SYSTEM AND METHOD FOR PROVIDING A RF PAYMENT SOLUTION TO A MOBILE DEVICE

Related Applications

[0001] This invention claims priority and the benefits of U.S. Provisional Application No. 60/512,297, filed October 17, 2003. This invention is also a continuation-in-part of, and claims priority to, U.S. Application No. 10/746,781, entitled "A SYSTEM AND METHOD FOR MANUFACTURING A PUNCH-OUT RF TRANSACTION DEVICE," filed December 24, 2003. This invention is also a continuation-in-part of, 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 July 9, 2002 (which itself claims priority to U.S. Provisional Patent Application No. 60/304,216, filed July 10, 2001).

[0002] The 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).

[0003] The entire contents of each of these applications is hereby incorporated by reference.

Field of Invention

[0004] The present invention generally relates to transaction devices, and more particularly, to a system and method for providing a Radio Frequency Identification (RFID) transaction solution to a nontraditional transaction device.

Background of the Invention

[0005] For many years, personal checks, travelers checks, money orders, traditional currency and the like were the most popular means for paying for goods or services. In recent years, however, transaction cards (*e.g.*, credit cards, debit cards, smart cards, pre-paid cards, and the like), have developed as a popular substitute for cash or personal checks. The average consumer often prefers the transaction cards over traditional currency since the transaction cards may be easily replaced by the card issuer if the user loses or misplaces the card or the card is stolen.

[0006] As the number of issued transaction cards increases, so do the security issues surrounding transaction card transactions. As a consequence, the transaction card industry started to develop more sophisticated transaction cards which allowed for the reading, transmission, and authorization of transaction card data, while lessening the elevating security concerns. One alternative transaction card that has gained popularity is the smart card. Smart cards are capable of transferring user information during transaction completion without the user ever having to lose physical control of the device. Thus, smart cards enhance the security of the transactions by virtually eliminating the need for the user to hand the card over to a merchant salesperson for transaction completion.

[0007] While smart cards enhanced some security surrounding transaction devices, smart cards did little to address fraud issues associated with a lost or stolen transaction card. Because smart cards are manufactured with the same size dimensions as traditional transaction cards, the user did little more to secure the

smart card against loss than the user did to secure a traditional credit card. This revelation has led transaction card providers to search for a suitable technology that encompassed the enhanced security given by smart cards and more. One such technology is radio frequency identification (RFID) technology.

[0008] Like barcode and voice data entry, RF is a contactless information acquisition technology. RF systems are wireless, and are usually extremely effective in hostile environments where conventional acquisition methods fail. In general, RF technology permits a card manufacturer to provide for a dimensionally smaller transaction device than a smart card or traditional transaction card. RF technology, therefore, is better suited for securing against loss or theft. For example, the RF technology may be embodied in a form factor attachable to the account holder's person or to an often used (or often handled) personal article, such as a key chain, fob or tag. The RF transaction device may be attached to the personal article in an unobtrusive manner because of its smaller size. As such, the user has increased security against loss or theft, since the user handles the personal article frequently, permitting the user to repeatedly be reminded that the card is present.

[0009] One of the more visible transaction devices which used RF technology is found in the introduction of Exxon/Mobil's Speedpass® and Shell's EasyPay® products, which are attachable to a user's key chain. These products use RF transponders placed in a fob or tag of irregular shape which enables automatic identification of the user when the fob is presented at a merchant 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 for completion of a transaction.

[0010] By providing a RF transaction device (*e.g.*, fob) as described above, transaction account providers are able to attract account users in increasing numbers. The account users often prefer account providers that offer the RF

transaction device option because of the convenience of use and the security using a RF transaction fob provides. The increased popularity of the RF fob has not gone unnoticed. Transaction account providers are now looking for various other devices in which to place RF technology for convenient consumer use. These other devices may be devices that the consumer uses more frequently than a traditional credit card or smart card. One suitable device is the mobile telephone. Mobile telephones are typically connected to a telephone network using a wireless connection. Because of their portability, users frequently carry mobile telephones with them throughout their day. Users often take their mobile telephones with them to the office, in the car, and wherever they might go. In this manner, functions within the mobile telephone are available to the user throughout the day. Moreover, the portability of mobile telephones, elevates mobile telephones to an important piece of equipment in consumers' every day lives.

