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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
22 September 2005 (22.09.2005)

PCT

(10) International Publication Number
WO 2005/086897 A2

(51) International Patent Classification: Not classified

(21) International Application Number:
PCT/US2005/007905

(22) International Filing Date: 9 March 2005 (09.03.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10/708,545 10 March 2004 (10.03.2004) US

(71) Applicant *(for all designated States except US)*: **AMERICAN EXPRESS TRAVEL RELATED SERVICES COMPANY, INC.** [US/US]; American Express Tower, World Financial Center, New York City, New York 10285-4900 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **BONALLE, David, S.** [US/US]; 77 Rose Hill Avenue, New Rochelle, New York 10804 (US). **ISENBERG, Susan, E.** [US/GB]; 78A Royal Hospital, London Sussex SW34HN (GB). **SAUNDERS, Peter, D.** [US/US]; 3710 East Palisade Drive, Salt Lake City, Utah 84109 (US). **WILLIAMSON, John, R.** [US/US]; 302 Pavonia Avenue, Jersey City, New Jersey 07302 (US).

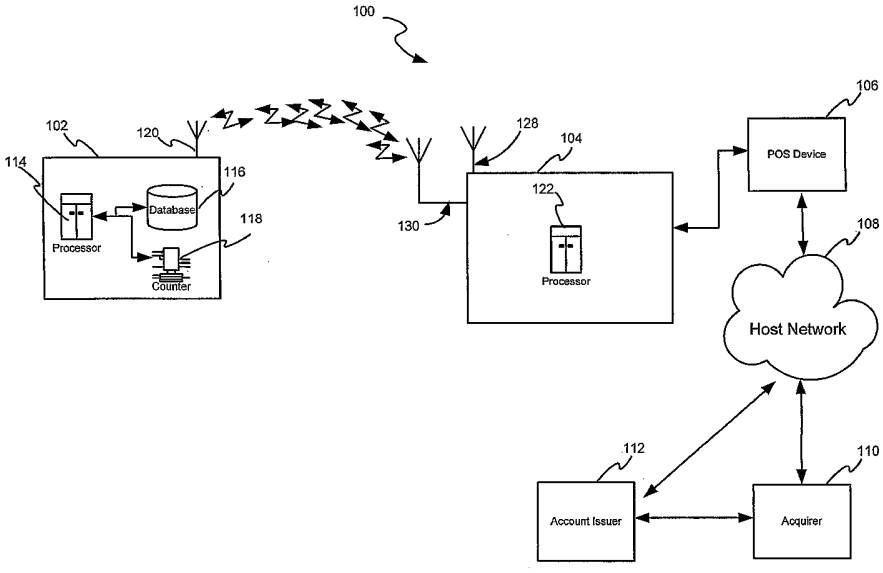
(74) Agent: **SOBELMAN, Howard, I.**; Snell & Wilmer L.L.P., One Arizona Center, 400 East Van Buren, Phoenix, Arizona 85004-2202 (US).

(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, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, 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, MC, NL, PL, PT, RO,

[Continued on next page]

(54) Title: SYSTEM AND METHOD FOR SECURING RF TRANSACTIONS 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. The RFID transaction device includes a transactions counter for tallying the number of transactions attempted or completed with the RFID transactions device. The counter may be incremented by any predetermined amount, which may be predefined for a particular transaction device counter. The counter value is provided to an account issuer for use in determining if the counter value has exceeded a predetermined value correlative to the maximum number of transactions which may be completed using a transaction device.

WO 2005/086897 A2

SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii)) for the following designations 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, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, 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, UZ, VC, VN, YU, ZA, ZM, ZW, ARIPO patent (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)*

— *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii)) for all designations*

Published:

— *without international search report and to be republished upon receipt of that report*

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.

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

Field of Invention

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

Background of the Invention

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.

Of late, companies are increasingly embodying RFID data acquisition technology in a fob or tag for use in completing financial transactions. A typical fob includes a 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. 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.

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. Alternatively, the fob may have an internal power source such that interrogation by the reader to activate the fob is not required.

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.

Minimizing fraud transactions in the RFID environment is typically important to the 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, the 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 the 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.

One problem with the conventional method of securing an RFID transaction is that the time for completing the transaction is increased. This is true since the RFID device user must delay the transaction to provide the alternate identification. As can be seen, this defeats one real advantage of the 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.

