express, MasterCard, Visa, Discover, and the like. In the preloaded value processing context, an exchange value (*e.g.*, money, rewards points, barter points, etc.) may be stored in a preloaded value database (not shown) for use in completing a requested transaction. The preloaded value database and thus the exchange value may not be stored on transaction device itself, but may be stored remotely, such as, for example, at account issuer 112 location. Further, the preloaded value database may be debited the amount of the transaction requiring the value to be replenished. The preloaded value may be any conventional value (*e.g.*, monetary, rewards points, barter points, etc.) which may be exchanged for goods or services. In that regard, the preloaded value may have any configuration as determined by issuer system 112.

[Para 41] In general, during operation of secure system 100, RFID reader 104 may provide an interrogation signal to transaction device 102 for powering device 102 and receiving transaction device related data. The interrogation signal may be received at a transaction device antenna 120 and may be further provided to a transponder (not shown). In response, a transaction device processor 114 may retrieve a transaction device identifier from a transaction device database 116 for providing to RFID reader 104 to complete a transaction request. Typically, transaction device identifier may be encrypted prior to providing the device identifier to a modulator/demodulator (not shown) for providing the identifier to RFID reader 104.

[Para 42] It should be noted that RFID reader 104 and RFID transaction device 102 may engage in mutual authentication prior to transferring any transaction device 102 data to RFID reader 104. For a detailed explanation of a suitable mutual authentication process for use with the invention, please refer to commonly owned U.S. Patent

Application No. 10/340,352, entitled "SYSTEM AND METHOD FOR INCENTING PAYMENT USING RADIO FREQUENCY IDENTIFICATION IN CONTACT AND CONTACTLESS TRANSACTIONS," filed January 10, 2003, incorporated by reference in its entirety.

[Para 43] In accordance with one embodiment of the present invention, a RF transaction using a RFID transaction device is secured by limiting the number of transactions which may be performed with a particular transaction device. Once the maximum transactions value is reached, transaction device may automatically disable itself against further usage. Alternatively, account issuer 112 may flag the transaction account correlating to transaction device such that account issuer system automatically prevents completion of transactions using transaction device

[Para 44] As such, RFID transaction device 102 in accordance with the present invention further includes a counter 118 for recording and reporting the number of transactions performed with a particular transaction device 102. Counter 118 may be any device capable of being initiated with a beginning value and incrementing that value by a predetermined amount when transaction device 102 is presented for completion of a transaction. Counter 118 may be a discrete electronic device on the transponder, or may be software or code based counter as is found in the art.

[Para 45] The initial counter value may be any value from which other similar values may be measured. The value may take any form, such as, alpha, numeric, a formation of symbols, or any combination thereof.

[Para 46] To facilitate understanding, the following description discusses all values to be in numeric units (0, 1, 2, 3...n). Thus, counter values, the value amount to be incremented, the total transactions counted value, and the maximum transactions value, are all whole numbers.

[Para 47] It should be noted that account issuer 112 may preset the initial counter value at any initial value as desired. Account issuer 112 may also predetermine the value amount to be incremented by counter 118 when transaction device is used to complete a transaction. Further, account issuer 112 may assign different values to be incremented for each distinct transaction device 102. Further still, account issuer 112 may determine the maximum transactions value, which may be particular to each individual transaction device 102 issued by account issuer 112. Where counter 118 value equals a maximum transactions value, the system 100 prevents the usage of transaction device 102 to complete additional transactions. Account issuer 112 may prevent the usage of transaction device 102 where account issuer flags the transaction account corresponding to transaction device 102, thereby preventing authorization for using the account to complete transactions. Alternatively, transaction device 102 may self-disable. For example, counter 118 value may trigger transaction device processor 114 to provide a signal for preventing the transfer of transaction device 102 identifier.

[Para 48] For example, account issuer 112 may preset the initial counter value at 5 units and counter value to be incremented at 10 units per transaction. Account issuer 112 may determine that transaction device 102 may be used to complete a total transaction value of 20 transactions. Since counter 118 increments counter value by the value to be incremented (*e.g.*, 10 units) for each transaction, then for a total of 20 transactions permitted, the maximum transactions value will be 205 units. Once counter value equals 205 units, then the operation of transaction device 102 may be disabled.

[Para 49] The operation of the exemplary embodiment described above, may be understood with reference to Figure 1 and to the method of securing a RFID transaction described in Figure 2. The operation may begin when RFID transaction device 102 is presented for completion of a transaction. Transaction device 102 may be placed in an interrogation field generated by RFID reader 104 (step 202). RFID reader 104 may interrogate RFID transaction device 102 enabling transaction device 102 operation. In response, RFID transaction device 102 may retrieve transaction device 102 identifier, account issuer 112 routing number and encrypted transaction device identifier from database 116 for providing to RFID reader 104 (step 204).

[Para 50] Once RFID transaction device 102 detects the interrogation signal provided by RFID reader 104, counter 118 may increment its counter value (step 206). Counter 118 value may be incremented by an amount predetermined by account issuer 112 (*e.g.*, value amount to be incremented). The resulting counter 118 value after incrementing is the total transactions counted value.

[Para 51] Upon determining the total transactions counted value, RFID transaction device 102 may provide the total transactions counted value, the encrypted transaction device 102 identifier, and account issuer 112 routing number to RFID reader 104 via RF transmission (step 208). RFID reader 104 may, in turn, convert transaction device 102 identifier, routing number, and total transactions counted value into merchant POS recognizable format and forward the converted information to merchant POS 106 (step 210). A merchant system, including POS 106, may then provide a transaction request to acquirer 110 via network 106. The transaction request may include the information received from transaction device 102 along with information (*e.g.*, amount, number of product, product/service identifier) concerning the transaction requested to be completed (step 216). The transaction request may include information relative to RFID reader 104.

[Para 52] Acquirer 110 may receive the transaction request and forward the transaction request to the appropriate account issuer 112 in accordance with the routing number provided (step 218). Account issuer 112 may then identify that a transaction request is being provided that relates to a transaction device. For example, merchant POS 106 may provide a code appended to the transaction request specially configured for identifying a transaction device transaction which may be recognized by account issuer 112. Alternatively, transaction device identifier, or a portion thereof, may be identified by account issuer 112 as originating with a RFID transaction device 102.