[0011] Another suitable device is the portable personal computer. As personal computers have increased in power and decreased in size, portable personal computers have become more useful and powerful. One smaller version of the personal computer design that has proven useful and quite popular is the so-called personal digital assistant (PDAs), such as Newton.RTM, by Apple Computer, Inc. In general, the average consumer uses the PDA to store telephone numbers and to manage the user's everyday schedule. However, because PDAs are highly programmable, PDAs may be loaded with various software packages that provide other functionality, such as wireless sending and receiving of data. As such, because of the increased popularity PDA use has become prevalent for managing a user's everyday affairs.

[0012] Both mobile telephones and miniaturized portable personal computers, such as PDAs, suffer from one drawback in that they are generally not configured for use in any other way than originally intended. Electronics designers are constantly

looking for ways to expand the functionality of the aforementioned mobile devices since the mobile devices are gaining increasing popularity amongst consumers. For example, it would be desirable to configure the mobile devices for transaction completion. Until then, the ordinary consumer is forced to carry the mobile device and at least one transaction device, such as a credit card, debit card, loyalty card, or radio frequency transaction device (*e.g.*, SPEEDPASS™ and EXPRESSPAY™) on his person. That is, the advent of the technology era has increased a need to combine the functionality of the mobile devices with the transaction completion capability of the transaction devices to limit the number of devices carried by the consumer.

Summary of the Invention

[0013] The present invention relates to a system and method for providing a RF operable transaction device that may be used to convert any article to a RF transaction device. Specifically, the present invention relates to a method of providing a RF transaction device that may be manufactured using conventional RF transaction card manufacturing machinery. The RF device may also be personalized using traditional personalizing machinery and processes.

[0014] It is, therefore, an object of the present invention to provide a RF operable transaction device manufacturing system and method which requires little retrofitting of conventional transaction card manufacturing and personalization machinery.

[0015] In one embodiment, the present invention relates to a process for producing a RF operable transaction device, having any one or more features, such as a holographic foil, integrated circuit chip, silver magnetic stripe with text on the magnetic stripe, opacity gradient, perforations included in the transparent device body for forming an outline of a shape, and an "active thru" date on the front of the device.

[0016] In one aspect, the RF transaction device of the present invention may use RF technology to initiate and complete financial transactions. In that regard, the transaction device included in the device may include one or more RF operable transponders and antennas, which are typically included during the transaction device fabrication. The system in which the RF transaction device may be used may include a RFID reader operable to provide a RF interrogation signal for powering the transaction device transponder system, receiving a transponder system RF signal including transponder system account data, and providing transponder system account data relative to the transponder system RF signal although, the transaction device may include its own internal power source. The RFID reader may include an RFID reader protocol/sequence controller in communication with one or more interrogators for providing an interrogation signal to a transponder of the transaction device, a RF authentication circuit for authenticating the signal received from the transponder, and a serial or parallel interface for interfacing with a point-of-interaction device.

[0017] The RFID reader may be configured to send a standing RF recognition signal which may be continuously or intermittently transmitted from the RFID reader via radio frequency (or electromagnetic) propagation. In one instance, the transaction device may be placed within proximity to the RFID reader such that the RF recognition signal may interrogate the device and initialize device identification or authorization procedures.

[0018] In another aspect of the invention, a transaction device is provided which may be issued to a user in a transaction device transporter wherein the user may remove the transaction device from the transporter for use with any form factor. In one exemplary transaction device manufacturing method, a plurality of transporter and transaction devices (called "transaction device combination" herein) is manufactured simultaneously on a single sheet using conventional manufacturing machinery.

Each of the plurality of transaction device combinations is manufactured as a removable subpart the sheet of the plurality of transaction device combinations, wherein each combination may be an independent operable RF transaction device, which is ISO/7810-1985 compliant in size. As such, the transaction device combination may be manufactured, stamped, and/or cut using conventional manufacturing equipment.

[0019] The transaction device transporter, including the removable transaction device, is manufactured with at least one border of the transaction device transporter directly adjacent a border of the next adjacent transporter, forming a sheet of conjoined transaction device transporters. In one embodiment, the sheet of transporters is manufactured including RF operable transaction devices. In one embodiment, the sheet is manufactured with RF operable transaction devices including conventional RF data transmission circuitry.