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

Summary of the Invention

Described herein is a system and method for securing RFID transactions which addresses the problems found in conventional transaction securing methods. The securing method described herein includes providing a RFID device including a transaction counter which may generate an indicia corresponding to the number of transactions conducted using a particular RFID transaction device.

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

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:

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

Figure 2 illustrates an exemplary method for securing a RFID transaction using a counter-generated indicia in accordance with the present invention.

Detailed Description

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 mircroprocessors 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.

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).

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.

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.

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.

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. The 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.

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.

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.

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 the RFID transaction device.

In one exemplary embodiment, the transaction device identifier may include a unique RFID transaction device serial number and user identification number, as well as specific application applets. The transaction device identifier may be stored on a transaction device database located on the transaction device. The transaction device database may be configured to store multiple account numbers issued to the 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, the RFID transaction device database may be configured to store the attendant loyalty or rewards points data.

The databases discussed herein may be any type of database, such as relational, hierarchical, object-oriented, and/or the like. Common database products that may be used to implement the databases include DB2 by IBM (White Plains, New York), any of the database products available from Oracle Corporation (Redwood Shores, California), Microsoft Access or MSSQL by Microsoft Corporation (Redmond, Washington), or any other database product. Databases

may be organized in any suitable manner, including as data tables or lookup tables. Association of certain data may be accomplished through any data association technique known and practiced in the art. For example, the association may be accomplished either manually or automatically. Automatic association techniques may include, for example, a database search, a database merge, GREP, AGREP, SQL, and/or the like. The association step may be accomplished by a database merge function, for example, using a "key field" in each of the manufacturer and retailer data tables. A "key field" partitions the database according to the high-level class of objects defined by the key field. For example, a certain class may be designated as a key field in both the first data table and the second data table, and the two data tables may then be merged on the basis of the class data in the key field. In this embodiment, the data corresponding to the key field in each of the merged data tables is preferably the same. However, data tables having similar, though not identical, data in the key fields may also be merged by using AGREP, for example.

In addition to the above, the 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, the 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.

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 the RFID transaction device and the 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.

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).

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 nondiscretionary data fields. In one example, the nondiscretionary 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.

As such, where information is provided in accordance with this invention, it may be provided in magnetic stripe format track. For example, the 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.

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.

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. The RFID reader 104 may be in further communication with a merchant point of sale (POS) device 106 for providing to the POS 106 data received from the RFID transaction device 102. The POS 106 may

be in further communication with an acquirer 110 or an account issuer 112 via a network 108 for transmitting transaction request data and receiving authorization concerning transaction completion.

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. The POS device 106 may receive RFID transaction device 102 information and provide the information to host network 108 for processing.

As used herein, an "acquirer" may be a third-party entity including various databases and processors for facilitating the routing of a payment request to an appropriate account issuer 112. The acquirer 112 may route the payment request to the account issuer in accordance with a routing number provided by the RFID transaction device 102, where the routing number corresponds to the account issuer 112. The "routing number" in this context may be a unique network address or any similar device for locating an account issuer 112 on a 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 payment request will not be discussed herein for brevity.

In addition, the account issuer 112 ("account provider") may be any entity which provides a transaction account useful 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 the transaction device itself, but may be

stored remotely, such as, for example, at the 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 the issuer system 112.

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

It should be noted that the RFID reader 104 and the RFID transaction device 102 may engage in mutual authentication prior to transferring any transaction device 102 data to the 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.

In accordance with 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, the transaction device may automatically disable itself against further usage. Alternatively, the account issuer 112 may flag the transaction account correlating to the transaction device such that the account issuer system automatically prevents completion of transactions using the transaction device.

As such, the RFID transaction device 102 in accordance with the present invention further includes a transaction counter 118 for recording and reporting the number of transactions performed with a particular transaction device 102. The

counter 118 may be any device capable of being initiated with a beginning value and incrementing that value by a predetermined amount when the transaction device is presented for completion of a transaction. The counter 118 may be a discrete electronic device on the transponder, or may be software or code based counter as if found in the art.

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.

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

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

For example, the account issuer 112 may preset the initial counter value at 5 units and the counter value to be incremented at 10 units per transaction. The account issuer 112 may determine that transaction device 102 may be used to complete a total transaction value of 20 transactions. Since the counter 118 increments the 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 the counter value equals 205 units, then the operation of the transaction device 102 is disabled.