[Para 53] In one exemplary embodiment, account issuer 112 receives the transaction device 102 identifier and checks to see if the transaction device identifier corresponds to a valid transaction account maintained on account issuer 112 system (step 220). For example, account issuer 112 may receive the encrypted transaction device identifier and locate the corresponding decryption key relating to the transaction account. If the encrypted identifier is invalid, such as, for example, when account issuer 112 is unable to locate the corresponding decryption key, account issuer 112 may provide a "Transaction Invalid" message to POS 106 (step 228). Transaction device 102 user may then be permitted to provide an alternate means of satisfying the transaction, or the transaction is ended (step 230).

[Para 54] If the RFID transaction device 102 encrypted identifier corresponding decryption key is located, the encrypted identifier is considered "valid" and account issuer 112 may then use the corresponding decryption key to "unlock" or locate transaction device account correlative to transaction device 102. Account provider 112 may then retrieve all information relating to the usage limits which have been predetermined by account issuer 112. Account issuer 112 may be able to determine if a particular transaction device 102 has reached its limit of available transactions.

[Para 55] For example, account issuer 112 may check to see if the total transactions counted value equals or exceeds the maximum transactions allowed (step 224). If the maximum transactions allowed have been reached then counter value is met or exceeded, and the transaction is considered "invalid." As such, account issuer 112 may then provide a "Transaction Invalid" message to POS 106 (step 228). In addition, account issuer 112 may determine whether the total transactions counted value is the next expected value. If not, then the transaction is considered "invalid" and account issuer 112 may also provide a "Transaction Invalid" message to POS 106 (step 228). The transaction device 102 user may then be permitted to provide alternate means of completing the transaction (step 226) or the transaction is ended.

[Para 56] Alternatively, where the total transactions counted value does not exceed or meet the maximum transactions allowed value, counter value is considered valid and a "Transaction Valid" message is sent to merchant POS 106 (step 230). The merchant system may then complete the transaction under business as usual standards as are employed by the merchant.

[Para 57] In accordance with the various embodiments described, the present invention addresses the problem of securing a RF transaction completed by a RFID transaction device. The invention provides a *system and method for an account issuer to determine if RFID* transaction device is a valid device for completing a transaction on a

RF transaction system. Account issuer can determine whether transaction device is valid by verifying transaction device counter, and encryption identifier. It should be noted, however, that the present invention contemplates various arrangements wherein RFID reader may also be validated.

[Para 58] Figure 3 illustrates another method 300 for usage of RFID transaction device counter 118 value for securing a RF transaction. In accordance with the method depicted, RFID reader 104 includes a random number generator 120, for producing a random number to be used in secure transactions. Random number generator 120 may be any conventional random number generator as is found in the art.

[Para 59] Method 300 may begin when a user presents RFID transaction device 102 for transaction completion (step 302). The user may, for example, place RFID transaction device 102 into the interrogation zone provided by RFID reader 104. The interrogation zone may be the area or zone defined by the interrogation signal cast by RFID reader 104.

[Para 60] Upon presentment of transaction device 102, RFID reader 104 may provide the random number to RFID transaction device 102 (step 304). RFID transaction device 102 may receive the random number and use it to create a RFID transaction device authentication tag (step 306). RFID transaction device 102 may receive the random number and use the random number, counter value, transaction account number and RFID transaction device encryption key to create a RFID transaction device authentication tag.

[Para 61] RFID transaction device 102 may provide RFID transaction device authentication tag to RFID reader 104. RFID transaction device 102 may also provide in-the-clear data, counter value, random number to RFID reader 104, along with RFID transaction device authentication tag (step 308). RFID transaction device processor 114 may increment counter 118 using any of the incrementing methods discussed above (step 310).

[Para 62] RFID reader 104 may receive the data provided by RFID transponder 102, and use the data to create a RFID reader authentication key using a RFID reader encryption key (step 312). RFID reader 104 may use the transaction data and RFID reader 104 encryption key to encrypt the authentication tag created by the RF transaction device using common techniques such as DES and Triple DES and pass the modified authentication tag together with the in-the-clear data, random number, counter value, modified RFID transaction device authentication tag, and RFID reader authentication tag into a format readable by POS 106 (step 314) and provide the converted data to POS 106 (step 316).

[Para 63] In an alternate embodiment, RFID reader 104 may receive the data provided by RFID transaction device 102, and use the data to create a RFID reader authentication key using a RFID reader encryption key (step 312). The reader authentication key is a digital signature created using the reader encryption key, RFID transaction device transaction data, and reader random number. RFID reader 104 may then pass the transaction data provided by the RF transaction device plus the reader authentication tag to POS 106.

[Para 64] POS 106 may seek satisfaction of the transaction (step 318). For example, POS 106 may form a transaction request using the data received from RFID transaction device 102, and RFID reader 104 encryption key and forward the transaction request to acquirer 110 who may forward the transaction request to account issuer 112 using the routing number.

[Para 65] Account issuer 112 may receive the transaction request and verify that RFID reader 104 and RFID transmission device 102 are valid. Account issuer 112 may validate RFID reader authentication tag by decrypting RFID reader authentication tag using a RFID reader encryption key stored on an account issuer database (not shown) (step 320). If the decryption is unsuccessful, then issuer system 112 may provide a "Transaction Invalid" message to POS 106 (step 322) and the transaction is terminated. Alternatively, if decryption is successful, issuer system 112 may seek to validate RFID transaction device authentication tag (step 332).

[Para 66] For example, account issuer 112 may use the RF transaction device account number to locate a RFID transaction device encryption key stored on the issuer 112 (step 324) database and use RFID transaction device encryption key to decrypt RFID transaction device authentication tag (step 326). If decryption is unsuccessful then issuer system 112 provides a "Transaction Invalid" message to POS 106 (step 322) and the transaction is terminated. Alternatively, if the decryption is successful, then issuer system 112 may validate counter value (step 328). Issuer system 112 may compare counter value to an expected counter value. In another exemplary embodiment, issuer system 112 may subject counter value received from RFID transaction device 102 to an algorithm the results of which are validated against an expected counter value. Issuer system 112 determines the expected value by referencing the algorithm used to increment counter value. For example, RFID transaction device 102 may have an algorithm (*e.g.*, "counter algorithm") stored on transaction device database which may be used to increment counter value. In an exemplary embodiment, issuer system 112, stores a substantially similar copy of counter algorithm on issuer system 112 which is used to determine an expected counter value based on transactions known to issuer system 112. In some instances, the expected counter value and counter value are not the same. That is, there may be differences due to, for example, transactions being processed off-line using RFID transaction device 102. By "off-line" what may be meant is that the transaction is not immediately reported to issuer system 112. Instead, the transaction may be approved for processing without prior approval from issuer system 112, and issuer system 112 is notified of the transaction at a later date (*e.g.*, not in real-time). In this case, counter algorithm may be such that a valid value is a value within an expected error range.