[0020] Once the sheet of transaction device combinations is manufactured, the sheet may then be fed through a stamping device for imprinting an outline of the transaction device (*e.g.,* key fob) within a single transporter. The outline of the transaction device is imprinted in the transporter with sufficient depth such that the transaction device and the RF module may be removed from the transporter with minimum physical force. The removable transaction device outline is imprinted such that the transaction device RF circuitry (called "RF module" herein), is included within the shape stamped (or imprinted) into the transaction device transporter, with at least a single imprint included within the transporter's borders. As such, the outline of the transaction device may typically serve as the shape of the transaction device which may be removed from the transporter.

[0021] The sheet may then be cut along the borders of the transaction device transporter into conventional transaction card dimensions, such as, for example, the ISO/IEC 7812 standardized card dimensions noted above. Preferably, the sheet is

cut such that the transaction card shaped transaction device combination resulting from the cutting process includes the removable transaction device. The resulting transaction device combination may then be delivered to a transaction device user, who may remove ("punch-out") the removable transaction device from the transaction device transporter by, for example, applying minimal physical force along lines (*e.g.,* alignment lines) defining the shape of the transaction device imprinted on the transporter. Once removed, the RF transaction device may be used to complete a RF transaction since the transaction device includes the RF module. Further, the outline of the imprinting may serve to define the shape of the transaction device. The transaction device manufacturer may predetermine the shape of the transaction device and imprint the predetermined shape in the transporter.

[0022] In another embodiment, the transaction device may not be removed from the transporter. Instead, the transaction device combination may be left intact. The combination may be used to complete a RF transaction since the RF module is included in the transaction device (which is included in the transaction device combination). In this way, the transaction device combination may be used in similar manner as a conventional RF transaction device to complete a transaction. That is, a user may position the transaction device combination in proximity to a RFID reader. The RF module may then provide transaction device account information (*e.g.*, account number, user identifier, device identifier) to the reader, which may forward the information to a merchant system or POS for transaction completion.

[0023] Alternatively, the transaction device combination may be equipped with a traditional magnetic stripe, which is ordinarily ISO/IEC 7800 et al., compliant. The magnetic stripe may include user account data which may be provided to a conventional magnetic stripe reader for completing a transaction using traditional magnetic stripe data processing methods. Thus, the user may use the transporter

and RF transaction device in similar manner as a traditional credit card or debit card, and the like.

[0024] In another exemplary embodiment, the transaction card body is cut and the transaction device outline is imprinted simultaneously. In this instance, the card manufacturer may utilize a cutting machine configured to imprint an outline of the removable transaction device when the cutting of the transporter is performed. In this way, only one machine action is necessary to cut the transporter body and imprint the removable transaction device outline.

[0025] In yet another exemplary embodiment, the transaction device includes a RF module completely contained within the transaction device outline formed by the imprinting action. The transaction device may be formed or shaped using any desired outline. For example, a suitable outline such as an irregularly shaped key fob outline may be pressed (*e.g.*, imprinted) within the perimeter of each of the plurality of transaction device transporters. The transaction device outline may be pressed or imprinted into the transporter such that the RF module is contained within the transaction device outline. The transaction device may then be "punched out" of ("removed from") the transporter by placing minimal physical force at the transaction device outline, such that the resulting RF transaction device is shaped in the transaction device outline provided.

[0026] In yet another exemplary embodiment of the invention, the transaction device manufacturer may manufacture a transaction device sheet including the RF module wherein the sheet may be cut in the traditional credit card ISO/IEC 7800 et al., compliant shapes and the transaction device is cut in any shape as desired for a RF transaction device (*e.g.*, teardrop fob shaped). In this way, a transaction device manufacturer may form both transaction cards and irregularly shaped RF transaction devices on the same sheet simply by designating the proper design or shape to be made.

[0027] In still another aspect, the invention includes a means for securing the transaction device to a user's person or to a user's frequently used personal apparatus. For example, in one particular embodiment, the outline of the transaction device may be shaped to include an opening or aperture for securing the transaction device to, for example, a chain, key ring, ring, watch, rope, or the like. The key ring or chain, for example, may be inserted through the opening to secure the payment device to the chain or key ring to guard against the payment device being easily lost or stolen.

[0028] In another exemplary embodiment, the RF module may be removed from the transaction device for use in completing a transaction independently of the transaction device or the transporter. The outline of the module may additionally be pressed inside a transaction device outline as well, although not required. In this instance, an outline of the RF module may be imprinted on the transaction device transporter wherein the module is positioned inside the transporter outline. The RF module outline may be imprinted or pressed into the transporter at sufficient depth to permit the module to be easily removed, in similar manner as discussed with the transaction device. The module may be removed from the transporter using any of the methods described herein.