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

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

Upon determining the total transactions counted value, the RFID transaction device 102 may provide the total transactions counted value, the encrypted transaction device 102 identifier, and the account issuer 112 routing number to the RFID reader 104 via RF transmission (step 208). The RFID reader 104 may, in turn, convert the transaction device 102 identifier, routing number, and total transactions counted value into merchant POS recognizable format and forward the converted information to the merchant POS 106 (step 210). The merchant system including the POS 106 may then provide a transaction request to an acquirer 110 via network 106. The transaction request may include the information received from the 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 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). The account issuer may then identify that a transaction request is being provided that relates to a transaction device. For example, the 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 the account issuer 112. Alternatively, the transaction device identifier, or a portion thereof, may be identified by the account issuer 112 as originating with a RFID transaction device 102.

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

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

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 the counter value is met or exceeded, and the transaction is considered "invalid." As such, the account issuer 112 may then provide a "Transaction Invalid" message to the POS 106 (step 228). In addition, the 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 the account issuer 112 may also provide a "Transaction

Invalid" message to the 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.

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

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 the RFID transaction device is a valid device for completing a transaction on a RF transaction system. The account issuer can determine whether the transaction device is valid by verifying the transaction device counter, and encryption identifier. It should be noted, however, that the present invention contemplates various arrangements wherein the transaction device may be validated.

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, the RFID reader may include an RFID reader encrypted identifier stored in the reader database, which may be validated by the account issuer in similar manner as with the transaction device encrypted identifier. Moreover, the 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.

Claims

What is claimed:

1. A Radio Frequency (RF) transaction securing system comprising:

a radio frequency identification (RFID) transaction device, including:

a RF operable transaction device transponder;

a transaction device processor in communication with said transponder;

a transaction device database in communication with said transaction device processor; and

a transactions counter in communication with said transaction device processor, said counter including a total transactions counted value.

2. A system according to claim 1, wherein said transaction device database stores at least one of a transaction device authentication tag and an encrypted transaction device identifier.

3. A system according to claim 2, further including a RFID reader operable to receive transaction device information from said transaction device via RF communications, said RFID reader comprising:

a RF operable reader transponder; and

a reader processor in communication with said transponder.

4. A system according to claim 3, wherein said RFID reader provides an interrogation signal for interrogating said transaction device.

5. A system according to claim 4, wherein said counter increments said total transactions value a predetermined value to be incremented in response to said interrogation signal, said counter further providing said incremented total transactions value to said transaction device processor.

6. A system according to claim 5 wherein said transaction device database provides said transaction device authentication tag and said transaction device encrypted identifier to said transaction device processor in response to said interrogation signal.

7. A system according to claim 6, wherein said processor provides at least one of said transaction device authentication tag, said transaction device encrypted identifier, and said incremented total transactions counted value to said transaction device transponder, said transaction device transponder for providing to said RFID reader transponder via RF communications.

8. A system according to claim 7, wherein said RFID reader further comprises a reader database in communication with said reader processor.

9. A system according to claim 8, wherein said reader database stores a reader authentication tag, said reader database further providing said reader authentication tag to said reader processor.

10. A system according to claim 9, further comprising:

a merchant point of sale (POS) device in communication with said RFID reader; and

an account issuer in communication with said POS via a network.

11. A system according to claim 10, wherein said RFID reader provides at least one of said transaction device authentication tag, said transaction device encrypted identifier, and said incremented total transactions counted value and said reader authentication tag to said POS, said POS forming a transaction request including transaction completion information and at least one of said transaction device authentication tag, said transaction device encrypted identifier, and said incremented total transactions counted value, and said reader authentication tag, said POS providing said transaction request to said account issuer.

12. A system according to claim 11, wherein said account issuer evaluates the validity of said transaction device in accordance with the total transactions counted value received.

13. A system according to claim 12, wherein said account issuer provides approval for transaction completion to said POS when said total transactions counted value is less than a predetermined maximum transactions value, and wherein said account issuer disallows the completion of a transaction when said total transactions counted value is greater than said maximum transactions value.

14. A system according to claim 13, wherein said account issuer evaluates the validity of said transaction device in accordance with the transaction device authentication tag received.

15. A system according to claim 14, wherein said account issuer evaluates the validity of said RFID reader in accordance with the reader authentication tag received.

16. A system according to claim 15, wherein said account issuer provides approval for transaction completion to said POS when said transaction device authentication tag is validated.

17. A system according to claim 16, wherein said account issuer provides approval for transaction completion to said POS when said reader authentication tag is validated.

