

SYSTEM AND METHOD FOR RFID PAYMENTS

Inventors: John R. Williamson, Jersey City, New Jersey
Alexandra Mayers, New York, New York
David S. Bonalle, New Rochelle, New York
Jennifer Anne Elwood, New York, New York
Peter D. Saunders, Salt Lake City, Utah
Michael J. Berardi, Fort Lauderdale, Florida
Kathryn D. Scheduling, New York, New York
Matthew C. Hood, Wayne, Pennsylvania
Susan E. Isenberg, New York, New York
Sejal Ajit Shah, New York, New York

Background

Like barcode, magnetic stripe, voice data entry and other automatic identification, RFID (Radio Frequency Identification) is an information acquisition technology. RFID is a relatively new technology, first appearing in tracking and access applications during the 1980s. These wireless systems typically allow for non-contact reading and consequently are usually effective in manufacturing and other hostile environments where barcode labels could not survive. RFID has established itself in a wide range of markets, ranging from the high-speed reading of railway containers to applications in retail that can be regarded as a potential successor to the barcoding technologies in use today. Because of its ability to track moving objects, it is being used with livestock identification and automated vehicle identification (AVI) systems. The technology has become a primary player in automated data collection, identification, and analysis systems worldwide.

RFID systems make use of the properties of radio frequency (or electromagnetic) propagation. Different frequencies of the radio system result in different reading ranges and properties of the system. One of the key differentiators of RFID systems is the frequency ranges that are typically used, such as, for example:

Type	Frequency Band	System Characteristics	Example Application
Low	100-500 kHz	Short read range Inexpensive	Access Control Animal Identification Inventory Control
Intermediate	10-15 MHz	Medium Read range	Access Control Smart Cards
High	850-950 MHz 2.4-5.0 GHz	Long Range read High reading speed Line of sight required Expensive	Railroad car monitoring Toll Collection Systems

RFID systems can further be broken down according to some characteristics of the transponders being used, namely, whether they are active or passive. Passive transponders contain no batteries and are designed to be disposable. Active transponders are hermetically sealed in a housing designed to tolerate harsh environmental conditions and will last many years. The classification of transponders can be taken to another step, such that regardless of whether they are active or passive, they can be either read-only, write-once-read-many (WORM), or read-write.

Regardless of the type of system being used, the significant advantage of all types of RFID systems is the non-contact, non-line-of-sight nature of the technology. The use of the radio system enables a transponder to be read if it is not visible to identify those goods remotely, either in the form of an identity code or more simply that something is present. This means the transponders can be read through a variety of substances such as snow, fog, ice, paint, crusted grime, wood, concrete, and other visually and environmentally challenging conditions, where barcodes or other optically read technologies would be limited. The transponder can also be read in challenging circumstances at remarkable speeds, in most cases responding in less than 100 milliseconds.

One of the more successful and visible uses of transponders has been the introduction of Mobil's SpeedPass and Shell's EasyPay products. These

offerings use transponders placed in a tag that can be placed onto a card or a car that enables the user to automatically identify themselves and a previously defined credit or check card that should be used to pay for the ensuing purchase. Although used primarily at the "pump", the card can also be used to
5 buy food or merchandise from the Mobil station. Recently, the completion of the ISO 14443 standard specifies a standard form of communication for contactless smart chips, which is incorporated herein by reference.

The laws about what frequencies are available for different applications often vary from country to country. The very low frequencies that TIRIS uses for
10 keyrings are usable everywhere. To meet the tough requirements for a reliable vehicle tag, TI combined low and high frequencies into one tag in a patented approach that works great. The high frequency is in the 900 MHz range which is endorsed for vehicle applications in North America. For European installations, we have brought our high frequency signal down to the 868 MHz range for
15 vehicle applications in those countries. -- Joe Pearson, Retail program manager Texas Instruments. For further information, see the following excerpt from "An Industry Roundtable Hosted by Texas Instruments as NACS-Tech '98" which is hereby incorporated by reference.

Detailed Description of Exemplary Embodiments

20 As set forth in the attached documents, in an exemplary embodiment, in general, the key fob utilizes RFID (radio frequency identification) to communicate wirelessly. A user will wave a transponder in front of a reader; the reader will decrypt the account information on the chip and send it to the POS (point of sale). The POS will send the transaction across the network and the
25 authorization and settlement process should primarily be business as usual.