[0029] Once removed, the RF module may be secured to a mobile device such as a mobile telephone, PDA or the like, for converting the mobile device for use as a RF transaction device. The module may be secured externally to the mobile device housing using an independent portable carrier, an adhesive or other attachment method. The portable carrier may be attachable to the mobile device and may be configured to encase a portion of the RF module and lock the module in place to the mobile device body.

[0030] In yet another exemplary embodiment, the RF module may be placed in physical and logical communication with the internal functional components of the

mobile device (*e.g.*, mobile device circuitry). The RF module may include electrical connections for communicating with the mobile device microprocessor. In this way, the mobile device may be used to power the RF module, transfer data between the mobile device microprocessor, mobile account issuer, and RF module account issuer, and provide secondary identification means for the RF transaction authentication process, or to personalize the RF module where necessary. Additionally, the RF module may be configured to transmit information to a mobile device universal bus (USB) connector for transmitting the information to an account issuer or merchant system for transaction processing. The mobile device USB connector may permit the RF module to communicate with an issuer or merchant provided kiosk, or to a transaction processing network for transaction completion.

[0031] Additional features and advantages of the present invention are described in, and will be apparent from, the detailed description of the present exemplary embodiments and from the drawings.

Brief Description of the Drawings

[0032] A more complete understanding of the present invention may be derived by referring to the detailed description and claims when considered in connection with the Figures, where like reference numbers refer to similar elements throughout the Figures, and:

[0033] Figure 1 illustrates an exemplary RF transaction device system in accordance with an exemplary embodiment of the present invention;

[0034] Figure 2 illustrates an exemplary prior art transaction card in accordance with an exemplary embodiment of the present invention;

[0035] Figure 3 illustrates an exemplary sheet of plurality of transaction cards in accordance with an exemplary embodiment of the present invention;

[0036] Figure 4 illustrates an exploded view of an exemplary sheet of a plurality of transaction cards including a RF circuitry sheet in accordance with an exemplary embodiment of the present invention;

[0037] Figure 5 depicts the front surface of an exemplary RF transaction device in accordance with an exemplary embodiment of the present invention;

[0038] Figure 6 shows an exemplary RF module in accordance with an exemplary embodiment of the present invention;

[0039] Figure 7 depicts the front surface of an exemplary RF transaction device combination in accordance with an exemplary embodiment of the present invention;

[0040] Figure 8 illustrates an overview of an exemplary method for providing a transaction device to an end user in accordance with exemplary embodiments of the present invention;

[0041] Figure 9 shows an exemplary sheet of a plurality of cojoined transaction device combination each including a RF transaction device, therein, in accordance with an exemplary embodiment of the present invention;

[0042] Figure 10 is an exemplary detailed flowchart of an exemplary method for providing a transaction device to an end user in accordance with exemplary embodiments of the present invention;

[0043] Figure 11 depicts an exemplary transporter and RF module combination in accordance with the present invention;

[0044] Figure 12 depicts an exemplary RF module removed from a transporter in accordance with the present invention;

[0045] Figure 13 depicts an exemplary embodiment of a suitable frequently used portable form factor comprising a recess for including a RF module in accordance with the present invention;

[0046] Figure 14 depicts an exemplary RF module carrier in accordance with the present invention;

[0047] Figure 15 depicts a transaction device combination including a magnetic stripe in accordance with exemplary embodiments of the present invention;

[0048] Figure 16 depicts a transaction device combination with the transaction device removed in accordance with exemplary embodiments of the present invention;

[0049] Figure 17 depicts an exemplary RF module in physical and logical communication with an exemplary mobile device microprocessor in accordance with exemplary embodiments of the present invention;

[0050] Figure 18 depicts an exemplary RF module including electrical contacts for use in a (SIM) slot for converting the mobile device to a RF transaction device in accordance with exemplary embodiments of the present invention;

[0051] Figure 19 depicts an exemplary mobile device including electrical contacts for inclusion of a subscriber identity module (SIM) in accordance with exemplary embodiments of the present invention;

[0052] Figure 20 illustrates an exemplary method for processing a transaction in accordance with exemplary embodiments of the present invention;

[0053] Figure 21 depicts the functional components of an exemplary RFID reader useful with the present invention; and

[0054] Figure 22 depicts an exemplary mutual authentication process in accordance with the present invention.