[Para 67] If counter value is unsuccessfully validated, then issuer system 112 may provide a 'Transaction Invalid" message to POS 106. Otherwise, issuer system 112 may process the RFID transaction account number under business as usual standards (step 330). In this way, the transaction is secured using a counter, by using counter to validate a RFID transaction device authentication tag and a RFID reader authentication tag.

[Para 68] Figure 4 illustrates another exemplary embodiment wherein RFID transaction device 102 is validated using counter value. In this exemplary embodiment, RFID transaction device 102 is presented (step 302) and RFID reader 104 sends a random number to RFID transaction device 102 (step 304). RFID transaction device 102 receives the random number and creates a RFID transaction device authentication tag using the random number, the in-the-clear data, and a counter value (step 306). RFID transaction device 102 may then provide RFID transaction device authentication tag, random number, counter value, and in-the-clear data to RFID reader 104 (step 308). RFID transaction device 102 may increment counter value by a predetermined value (step 310).

[Para 69] RFID reader 104 may receive RFID transaction device authentication tag, in-the-clear data and counter value and convert counter value, in-the-clear data and RFID transaction device authentication tag to a merchant POS 106 format (step 414). RFID reader 104 may then provide the converted data to POS 106 (step 316). Merchant POS 106 may then provide the data received from RFID reader 104 to issuer system 112 for transaction satisfaction (step 318). Issuer system 112 may receive the data and verify RFID transaction device authentication tag (step 332). For example, issuer system 112 may validate the RFID transaction authentication tag and counter value in accordance with steps 324-328.

[Para 70] Under yet another embodiment, Figure 5 illustrates an aspect of the invention wherein RFID reader 104 is validated, when RFID transaction device 102 is not. According to the invention RFID transaction device 102 is validated using counter value. In this exemplary embodiment, RFID transaction device 102 is presented for transaction completion (step 302). RFID transaction device 102 may then provide counter and the in-the-clear data to RFID reader 104 (step 508). RFID transaction device 102 may increment counter value by a predetermined value (step 310). Alternatively, RFID reader 104 may provide a signal to transaction device 102 for use in incrementing the counter value.

[Para 71] RFID reader 104 may receive the in-the-clear data and counter value and prepare RFID reader authentication tag using a RFID reader encryption key (step 512). RFID reader may then convert the in-the-clear data and RFID reader authentication tag to a merchant POS 106 format (step 514) and provide the converted data to POS 106 (step 316). The merchant POS 106 may then provide the data received from RFID reader 104 to an issuer system 112 for transaction satisfaction (step 318). In one exemplary embodiment, the merchant POS 106 provides issuer system 116 with a POS identifier associated with POS 106 (step 519). Issuer system 116 may then seek to verify RFID reader 104 (step 532). For example, issuer system 112 may receive the POS identifier, and locate a related POS encryption key stored on an issuer system database (step 524). Issuer system 112 may receive the encryption key data and verify RFID reader authentication tag using the POS encryption key data (step 526). For example, issuer system 112 may validate the RFID transaction authentication tag by attempting to decrypt RFID reader authentication tag using the POS encryption key (*i.e.*, step 526). If RFID reader authentication tag is successfully decrypted, then the transaction may be processed under business as usual standards (step 330). In another exemplary embodiment, prior to processing the transaction request (step 330), issuer system 112 may further verify RFID reader 104 by verifying counter value used to create the RFID authentication tag (step 528), in similar manner as was done with step 328.

[Para 72]

The preceding detailed description of exemplary embodiments of the invention makes reference to the accompanying drawings, which show the exemplary embodiment by way of illustration. While these exemplary embodiments are described in sufficient detail to enable those skilled in the art to practice the invention, it should be understood that other embodiments may be realized and that logical and mechanical changes may be made without departing from the spirit and scope of the invention. For example, RFID reader may include an RFID reader encrypted identifier stored in the reader database, which may be validated by account issuer in similar manner as with transaction device encrypted identifier. Moreover, counter may increment the total transactions counted value by the predetermined incremental value at the completion of a successful transaction. In addition, the steps recited in any of the method or process claims may be executed in any order and are not limited to the order presented. Further, the present invention may be practiced using one or more servers, as necessary. Thus, the preceding detailed description is presented for purposes of illustration only and not of limitation, and the scope of the invention is defined by the preceding description, and with respect to the attached claims.

What is claimed is:

[Claim 1] A method for securing a radio frequency (RF) transaction comprising:
receiving a RF reader authentication tag, a transaction account number, a RF transaction device authentication tag, and a RF transaction device counter value;
verifying the RF reader authentication tag, RF transaction device authentication tag, and RF transaction device counter value;
processing a transaction request, wherein the RF transaction device authentication tag, RF reader authentication tag, and RF transaction device counter value are verified, the RF transaction device authentication tag being produced using a RF transaction device encryption key, the RF transaction device counter value, the transaction account number, and a random number, where the RF transaction device encryption key, the RF transaction device counter value, and the transaction account number are provided by a RF transaction device and the random number is provided by a RF reader, and
wherein the RF reader authentication tag is produced using the RF transaction device authentication tag, the RF transaction device counter value, the random number, and transaction account number.

[Claim 2] A method of claim 1 comprising locating a RF reader encryption key using a merchant Point-of-Sale (POS) identifier.

[Claim 3] A method of claim 1 comprising receiving a converted RF reader authentication tag, converted RF transaction device authentication tag, converted RF transaction device counter value, converted random number, and converted transaction number, where the conversion is done in accordance with a merchant POS recognized format.

[Claim 4] A method of claim 3 comprising reproducing the RF reader authentication tag, the transaction account number, counter value, the random number and the RF transaction device authentication tag from the RF reader authentication tag using the RF reader encryption key.

[Claim 5] A method of claim 4 where the RF transaction device authentication tag is verified using a corresponding RF transaction device encryption key, the corresponding RF transaction device encryption key corresponding to the RF transaction device encryption key.

[Claim 6] A method of claim 5 where counter value is verified by comparing counter value to an expected counter value.