The value proposition to the user is, for example, speed, convenience and alternative to cash. The value proposition to the merchant is, for example, additional throughput/more customer spend, customer loyalty, enhanced

effectiveness of incentive programs, personnel savings, small investment, possible short-term category exclusivity, and ability to capture market data on historical cash spend. The value proposition to the host/issuer is profitable method of entry to low ROC (record of card) industries, merchant interest in
5 accepting smart chip products, marketplace differentiation/retention of technology leadership in financial services, allows capture of a larger portion of cash spend and ability to capture market data on historical cash spend.

More specifically, in an exemplary embodiment, the present invention consists of a smart card payment device in a keyring fob format, which uses
10 contactless technology for a wireless (RFID) interface between the keyring fob and the contactless RF reader. The fob is a multi-frequency device supporting both the ISO 14443 standard and the TI Low Frequency (134kHz) for compatibility with Mobil SpeedPass systems. At the merchant, a RF transceiver reader (ISO 14443 compliant) interfaces to the merchant transaction terminal
15 and presents the terminal with data in magnetic stripe (ISO 7813) format. Although there are currently no security standards for contactless payment devices, suitable security will be provided to minimize risk. In one embodiment, the system supports EMV standards. All of the foregoing standards and systems are herein incorporated by reference.

20 The exemplary fob includes a USB interface to the ISO 14443 chip for online Internet payments and other online applications. The fob also contains a USB connector that interfaces to the ISO 14443 chip. The fob can be connected to a USB port on any PC and communicate without needing any additional reader device. The fob is able to perform read and write functions via the ISO
25 14443 interface as well as the USB interface. The data stored on the fob includes, for example, a unique serial number, user identification, track I and II data, as well as specific application applets. Enough expansion is provided to support new applets in the future. The system may be compatible with other smart card standards and support systems (such as AMI) to manage the chip

environment. **Refer to diagram 1.** User uses the fob with the USB port in the same way as they would use the a smart card providing an X.509 Certificate and enabling interactive applications on the Internet. No reader is required because the connection is made directly using the USB port. **Refer to diagram 5.**

5 The device could support an optional on/off switch that would allow the user to enable the fob at the point-of-sale. This feature would provide an enhanced security service, as it would eliminate concerns about transponder information being unintentionally retrieved when passing close to a reader device.

10 A two-factor authentication may be provided for certain transactions (e.g. payments of over \$50). A PIN will be stored in the fob for this purpose. If requested, a user-entered PIN (personal identification number) will be verified with the stored PIN.

15 The ISO 14443 chip may include security procedures for contactless payment as well as the online USB interface. No standards are available for contactless payment but the security will provide suitable protection to meet predetermined risk requirements. A future requirement maybe to use biometrics on the fob instead of a PIN to improve ease of use and to reduce modification at the merchant terminal. **Refer to Diagram 2.** Generally, the system may protect the
20 ability to authenticate with anything the user knows (this is the PIN in the case above), or anything the user is (refers to the biometrics point above), in addition the device which the user has.

25 The merchant terminal may be supplied in two formats: a reader that can be integrated into current merchant transaction terminals or a stand-alone terminal. In an exemplary embodiment, the system includes a very low cost reader that can be simply integrated with existing Transaction Terminals with little/no change in the existing POS infrastructure. **Refer to Diagram 3.**

The system may be used for purchases under \$50 in order to make the implementation at the POS simpler. In this case, the back-end authorization system will not authorize purchases over \$50. When the system is used for purchases over \$50, in one embodiment, the cardmember provides additional authentication too and a PIN will be used for these purchases. The PIN authentication will be done locally via the fob and will not involve the Amex back-end system in any way. The Amex backend system will not see any difference in the authorization process and assume that the reader has made the determination for PIN usage and completed the PIN authentication by the time that the authorization request is sent to Amex.

The transaction flow would be:

1. ECR sends total purchase value to Reader
 2. Reader checks total value of purchase. If over \$50.00 Reader requests PIN. If below \$50, the PIN is not requested.
 3. Cardmember enters PIN
 4. PIN validated by fob
 5. Access Amex for authorization as any other magnetic stripe card
 6. Authorization sent to merchant
- Printed receipt if desired. (option selection to be defined)

The combination of features provides a unique tool to provide fast, secure payment and Internet access. In one embodiment, specific features include:

- Multi-frequency operation
- USB connector on an RF contactless smart card device
- On/Off switch for unwanted radio frequency control
- Self-contained biometrics replacing PIN in a payment device
- Use of a keyring fob for charge and lending product payments

This invention may also feature an encrypted account number stored on the transponder device. This encrypted form is transmitted to the reader device,

which performs unencryption prior to passing the plaintext account number along the network. All other known implementations employ a unique identification code, which the reader passes along the network, to be mapped to the account number by a database lookup on the system of record.