Detailed Description

[0055] The present invention relates to contactless transaction devices and methods of making and using the same. Specifically, the present invention relates to a system and method for providing a RF transaction device using conventional transaction card manufacturing procedures. The present invention addresses the

shortcomings in the prior art by providing a cost effective method for manufacturing irregular shaped RF transaction devices.

[0056] 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.

[0057] 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).

[0058] Figure 1 illustrates an exemplary Radio Frequency (RF) transaction device system 100 for use with the present invention, wherein exemplary components for use in completing a contactless transaction are depicted. In general, the operation of system 100 may begin when a contactless transaction device 102 is presented for payment. In this context, the transaction device 102 is a device which includes the RF module 20. The device 102 may be presented for payment by, for example, waiving the device 102 in proximity to a RFID reader 104. The RFID reader 104 provides an interrogation signal for powering the device 102 and the transaction device 102 is positioned in such proximity to the reader 104 that the device 102 may be positioned to be in communication with the transaction device 102 via RF transmission of the interrogation signal. The interrogating signal may power the contactless transaction device 102 thereby initiating operation of the device 102. The contactless transaction device 102 may provide a transponder identifier and/or account identifier to the RFID reader 104, via RF transmissions and the reader 104 may further provide the identifier to the merchant system 130 POS device 110 for transaction completion. Details for the operation of an exemplary RF transponder system for transaction completion is found in U.S. Patent Application No. 10/192,488, entitled "SYSTEM AND METHOD FOR PAYMENT USING RADIO FREQUENCY IDENTIFICATION IN CONTACT AND CONTACTLESS TRANSACTIONS," and its progeny which is hereby incorporated by reference.

[0059] Although the point-of-interaction device 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 device account data. In this regard, the POS may be any point-of-interaction device or transaction acceptance device enabling the user to complete a transaction using an RF responsive transponder.

[0060] The RFID reader 104 may be configured to communicate using a RF internal antenna 106. Alternatively, RFID reader 104 may include an external antenna 108 where the external antenna 108 may be made remote to the RFID reader 104 using a suitable cable and/or data link. RFID reader 104 may be further in communication with a transaction completion system (*e.g.*, merchant system 130) via a data link. In one exemplary embodiment the transaction completion system may include POS device 110 in communication with a RFID reader 104 (via a data link), and a customer interface 118 in communication with the POS device 110. The POS 112 may be in further communication with an account issuer system (not shown) via a network 112 which may be provided the account number and any transaction identifying information (*e.g.*, time, duty, cost of transaction, item negotiated) for transaction completion.

[0061] The terms "Internet" or "network" as used herein, 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.

[0062] By being in "communication," what is described may be that a signal may travel to/from one component of the invention 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.

[0063] Where required, the system user may interact with the system to complete a transaction via any input device or user interface 118, 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.

[0064] A variety of conventional communications media and protocols may be used for the data links. For example, 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 130 including the POS device 110 and host network 112 may reside on a local area network which interfaces to a remote network (not shown) for remote authorization of an intended transaction. The merchant system 130 may communicate with the remote network via a leased line, such as a T1, D3 line, or the like. In addition, the merchant system 130, including the POS 110 and host network 112, may reside on a local area network, which interfaces with a

remote network (not shown) for remote transaction authorization. Such communications lines are described in a variety of texts, such as, "Understanding Data Communications," by Gilbert Held, which is incorporated herein by reference.

[0065] A device account identifier or account number, 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.

[0066] In general, the transaction devices 102 which use the above RF transmission process may take any form. The RF module 20 may be included in RF transaction device 102 for use in completing a RF transaction. Any transaction device discussed herein, excluding the RF module 20, may also be termed a mobile device 102, wherein the mobile device is configured to accept the RF module 20. In an exemplary embodiment, the mobile device 102 includes a microprocessor for controlling the mobile device 102 functional components as discussed below. In one embodiment, the mobile device 102 is one whose ordinary function is not for financial transaction completion or the completion of a transaction using loyalty or rewards points, etc. In this instance, the mobile device may be termed a "non-traditional transaction device" herein.

[0067] To facilitate understanding of this invention, Figure 5 illustrates a transaction device 102 shaped as a teardrop shaped transaction device 102, although other configurations are contemplated. Figure 5 shows an exemplary teardrop shaped RF transaction device 102, including RF module 20 for conducting a RF transaction.