[Claim 7] A method of claim 6, where the transaction account number, transaction account expiration date, RF transaction device encryption key, and a RF transaction device counter for providing counter value are included on a RF transaction device when the RF transaction device is manufactured.

[Claim 8] A method of claim 6, where counter value is a value incremented by a random amount from a counter beginning value.

[Claim 9] A method of claim 6, where counter value is a value incremented by a predetermined amount from a counter beginning value.

[Claim 10] A method for facilitating securing a radio frequency transaction comprising:

receiving a RF transaction device authentication tag, a transaction account number, a transaction account expiration date, and a RF transaction device counter value;

verifying the RF transaction device authentication tag using a corresponding RF transaction device encryption key, the corresponding RF transaction device encryption key corresponding to a RF transaction device encryption key referenced to a RF transaction device;

verifying the RF transaction device counter value; and

processing a transaction request wherein the RF transaction device authentication tag and the RF transaction device counter is verified, the RF transaction device authentication tag being produced using the RF transaction device encryption key, a random number, the RF transaction device counter value and the transaction account number, where the RF transaction device encryption key, the RF transaction device counter value, and the transaction account number are provided by a RF transaction device, and

wherein the random number is provided by a RF reader.

[Claim 11] A method of claim 10 comprising receiving a converted RF transaction device authentication tag, converted RF transaction device counter value, converted random number, and converted transaction number, where the conversion is done in accordance with a merchant POS recognized format.

[Claim 12] A method of claim 11 where counter value is verified by comparing counter value to an expected counter value.

[Claim 13] A method of claim 12, where the transaction account number, transaction account expiration date, RF transaction device encryption key, and RF transaction device counter for providing counter value are included on the RF transaction device when the RF transaction device is manufactured.

[Claim 14] A method of claim 12, where counter value is a value incremented by a random amount from a counter beginning value.

[Claim 15] A method of claim 12, where counter value is a value incremented by a predetermined amount from a counter beginning value.

[Claim 16] A method for facilitating securing a radio frequency (RF) transaction comprising:

receiving a RF reader authentication tag, a transaction account number, and a merchant POS encryption key;

verifying the RF reader authentication tag using the merchant POS encryption key; and

processing a transaction request where the RF reader authentication tag is verified, the RF reader authentication tag being produced using a RF transaction device counter value, a RF reader encryption key, and transaction account number, where the RF transaction device counter value and the transaction account number is provided by a RF transaction device, and the RF reader encryption key is provided by a RF reader.

[Claim 17] A method of claim 16 comprising verifying the RF reader authentication tag using the merchant POS encryption key, the merchant POS encryption key being provided by a merchant POS.

[Claim 18] A method of claim 17, where the transaction account number and a RF transaction device counter for providing counter value are included on the RF transaction device when the RF transaction device is manufactured.

[Claim 19] A method of claim 17, where counter value is a value incremented by a random amount from a counter beginning value.

[Claim 20] A method of claim 17, where counter value is a value incremented by a predetermined amount from a counter beginning value.

[Claim 21] A system configured to facilitate securing a RF transaction comprising:

a. RF transaction device, said RF transaction device including:

i. a RF transaction device database configured to store transaction account number, transaction account expiration date, RF transaction device encryption key;

ii. a RF transaction device counter, said counter having a counter value;

iii. a RF transaction device processor configured to increment said counter value; and

iv. a RF transponder configured to transmit said transaction account number, transaction account expiration date, RF transaction device encryption key and counter value;

b. a RFID reader in RF communication with said RF transaction device configured to receive said transaction account number, transaction account expiration date, RF transaction device encryption key, and said counter value, said RFID reader including a random number generator for generating a random number, said RFID reader configured to provide said random number to said RF transaction device;

c. a merchant point of sale (POS) in communication with said RFID reader, said merchant POS including a merchant POS identifier,

i. said RF transaction device configured to receive said random number and produce a RF transaction device authentication tag using the RF transaction device encryption key, said random number, said counter value and said RF transaction device encryption key, said RF transaction device configured to provide said RF transaction device authentication tag, RF transaction device encryption key, said random number, said counter value and said RF transaction device encryption key to said RFID reader, said RFID reader configured to produce a RFID reader authentication tag using said RF transaction device authentication tag, said random number, said counter value and said transaction account number, said RFID reader configured to convert said RF transaction device authentication tag, RF transaction device encryption key, said random number, said counter value and said transaction account number to a merchant POS recognizable format; and

d. an issuer system in communication with said merchant POS, said issuer system configured to locate a RFID reader encryption key using said merchant POS identifier, rehash from said RFID reader authentication tag, the transaction account number, counter value, random number, and said RF transaction device authentication tag using said RFID reader encryption key, verify said RF transaction device authentication tag using a corresponding RF transaction device encryption key, and verify said counter value, and to process a transaction request where said RFID reader authentication tag, said RF transaction device authentication tag, and said counter value are verified.

[Claim 22] A system configured to facilitate securing a RF transaction comprising:

a. a RF transaction device, said RF transaction device including:

i. a RF transaction device database configured to store transaction account number, transaction account expiration date, RF transaction device encryption key;

ii. a RF transaction device counter, said counter having a counter value;

iii. a RF transaction device processor configured to increment said counter value; and

iv. a RF transponder configured to transmit said transaction account number, transaction account expiration date, RF transaction device encryption key and counter value;

b. a RFID reader in RF communication with said RF transaction device configured to receive said transaction account number, transaction account expiration date, RF transaction device encryption key, and said counter value, said RFID reader including a random number generator for generating a random number, said RFID reader configured to provide said random number to said RF transaction device;

c. a merchant point of sale (POS) in communication with said RFID reader, said merchant POS including a merchant POS identifier, said RF transaction device configured to receive said random number and produce a RF transaction device authentication tag using the RF transaction device encryption key, said random number, said counter value and said RF transaction device encryption key, said RF transaction device configured to provide said RF transaction device authentication tag, RF transaction device encryption key, said random number, said counter value and said RF transaction device encryption key to said RFID reader, said RFID reader configured to convert said RF transaction device authentication tag, RF transaction device encryption key, said random number, said counter value and said transaction account number to a merchant POS recognizable format; and

d. an issuer system in communication with said merchant POS, said issuer system configured verify said RF transaction device authentication tag using a using a corresponding RF transaction device encryption key, and verify said counter value, and process a transaction request where said RF transaction device authentication tag and said counter value are verified.