- 5 The combination of 134 kHz RFID, 13.56MHz Contactless Smart card, the USB interface, and the PIN/biometrics replacement in a single payment device is unique. Other unique components include, for example, multi-frequency operation, USB connector on an RF contactless smart chip device, On/Off switch for unwanted radiation control, Self-contained biometrics replacing PIN in
- 10 a payment device. This invention also features an encrypted account number stored on the transponder device. This encrypted form is transmitted to the reader device, which performs unencryption prior to passing the plaintext account number along the network. All other known implementations employ a unique identification code, which the reader passes along the network, to be
- 15 mapped to the account number by a database lookup on the system of record.

- The system may include a host server or other computing systems including a processor for processing digital data, a memory coupled to said processor for storing digital data, an input digitizer coupled to the processor for inputting digital data, an application program stored in said memory and
- 20 accessible by said processor for directing processing of digital data by said processor, a display coupled to the processor and memory for displaying information derived from digital data processed by said processor and a plurality of databases, said databases including client data, merchant data, financial institution data and/or like data that could be used in association with the
- 25 present invention. As those skilled in the art will appreciate, user computer will typically include an operating system (e.g., Windows NT, 95/98/2000, Linux, Solaris, etc.) as well as various conventional support software and drivers typically associated with computers. User computer can be in a home or business environment with access to a network. In an exemplary embodiment,

access is through the Internet through a commercially-available web-browser software package.

Communication between the parties to the transaction and the system of the present invention is accomplished through any suitable communication means, such as, for example, a telephone network, Intranet, Internet, point of interaction device (point of sale device, personal digital assistant, cellular phone, kiosk, etc.), online communications, off-line communications, wireless communications, and/or the like. One skilled in the art will also appreciate that, for security reasons, any databases, systems, or components of the present invention may consist of any combination of databases or components at a single location or at multiple locations, wherein each database or system includes any of various suitable security features, such as firewalls, access codes, encryption, de-encryption, compression, decompression, and/or the like.

Database 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, NY), any of the database products available from Oracle Corporation (Redwood Shores, CA), Microsoft Access by Microsoft Corporation (Redmond, Washington), or any other database product. Database 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.

The computer may provide a suitable website or other Internet-based graphical user interface which is accessible by users. In one embodiment, the Internet Information Server, Microsoft Transaction Server, and Microsoft SQL Server, are used in conjunction with the Microsoft operating system, Microsoft NT web server software, a Microsoft SQL database system, and a Microsoft Commerce Server. Additionally, components such as Access Sequel Server, Oracle, MySQL, Intervase, etc., may be used to provide an ADO-compliant database management system. The term "webpage" as it is used herein is not meant to limit the type of documents and applications that might be used to interact with the user. For example, a typical website might include, in addition to standard HTML documents, various forms, Java applets, Javascript, active server pages (ASP), common gateway interface scripts (CGI), extensible markup language (XML), dynamic HTML, cascading style sheets (CSS), helper applications, plug-ins, and the like.

The present invention may be described herein in terms of functional block components, screen shots, optional selections and various processing steps. It should be appreciated that such functional blocks may be realized by any number of hardware and/or software components configured to perform the 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), 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
5 for data transmission, signaling, data processing, network control, and the like. Still further, the invention could be used to detect or prevent security issues with a client-side scripting language, such as JavaScript, VBScript or the like. For a basic introduction of cryptography, please review a text written by Bruce Schneider which is entitled "Applied Cryptography: Protocols, Algorithms, And
10 Source Code In C," published by John Wiley & Sons (second edition, 1996), which is hereby incorporated by reference.