[0068] The RF transaction device 102 (described more fully below) may come in many different shapes. Because a typical card manufacturer may provide both

traditional credit card shaped transaction cards and irregularly shaped RF transaction devices, the manufacturer must have proper machinery for cutting sheets of the devices into the appropriate device size. The present invention provides a system and method for forming the irregularly shaped transaction devices, which utilizes conventional dimensional standards for transaction cards (*e.g.*, credit cards, smart cards, etc.) irrespective of the RF transaction device shape. This, in turn, allows the manufacturer to manufacture irregularly shaped transaction devices using conventional card manufacturing machinery, with little retrofitting. The invention allows for a manufacturer to use coextensive transaction card and RF transaction device manufacturing processes which produce both transaction devices simultaneously or individually. The process is termed coextensive since identical material layers and/or circuitry may be used whether the card manufacturer desires to cut transaction cards or RF transaction devices.

[0069] Figure 2 depicts the dimensional relationship of an exemplary transaction card 1. Transaction card 1 is shown with dimensional characteristics which conform to the ISO card size standard, typically ISO/IEC 7800 et al. Generally, transaction card 1 is about 2" X 3.5".

[0070] Manufacturers of transaction cards 1 take advantage of mass production techniques when manufacturing transaction cards. Instead of producing the cards 1 individually, the cards 1 are produced en masse in sheets 200 which are then cut into the appropriate individual size. Figure 3 is a depiction of an exemplary sheet 200 of a plurality of transaction cards 1, which may be manufactured using a conventional transaction card manufacturing process.

[0071] Sheet 200 may be prepared using any conventional method of manufacturing a sheet of multiple transaction devices 1. The present invention modifies conventional methods by including perforation, impressing and RF circuitry as discussed below. The following description is an exemplary method of

manufacturing sheet 200 according to the invention. The description is offered to facilitate a understanding of the invention and not by way of limitation.

[0072] In the exemplary embodiment shown, sheet 200 may be formed using multiple material layers. Figure 4 illustrates an exploded view of an exemplary sheet 200, which may be used with the present invention. Sheet 200 includes a front material layer 10 and back material layer 12 consisting of a plastic substrate such as, for example, clear core PVC. One skilled in the art will appreciate that layers 10 and 12 of card 1 may be any suitable transparent, translucent and/or opaque material such as, for example, plastic, glass, acrylic and/or any combination thereof. Each material layer 10, 12 is substantially identical and is preferably about 3' X 4' (622mm X 548mm) and about 0.005-0.350 inches, or more preferably 0.01-0.15 inches or 13.5 mil thick.

[0073] The fabrication of the individual card sheets 200 may include either direct layout (9 layers) of film or the use of a sub-assembly (5 layers). An exemplary sub-assembly layer 21 may consist of 5 layers of film with room temperature tack adhesive applied over thermoset and thermoplastic adhesives. The resulting cards comprise (from the card front towards the card back) 2.0 mil outer laminate (PVC, polyvinylchloride) including having a holographic foil, embossed surface, chip and other indicia on its surface, 9.0 mil printed PVC core with print side out (card front), 2.0 mil PVC adhesive, 1.7 mil PET GS (extrusion coated polyethyleneterephthalate - gluable/stampable) manufactured by D&K (525 Crossen, Elk Grove Village, Illinois 60007), 2.0 mil PET IR blocking film, 1.7 mil PET GS, 2.0 mil PET adhesive, 9.0 mil printed PVC core with the print side out (card back), and 2.0 mil outer back laminate with a signature panel, applied magnetic stripe and other indicia. Optimally, the PET IR blocking film is fabricated in the middle of the layers to balance the card and minimize warping of the resulting card product.

[0074] After eventually combining the sheets, by preferably adhering the front layer 10 on top of the back sheet 12, the total thickness of the transaction card 1, including the subassembly sheet 21, is about .032 in. (32 mil.), which is within the ISO thickness standard for smart cards. In one embodiment, the subassembly sheet 21 may be formed including RF module 20, which may be of sufficient thickness to maintain the smart card standard thickness. Alternatively, the RF module 20 may be embedded in the sheet 12 or card 1 via a suitable conventional milling process. Because the RF module 20 (called "RF module 20" herein) may eventually embedded into the surface of the substrate or the subassembly 21 as described more fully below, the module 20 does not affect the thickness of the overall card 1. Moreover, the about 3' X 4' sheets include predefined alignment markings which define the boundaries of the individual cards 1 to be cut from the sheet. Each exemplary sheet yields over 50 transaction cards (typically 56 cards), wherein each card 1 is within the ISO card size standard, namely about 2" X 3.5".