[Claim 23] A system configured to facilitate securing a RF transaction comprising:

a. a RF transaction device, said RF transaction device including:

i. a RF transaction device database configured to store transaction account number, and a transaction account expiration date;

ii. a RF transaction device counter, said counter having a counter value;

iii. a RF transaction device processor configured to increment said counter value; and

iv. a RF transponder configured to transmit said transaction account number, transaction account expiration date, and counter value;

b. a RFID reader in RF communication with said RF transaction device configured to receive said transaction account number, transaction account expiration date, and said counter value;

c. a merchant point of sale (POS) in communication with said RFID reader, said merchant POS including a merchant POS encryption key, said RF transaction device configured to receive said random number and said RF transaction device configured to provide said RF transaction device authentication tag, RF transaction device encryption key, said random number, said counter value to said RFID reader, said RFID reader configured to produce a RFID reader authentication tag using a RFID reader encryption key, said RFID reader configured to convert, RFID authentication tag, said random number, said counter value and said transaction account number to a merchant POS recognizable format; and

d. an issuer system in communication with said merchant POS, said issuer system configured to locate a RFID reader encryption key using said merchant POS encryption key, verify said RFID reader authentication tag using said merchant POS encryption key, and verify said counter value, and to process a transaction request where said RFID reader authentication tag and said counter are verified.

[Claim 24] A computer-readable storage medium containing a set of instructions for a general purpose computer configured for:

receiving a RF reader authentication tag, a transaction account number, a RF transaction device authentication tag, and a RF transaction device counter value;

verifying the RF reader authentication tag, RF transaction device authentication tag, and RF transaction device counter value; and

processing a transaction request where the RF transaction device authentication tag, RF reader authentication tag, and RF transaction device counter value are verified, the RF transaction device authentication tag being produced using a RF transaction device encryption key, the RF transaction device counter value, the transaction account number, and a random number, where the RF transaction device encryption key, the RF transaction device counter value, and the transaction account number are provided by a RF transaction device and the random number is provided by a RF reader, and

wherein the RF reader authentication tag is produced using the RF transaction device authentication tag, the RF transaction device counter value, the random number, and transaction account number.

[Claim 25] A computer-readable storage medium containing a set of instructions for a general purpose computer configured for:

receiving a RF transaction device authentication tag, a transaction account number, a transaction account expiration date, and a RF transaction device counter value,

verifying the RF transaction device authentication tag using a corresponding RF transaction device encryption key, the corresponding RF transaction device encryption key corresponding to a RF transaction device encryption key referenced to a RF transaction device;

verifying the RF transaction device counter value; and

processing a transaction request where the RF transaction device authentication tag and the RF transaction device counter is verified, the RF transaction device authentication tag being produced using the RF transaction device encryption key, a random number, the RF

transaction device counter value and the transaction account number, where the RF transaction device encryption key, the RF transaction device counter value, and the transaction account number are provided by a RF transaction device,
wherein the random number is provided by a RF reader.

[Claim 26] A computer-readable storage medium containing a set of instructions for a general purpose computer configured for:
receiving a RF reader authentication tag, a transaction account number, and a merchant POS encryption key;
verifying the RF reader authentication tag using the merchant POS encryption key; and
processing a transaction request where the RF reader authentication tag is verified, the RF reader authentication tag being produced using a RF transaction device counter value, a RF reader encryption key, and transaction account number, where the RF transaction device counter value and the transaction account number is provided by a RF transaction device, and wherein the RF reader encryption key is provided by a RF reader.