It will be appreciated, that many applications of the present invention could be formulated. One skilled in the art will appreciate that the network may include any system for exchanging data or transacting business, such as the
15 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 (ITV) network. The users may interact with the system via any input device such as a keyboard, mouse, kiosk, personal digital assistant, handheld computer (e.g., Palm Pilot®), cellular phone and/or
20 the like. Similarly, the invention could be used in conjunction with any type of personal computer, network computer, workstation, minicomputer, mainframe, or the like running any operating system such as any version of Windows, Windows NT, Windows2000, Windows 98, Windows 95, MacOS, OS/2, BeOS, Linux, UNIX, Solaris or the like. Moreover, although the invention is frequently
25 described herein as being implemented with TCP/IP communications protocols, it will be readily understood that the invention could also be implemented using IPX, Appletalk, IP-6, NetBIOS, OSI or any number of existing or future protocols. Moreover, the system contemplates the use, sale or distribution of any goods,

services or information over any network having similar functionality described herein.

The computing units may be connected with each other via a data communication network. The network may be a public network and assumed to be insecure and open to eavesdroppers. In the illustrated implementation, the network may be embodied as the internet. In this context, the computers may or may not be connected to the internet at all times. For instance, the customer computer may employ a modem to occasionally connect to the internet, whereas the bank computing center might maintain a permanent connection to the internet. 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.

The systems may be suitably coupled to network via data links. A variety of conventional communications media and protocols may be used for data links. Such as, for example, a connection to an Internet Service Provider (ISP) over the local loop as is typically used in connection with standard modem communication, cable modem, Dish networks, ISDN, Digital Subscriber Line (DSL), or various wireless communication methods. Merchant system might also reside within a local area network (LAN) which interfaces to network via a leased line (T1, D3, etc.). Such communication methods are well known in the art, and are covered in a variety of standard texts. See, e.g., GILBERT HELD, UNDERSTANDING DATA COMMUNICATIONS (1996), hereby incorporated by reference.

The merchant computer and the bank computer are interconnected via a second network, referred to as a payment network. The payment network represents existing proprietary networks that presently accommodate transactions for credit cards, debit cards, and other types of financial/banking cards. The payment network is a closed network that is assumed to be secure from eavesdroppers. Examples of the payment network include the American Express®, VisaNet® and the Veriphone® network.

The electronic commerce system is implemented at the customer and issuing bank. In an exemplary implementation, the electronic commerce system is implemented as computer software modules loaded onto the customer computer and the banking computing center. The merchant computer does not require any additional software to participate in the online commerce transactions supported by the online commerce system.

An "account number", as used herein, includes any device, code, or other identifier/indicia suitably configured to allow the consumer to interact or communicate with the system, such as, for example, authorization/access code, personal identification number (PIN), Internet code, other identification code, and/or the like which is optionally located on a rewards card, charge card, credit card, debit card, prepaid card, telephone card, smart card, magnetic stripe card, bar code card, and/or the like. The account number may be distributed and stored in any form of plastic, electronic, magnetic, and/or optical device capable of transmitting or downloading data from itself to a second device. A customer account number 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". 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.

It should be appreciated that the particular implementations shown and described herein are illustrative of the invention and its best mode and are not intended to otherwise limit the scope of the present invention in any way. Indeed, for the sake of brevity, conventional data networking, application development and other functional aspects of the systems (and components of the individual operating components of the systems) may not be described in detail herein. Furthermore, the connecting lines shown in the various figures contained herein are intended to represent exemplary functional relationships and/or physical couplings between the various elements. It should be noted that many alternative or additional functional relationships or physical connections may be present in a practical electronic transaction system.

As will be appreciated by one of ordinary skill in the art, the present invention may be embodied as a method, a data processing system, a device for data processing, and/or a computer program product. Accordingly, the present invention may take the form of an entirely software embodiment, an entirely hardware embodiment, or an embodiment combining aspects of both software and hardware. Furthermore, the present invention may take the form of a computer program product on a computer-readable storage medium having computer-readable program code means embodied in the storage medium. Any suitable computer-readable storage medium may be utilized, including hard disks, CD-ROM, optical storage devices, magnetic storage devices, and/or the like.

The present invention is described herein with reference to screen shots, block diagrams and flowchart illustrations of methods, apparatus (e.g., systems), and computer program products according to various aspects of the invention. It

will be understood that each functional block of the block diagrams and the flowchart illustrations, and combinations of functional blocks in the block diagrams and flowchart illustrations, respectively, can be implemented by computer program instructions. These computer program instructions may be loaded onto a general purpose computer, special purpose computer, or other programmable data processing apparatus to produce a machine, such that the instructions which execute on the computer or other programmable data processing apparatus create means for implementing the functions specified in the flowchart block or blocks.