[0075] In an exemplary embodiment, certain compounds are printed over the surface of sheets 10 and 12. The compounds may be printed in accordance with accepted ISO standards. One skilled in the art will appreciate that the printing of the text 30 and logo 50, and optically recognizable ink may be applied to any surface of card 1 such as, for example, the front 10 face (front material layer 10), the rear 12 face (rear material layer 12), the inside or outside surface of either face, between the two sheets of base material and/or a combination thereof. Moreover, any suitable printing, scoring, imprinting, marking or like method is within the scope of the present invention.

[0076] The text 30 and logo 50 are printed on the outside surface of each material layer 10, 12 by a known printing process, such as an offset printing process, which provides a thinner ink coverage, but clearer text. More particularly, with respect to offset printing, the artwork is duplicated onto a metal plate and the metal plate is

placed onto an offset press printing machine which can print up to four colors during a single run. The offset printed text may include, for example, a corporate name, a copyright/trademark/patent notice, a batch code number, an "active thru" date, contact telephone numbers, legal statements and/or the like. The exemplary offset text may be printed in 4DBC in opaque white ink or a special mix of Pantone Cool Gray 11 called UV AMX Gray. In one exemplary embodiment, the offset printed text is printed directly on the RF module 20, such that the text is visible on the module 20 through casual inspection.

[0077] A laminate material layer 15 is applied to the back layer 12 of card 1. In one preferred embodiment, the laminate layer 15 includes rows of ISO compliant magnetic stripes 40, wherein each magnetic stripe 40 corresponds to an individual card 1. The magnetic stripe 40 may extend along one length of the card 1 and is applied to the back surface 12. The magnetic stripe 40 may be any width, length, shape, and placed on any location on card 1. In an exemplary embodiment, the magnetic stripe 40 is applied to the outer laminate layer 15 using a tape layer machine which bonds the cold peel magnetic stripe 40 to the outer laminate 15 when it is in a rolled position (not shown). The laminate 15 roll with a rolling hot die and at suitable pressure. The roll is then cut into layers 10, 12 before the card layers are assembled.

[0078] After the desired printing is complete and the magnetic stripe applied, the front 10 and back 12 material layers are placed together, and the layers are preferably adhered together by any suitable adhering process, such as a suitable adhesive. One skilled in the art will appreciate that, instead of printing on two material layers and combining the two material layers, a single plastic material layer can be used, wherein the single material layer is printed on one side, then the same material layer is re-sent through the printer for printing on the opposite side.

[0079] In the present invention, after adhering the layers together, a layer of lamination (not shown), approximately the same dimensions as the plastic sheets, namely 3' X 4', may be applied over the front 10 and back 12 of card 1. After the laminate is applied over the front 10 and back 12 of the combined plastic material layers, card 1 layers are suitably compressed at a suitable pressure and heated at about 300 degrees, at a pressure of between 90-700 psi, with a suitable dwell time to create a single card 1 device. The aforementioned card fabrication can be completed by, for example, Oberthur Card Systems, 15 James Hance Court, Exton, Pennsylvania.

[0080] In an exemplary embodiment, the card layers 10 and 12 are fused together in a lamination process using heat and pressure. During the hot press phase, the press is heated to about 300F degrees and the pressure builds to about 1000 psi and holds for about 90 seconds. The pressure then ramps up to about 350 psi over an about 30-second period and holds for 16 minutes at the same temperature, namely 300F degrees. The sheet 200 is then transferred to a cold press which is at about 57F degrees. The pressure builds to about 400 psi and is held for about 16 minutes as chilled water of about 57F degrees is circulated in the plates. The cold press then unloads the sheet 200.

[0081] In one exemplary manufacturing embodiment, the cards 1 may include internal circuitry for use in completing contactless transactions. For example, card 1 may include a RF module 20 included in the card body and preferably may be included in subassembly sheet 21. The RF module 20 is preferably positioned substantially central to the card body but may be positioned at any desired location therein. The RF module 20 may be included interposed between front surface material layer 10 and back surface material layer 20 during fabrication of the sheet 200. Specifically, the module 20 may be included interposed between at least two layers of the subassembly sheet 20. Alternatively, after lamination, the RF module

20 may be included within an individual card 1 within a space created by milling the card body and providing room for the insertion of the RF module 20. As such, upon including the RF module 20, sheet 200 will comprise a plurality of RF operable transaction cards 1 wherein each transaction card 1 includes a RF module 20. Traditional methods for including RF module 20 in transaction devices 1 are well known, and are intended to be within the scope of the invention.