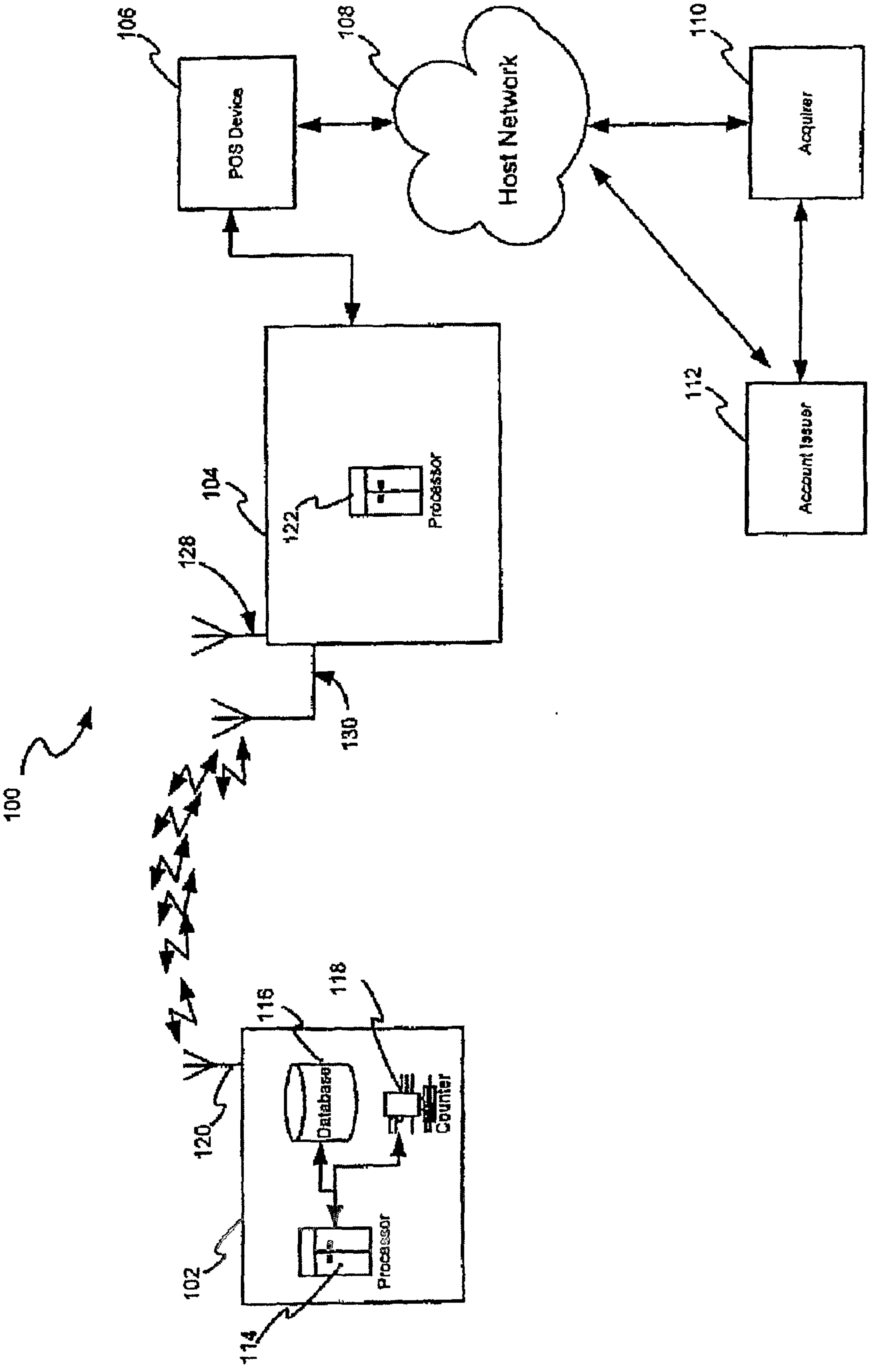

106
POS Device
108
Host Network
110
Acquirer
112
Account Issuer
104
122
Processor
128
130
100
116
Database
118
Counter
120
102
Processor
114

FIGURE 1

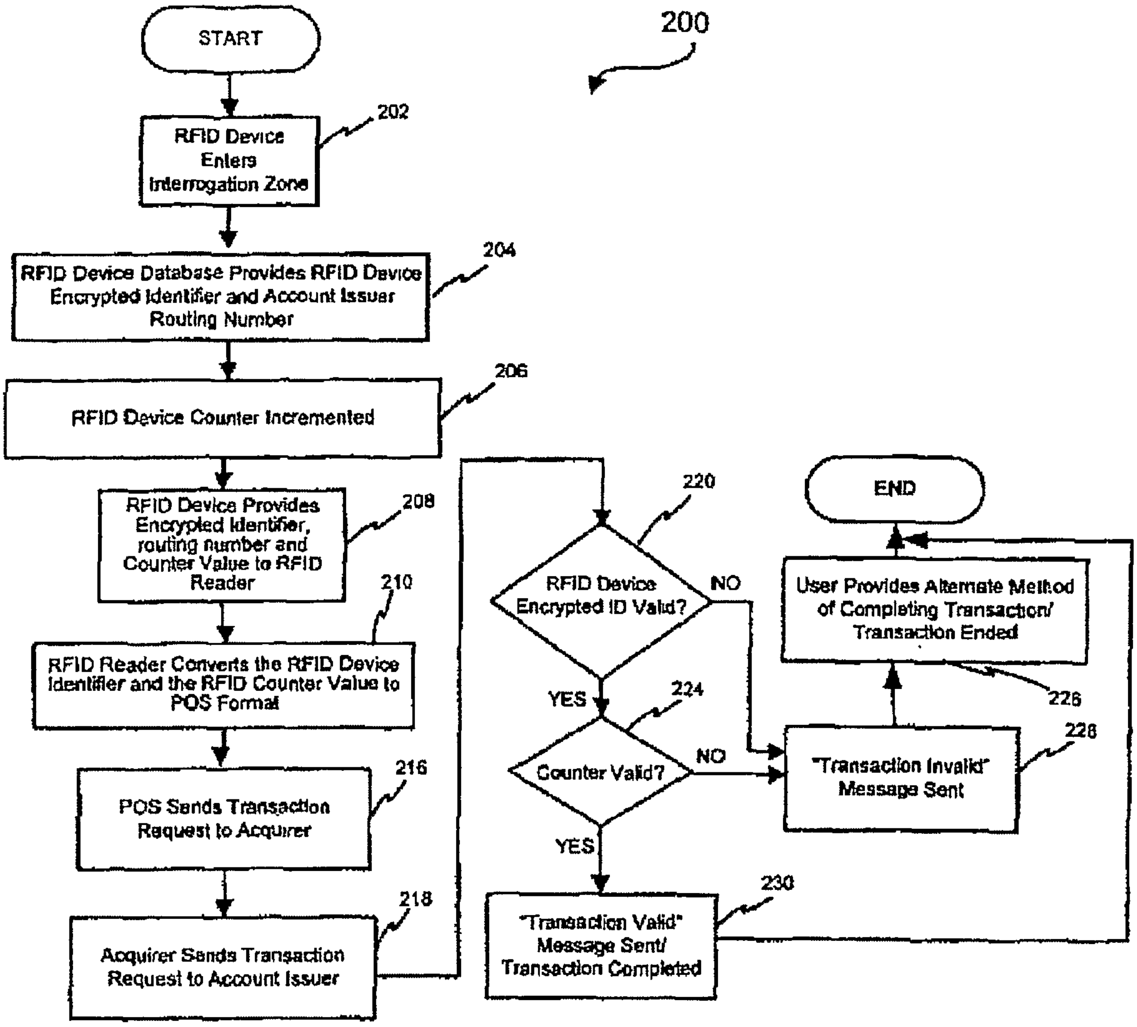

200
START
RFID Device Enters Interrogation Zone
202
RFID Device Database Provides RFID Device Encrypted Identifier and Account Issuer Routing Number
204
RFID Device Counter Incremented
206
RFID Device Provides Encrypted Identifier, routing number and Counter Value to RFID Reader
208
RFID Reader Converts the RFID Device Identifier and the RFID Counter Value to POS Format
210
POS Sends Transaction Request to Acquirer
216
Acquirer Sends Transaction Request to Account Issuer
218
RFID Device Encrypted ID Valid?
220
NO
YES
Counter Valid?
224
NO
YES
"Transaction Valid" Message Sent/ Transaction Completed
230
"Transaction Invalid" Message Sent
228
User Provides Alternate Method of Completing Transaction/ Transaction Ended
226
END