These computer program instructions may also be stored in a computer-readable memory that can direct a computer or other programmable data processing apparatus to function in a particular manner, such that the instructions stored in the computer-readable memory produce an article of manufacture including instruction means which implement the function specified in the flowchart block or blocks. The computer program instructions may also be loaded onto a computer or other programmable data processing apparatus to cause a series of operational steps to be performed on the computer or other programmable apparatus to produce a computer-implemented process such that the instructions which execute on the computer or other programmable apparatus provide steps for implementing the functions specified in the flowchart block or blocks.

Accordingly, functional blocks of the block diagrams and flowchart illustrations support combinations of means for performing the specified functions, combinations of steps for performing the specified functions, and program instruction means for performing the specified functions. It will also be understood that each functional block of the block diagrams and flowchart illustrations, and combinations of functional blocks in the block diagrams and flowchart illustrations, can be implemented by either special purpose hardware-

based computer systems which perform the specified functions or steps, or suitable combinations of special purpose hardware and computer instructions.

In the foregoing specification, the invention has been described with reference to specific embodiments. However, it will be appreciated that various
5 modifications and changes can be made without departing from the scope of the present invention. The specification and figures are to be regarded in an illustrative manner, rather than a restrictive one, and all such modifications are intended to be included within the scope of present invention. Accordingly, the scope of the invention should be determined by the appended claims and their
10 legal equivalents, rather than by the examples given above. For example, 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.

Benefits, other advantages, and solutions to problems have been described above with regard to specific embodiments. However, the benefits,
15 advantages, solutions to problems, and any element(s) that may cause any benefit, advantage, or solution to occur or become more pronounced are not to be construed as critical, required, or essential features or elements of any or all the claims. As used herein, the terms "comprises", "comprising", or any other variation thereof, are intended to cover a non-exclusive inclusion, such that a
20 process, method, article, or apparatus that comprises a list of elements does not include only those elements but may include other elements not expressly listed or inherent to such process, method, article, or apparatus. Further, no element described herein is required for the practice of the invention unless expressly described as "essential" or "critical".