18. A method for securing Radio Frequency (RF) transactions comprising the steps of:

providing an interrogation signal for interrogating a RF transaction device including a RF operable transaction device transponder;

providing a counter for counting the total transactions completed with the RF transaction device;

incrementing the counter value a predetermined incremental value when a transaction request is provided, thereby providing the total number of transactions completed with the transaction device; and

approving a transaction based on the value of the total number of transactions completed.

19. A method of completing a secure Radio Frequency transaction comprising:

providing a RFID transaction device including a counter for counting the number of transactions completed with the device; and

approving a transaction based on the number of transactions completed with the device.

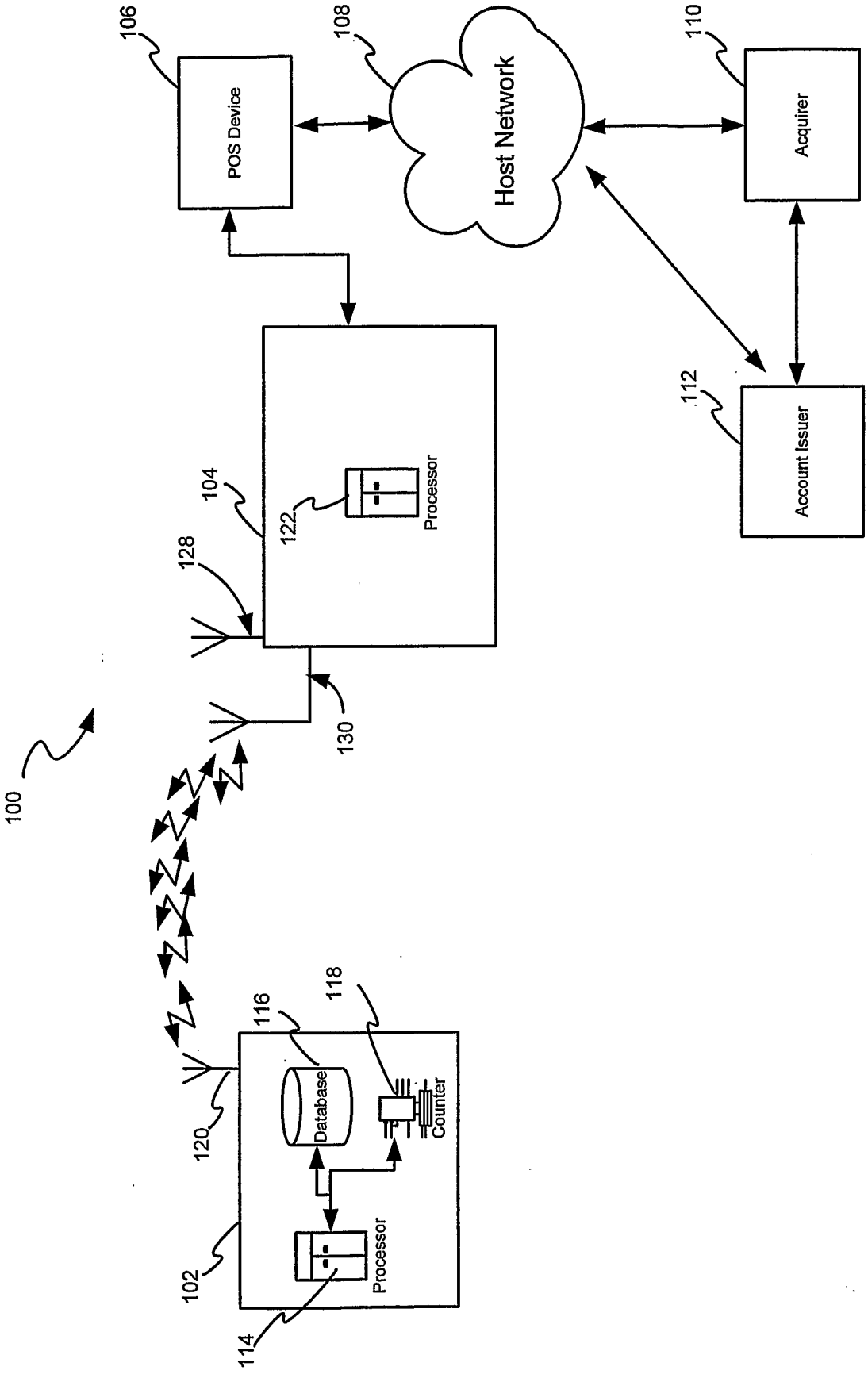

106
POS Device
108
Host Network
110
Acquirer
112
Account Issuer
104
122
Processor
128
130
100
116
118
Database
Counter
120
102
Processor
114