FIGURE 2

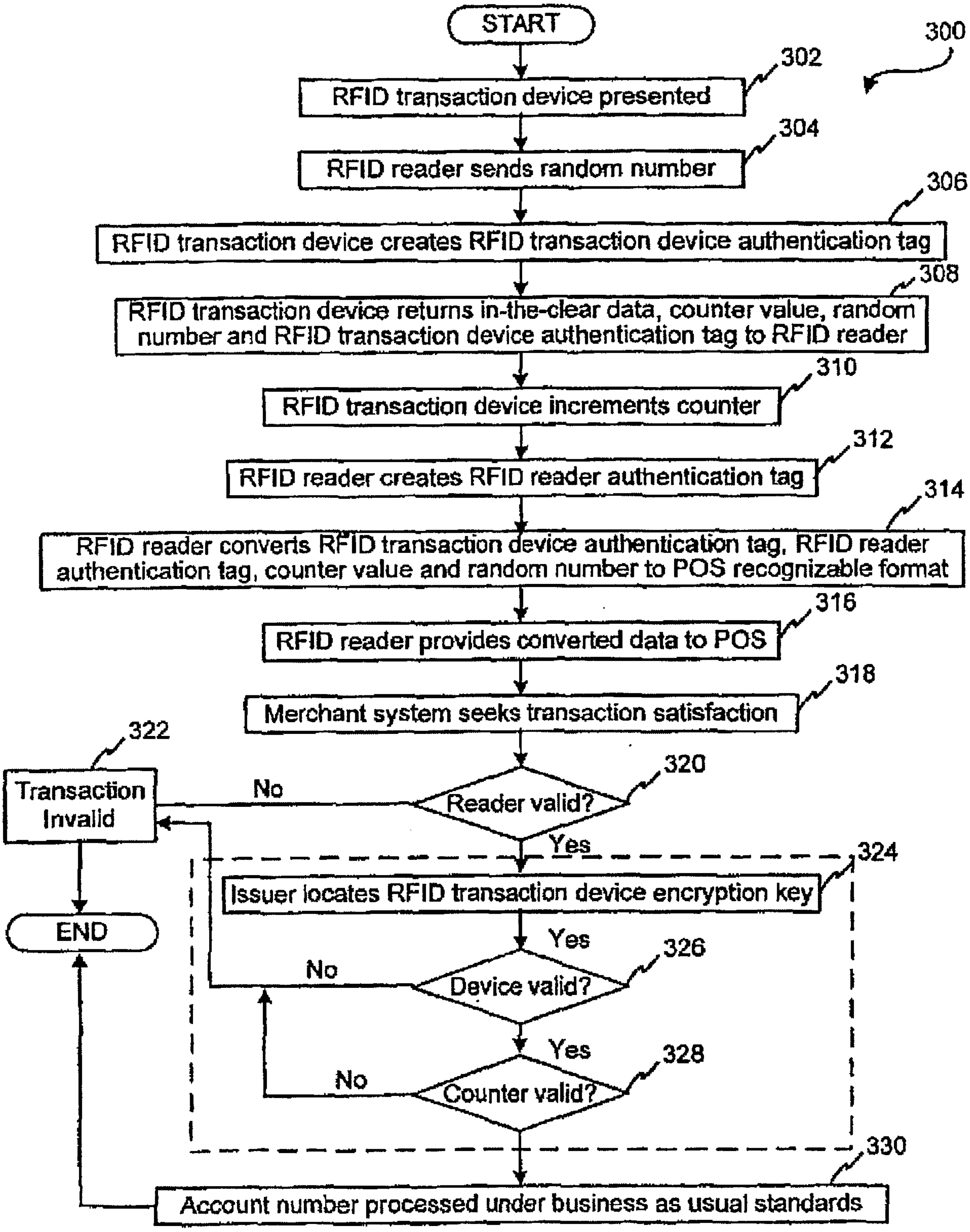

START
300
302
RFID transaction device presented
304
RFID reader sends random number
306
RFID transaction device creates RFID transaction device authentication tag
308
RFID transaction device returns in-the-clear data, counter value, random number and RFID transaction device authentication tag to RFID reader
310
RFID transaction device increments counter
312
RFID reader creates RFID reader authentication tag
314
RFID reader converts RFID transaction device authentication tag, RFID reader authentication tag, counter value and random number to POS recognizable format
316
RFID reader provides converted data to POS
318
Merchant system seeks transaction satisfaction
322
Transaction Invalid
No
320
Reader valid?
Yes
324
Issuer locates RFID transaction device encryption key
END
Yes
326
No
Device valid?
Yes
328
No
Counter valid?
330
Account number processed under business as usual standards