Diagram 1: Fob hardware design

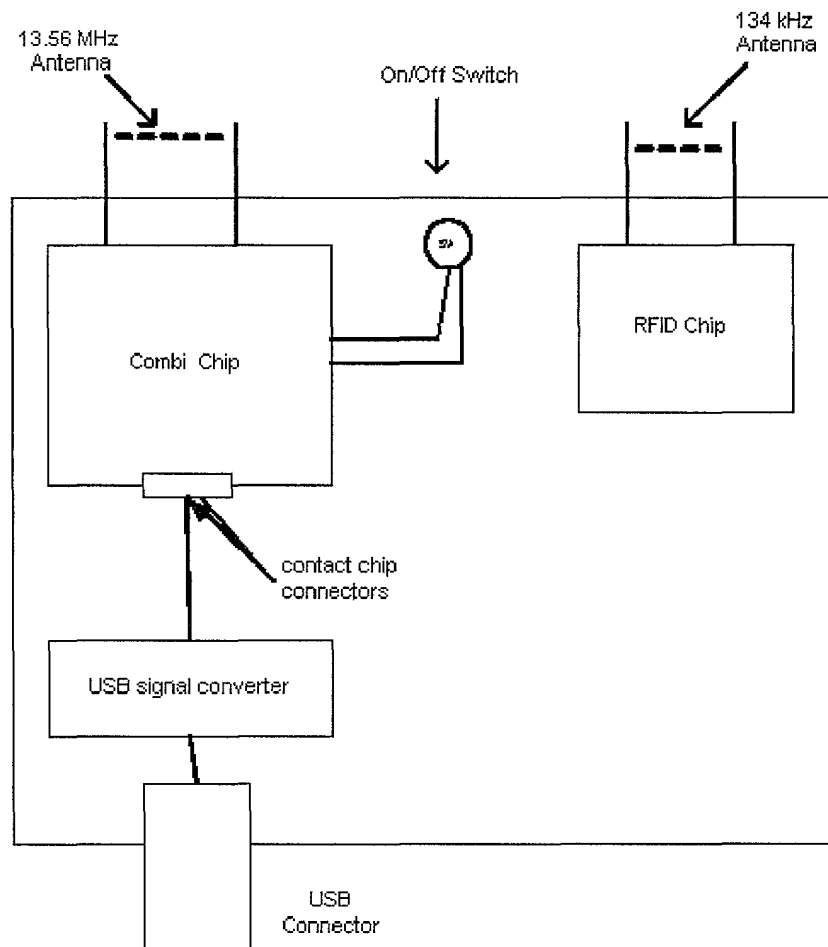


Diagram 2: Fob hardware design including biometric authentication

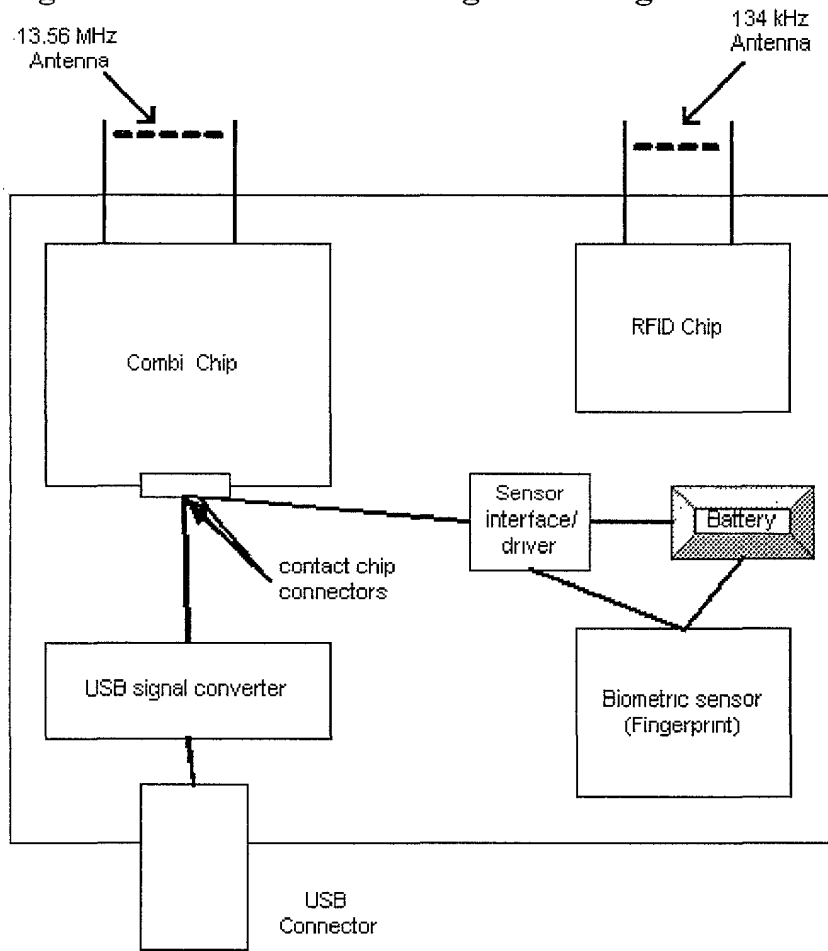


Diagram 3: Two Merchant Configuration Options