FIGURE 1

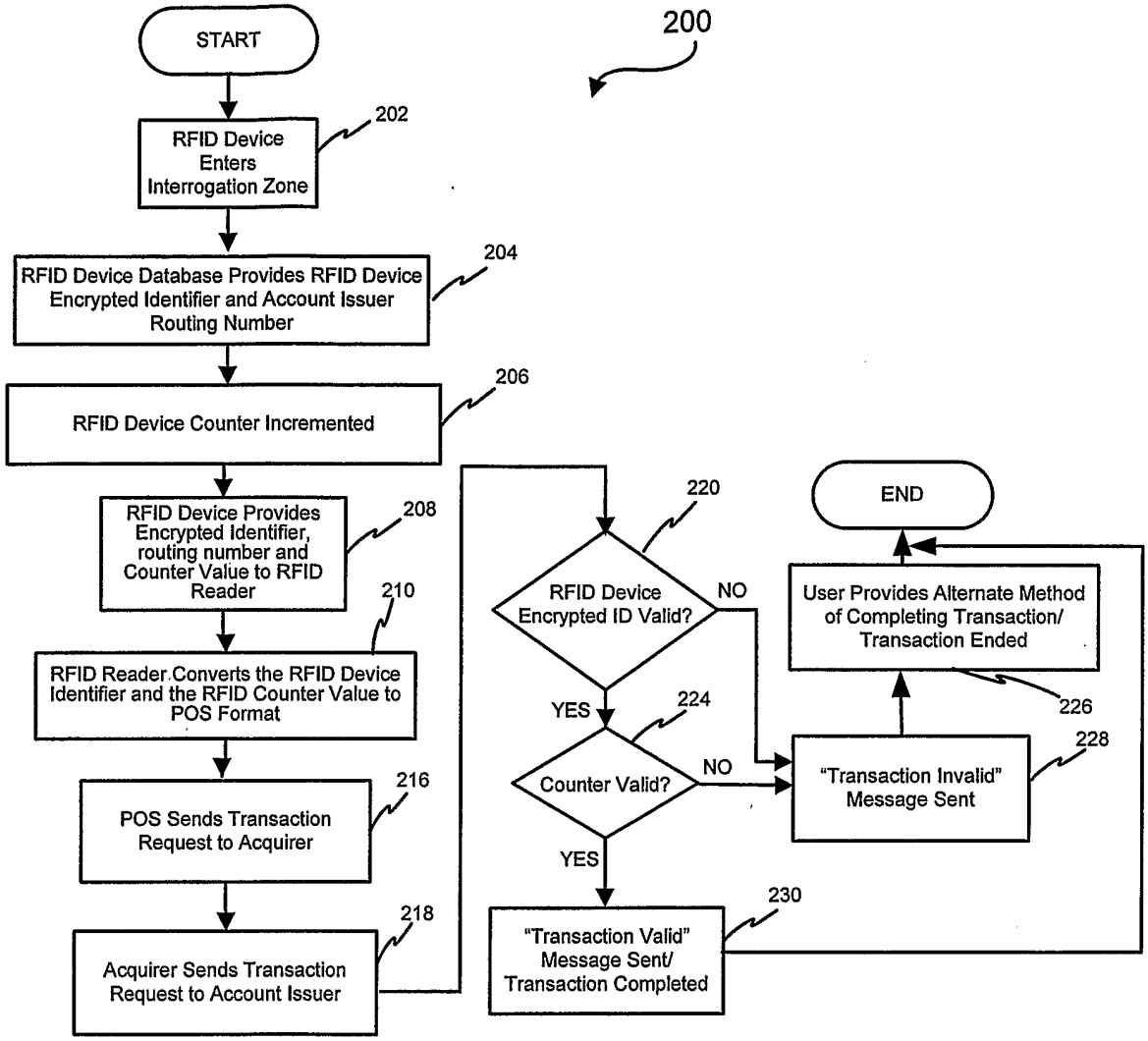

200
START
202
RFID Device Enters Interrogation Zone
204
RFID Device Database Provides RFID Device Encrypted Identifier and Account Issuer Routing Number
206
RFID Device Counter Incremented
208
RFID Device Provides Encrypted Identifier, routing number and Counter Value to RFID Reader
210
RFID Reader Converts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

FIGURE 2