FIGURE 3

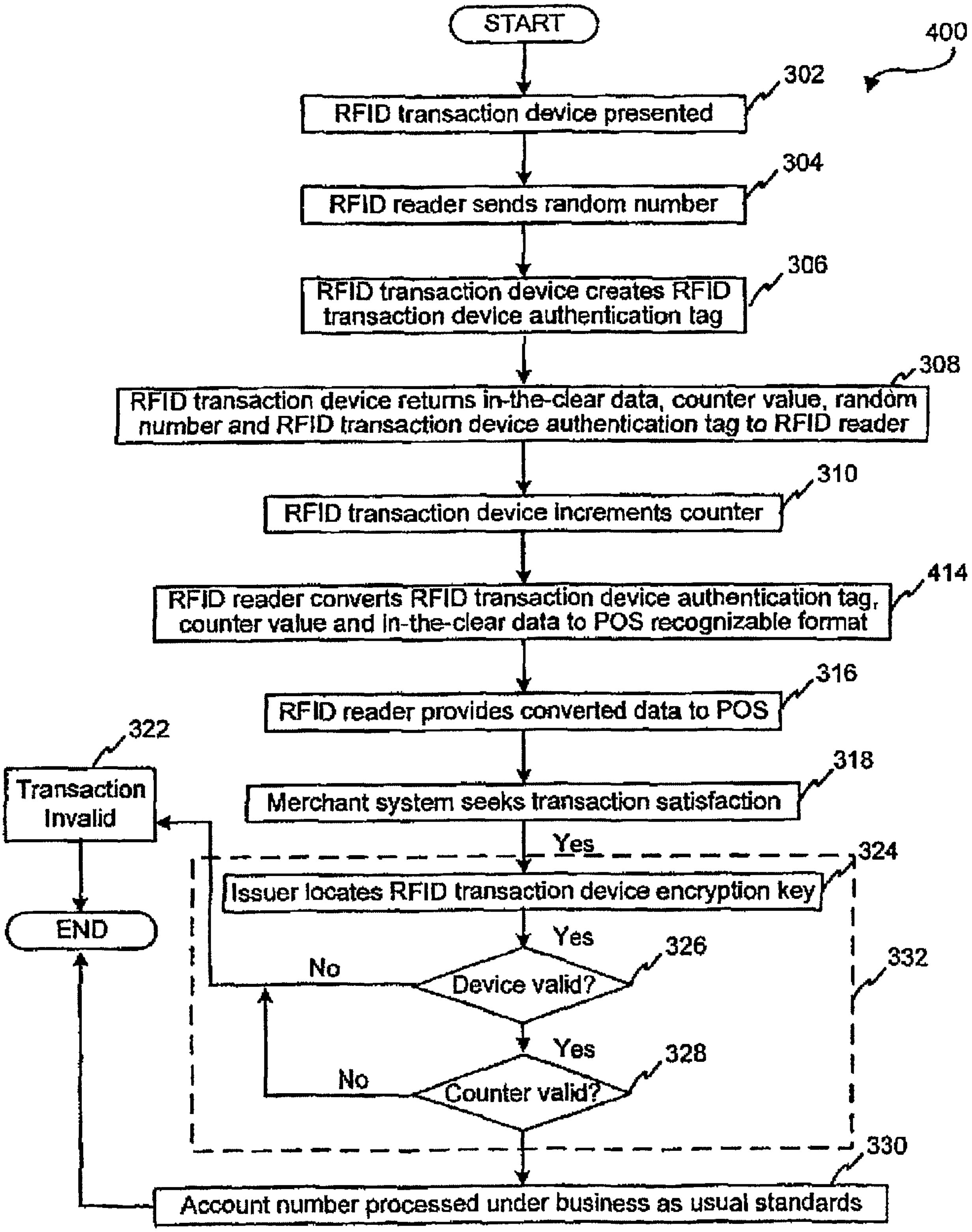

START
400
302
RFID transaction device presented
304
RFID reader sends random number
306
RFID transaction device creates RFID transaction device authentication tag
308
RFID transaction device returns in-the-clear data, counter value, random number and RFID transaction device authentication tag to RFID reader
310
RFID transaction device increments counter
414
RFID reader converts RFID transaction device authentication tag, counter value and in-the-clear data to POS recognizable format
316
RFID reader provides converted data to POS
322
Transaction Invalid
318
Merchant system seeks transaction satisfaction
Yes
324
Issuer locates RFID transaction device encryption key
END
Yes
326
No
Device valid?
332
Yes
328
No
Counter valid?
330
Account number processed under business as usual standards

FIGURE 4

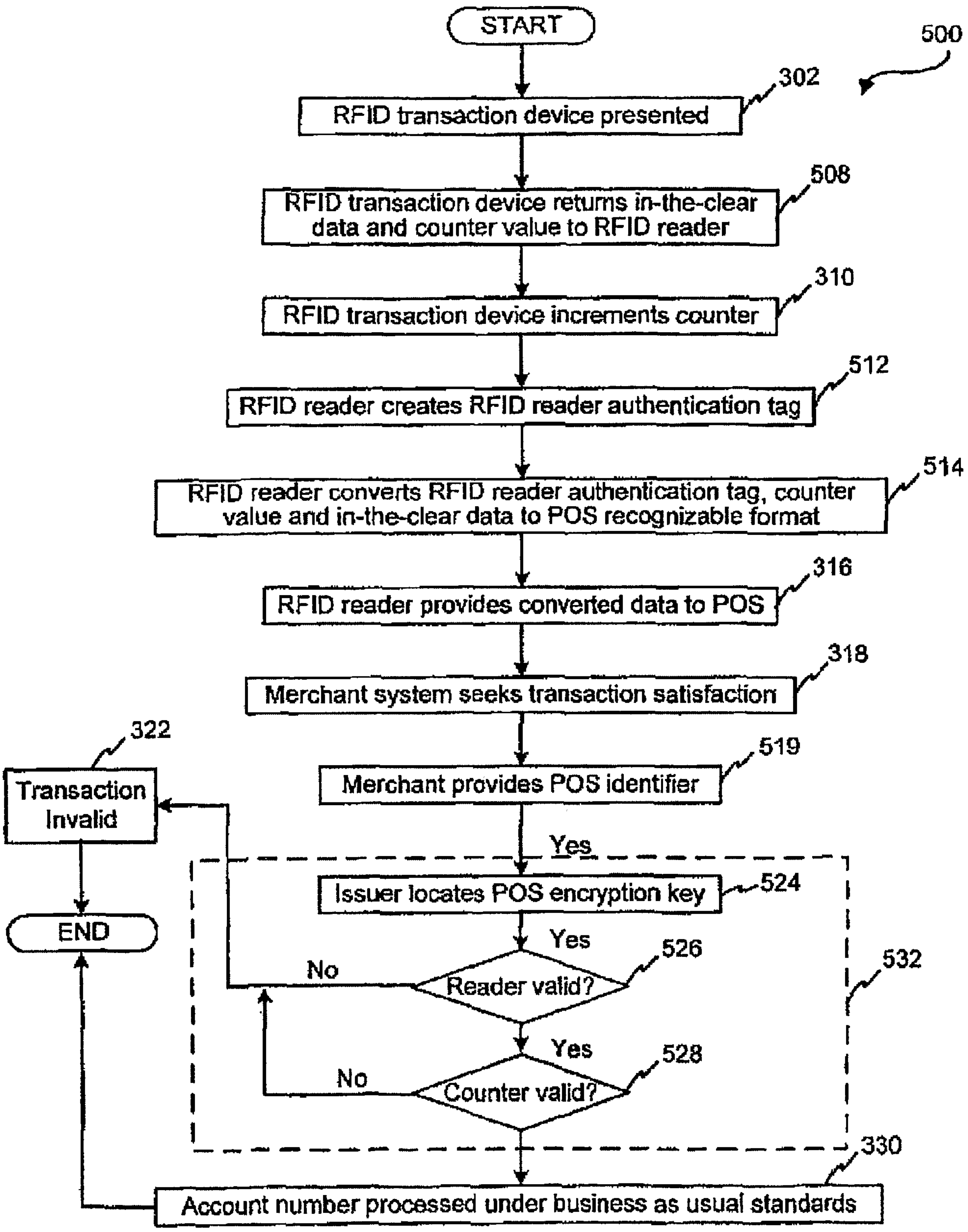

START
500
302
RFID transaction device presented
508
RFID transaction device returns in-the-clear data and counter value to RFID reader
310
RFID transaction device increments counter
512
RFID reader creates RFID reader authentication tag
514
RFID reader converts RFID reader authentication tag, counter value and in-the-clear data to POS recognizable format
316
RFID reader provides converted data to POS
318
Merchant system seeks transaction satisfaction
322
Transaction Invalid
519
Merchant provides POS identifier
Yes
END
Issuer locates POS encryption key
524
Yes
526
No
Reader valid?
532
Yes
528
No
Counter valid?
330
Account number processed under business as usual standards

FIGURE 5