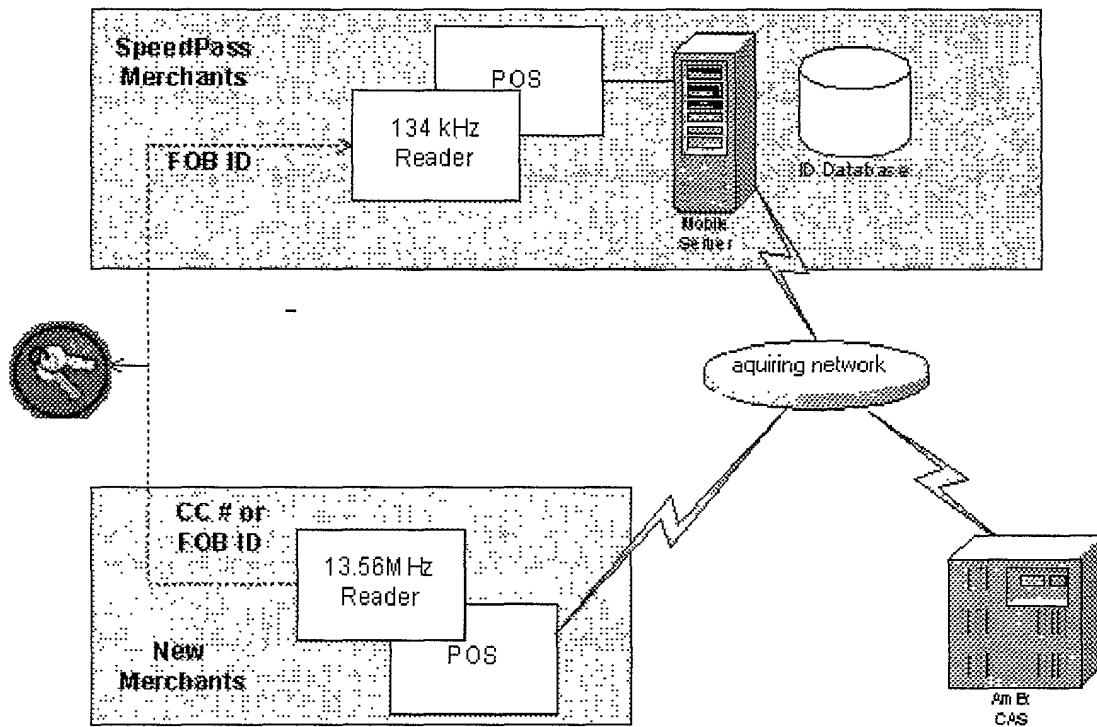


Diagram 4: Transaction terminal configuration

AmEx Roadrunner Transaction Terminal Functional Overview

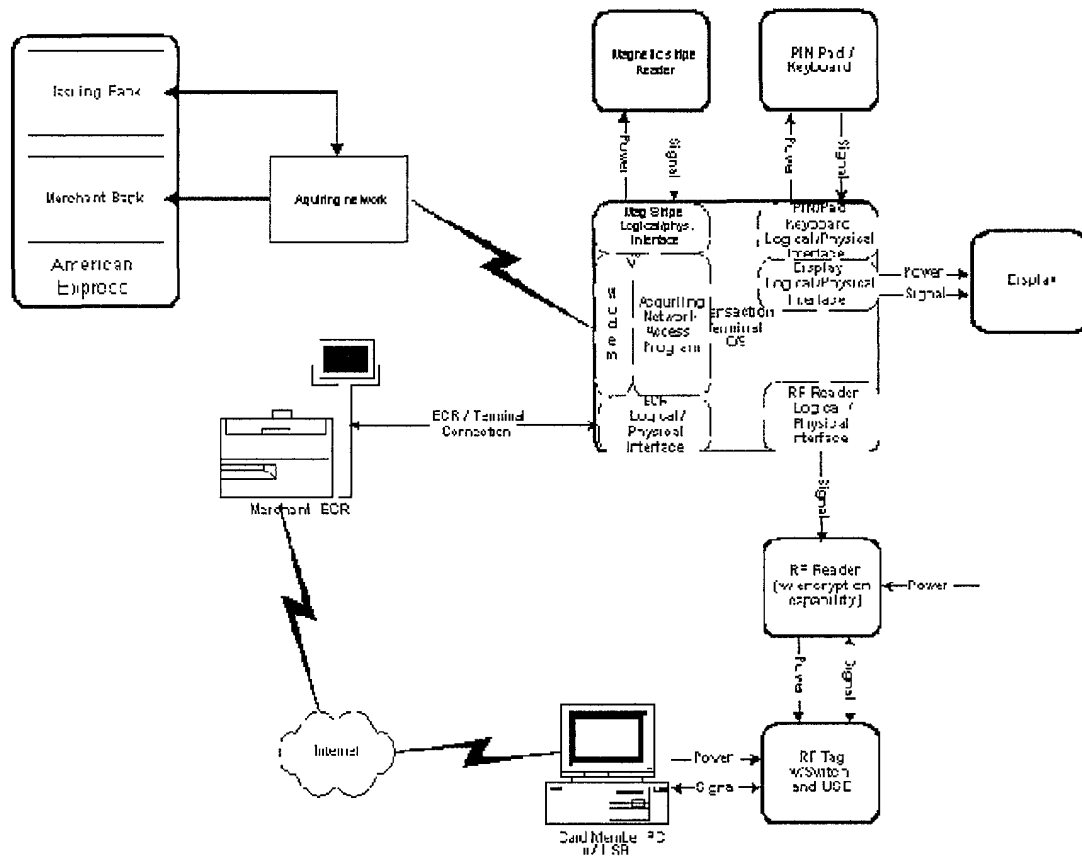
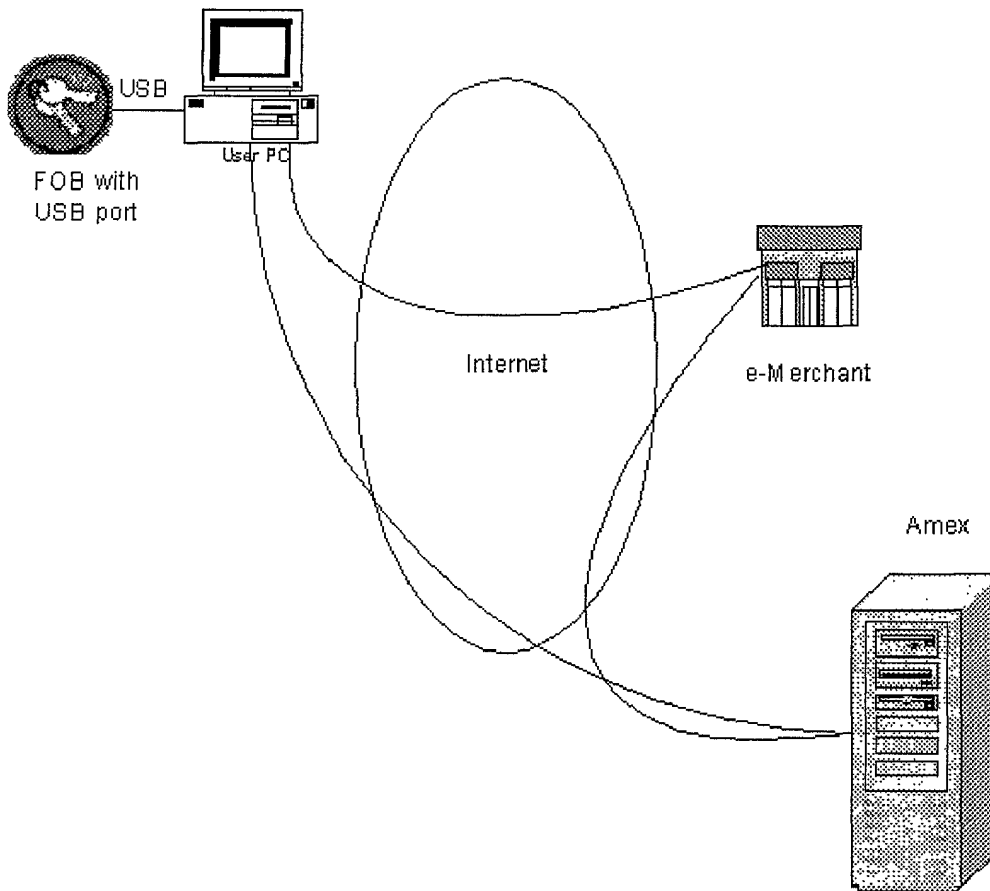


Diagram 5: Internet Usage



Texas Instrument Transponder Patents:

6,239,675, 6,232,917, 6,215,437, 6,198,875, 6,192,255, 6,167,236,
6,133,834, 6,118,189, 6,064,320, 5,970,148, 5,955,969, 5,948,116,
5,929,801, 5,905,798, 5,880,675, 5,870,915, 5,870,031, 5,867,100,
5,864,323, 5,858,006, 5,842,088, 5,841,364, 5,825,302, 5,809,142,
5,798,709, 5,797,060, 5,794,095, 5,793,324, 5,792,337, 5,785,680,
5,748,137, 5,732,579, 5,731,957, 5,729,236, 5,729,053, 5,701,127,
5,691,731, 5,686,920, 5,675,342, 5,673,106, 5,660,319, 5,646,607,
5,638,080, 5,629,981, 5,625,370, 5,625,366, 5,621,412, 5,621,411,
5,621,396, 5,619,207, 5,608,406, 5,602,919, 5,602,538, 5,600,175,
5,597,534, 5,594,448, 5,592,150, 5,569,187, 5,563,582, 5,561,430,
5,557,279, 5,552,789, 5,550,548, 5,550,536, 5,548,291, 5,543,798,
5,541,604, 5,525,994, 5,525,992, 5,513,525, 5,500,651, 5,497,121,
5,493,312, 5,491,715, 5,491,484, 5,491,483, 5,489,908, 5,488,376