[0082] Figure 6 illustrates a block diagram of the many functional components of an exemplary RF module 20 in accordance with the present invention. Module 20 may include any conventional RF circuitry capable of communicating via Radio Frequency transmission. A suitable module 20 may be presented by the user to facilitate an exchange of funds or points, etc., for receipt of goods or services.

[0083] RF module 20 may include an antenna 204 for receiving an interrogation signal from RFID reader 104 via antenna 106 (or alternatively, via external antenna 108). Module antenna 204 may be in communication with a transponder 214. In one exemplary embodiment, transponder 214 may be a 13.56 MHz transponder compliant with the ISO/IEC 14443 standard, and antenna 204 may be of the 13 MHz variety. The transponder 214 may be in communication with a transponder compatible modulator/demodulator 206 configured to receive the signal from transponder 214 and configured to modulate the signal into a format readable by any later connected circuitry. Further, modulator/demodulator 206 may be configured to format (*e.g.*, demodulate) a signal received from the later connected circuitry in a format compatible with transponder 214 for transmitting to RFID reader 104 via antenna 204. For example, where transponder 114 is of the 13.56 MHz variety, modulator/demodulator 206 may be ISO/IEC 14443-2 compliant.

[0084] Modulator/demodulator 206 may be coupled to a protocol/sequence controller 208 for facilitating control of the authentication of the signal provided by RFID reader 104, and for facilitating control of the sending of the module 20 account number. In

this regard, protocol/sequence controller 208 may be any suitable digital or logic driven circuitry capable of facilitating determination of the sequence of operation for the module 20 inner-circuitry. For example, protocol/sequence controller 208 may be configured to determine whether the signal provided by the RFID reader 104 is authenticated, and thereby providing to the RFID reader 104 the account number stored on module 20.

[0085] To authenticate the signal, the protocol/sequence controller 208 may be further in communication with authentication circuitry 210 for facilitating authentication of the signal provided by RFID reader 104. Authentication circuitry may be further in communication with a non-volatile secure memory database 212. Secure memory database 212 may be any suitable elementary file system such as that defined by ISO/IEC 7816-4 or any other elementary file system allowing a lookup of data to be interpreted by the application on the chip. Database 212 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. Database 212 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.

[0086] The data received from the reader 104 or the database 212 may be used by protocol/sequence controller 208 for data analysis and used for management and control purposes, as well as security purposes. Authentication circuitry 216 may authenticate the signal provided by RFID reader 104 by association of the RF signal to authentication keys stored on database 212. Authentication circuitry 216 may be in further communication with an encryption circuitry 216 which may encrypt or decrypt the reader 104 signal or the data (*e.g.*, account number, user identifier, device identifier, etc.) returned from database 212 prior to transmitting the data. Encryption circuitry 216 may use keys stored on database 212 to perform encryption and/or decryption of signals sent to or from the RFID reader 104.

[0087] In addition, protocol/sequence controller 208 may be in communication with a database 212 for storing at least one of a module 20 account data, a unique module 20 identification code, user identification code, or transaction device identifier. Protocol/sequence controller 208 may be configured to retrieve the account number from database 212 as desired. Database 212 may be of the same configuration as database 212 described above. The account data and/or unique device identification code stored on database 212 may be encrypted prior to storage. Thus, where protocol/sequence controller 208 retrieves the account data, and or unique transaction device identifier, or the like, from database 212, the data may be encrypted by the encryption circuit 216 when being provided to RFID reader 104. Further, the data stored on database 212 may include, for example, an unencrypted

unique module 20 identification code, a user identification ISO/IEC, Track 1 and 2 data, as well as specific application applets. The data may additionally be stored in the database 212 in Track 1 / Track 2 format and may also be in Track 1 / Track 2 format when provided to the reader 104

[0088] In one exemplary embodiment, module 20 antenna 218 may be 134 KHz rated configured to communicate with a 134 KHz transponder 214. In this exemplary configuration, an ISO/IEC 14443-2 compliant modulator/demodulator 206 may not be required. Further still, reader 104 may also include an antenna 106, 108 and a transponder modulator which is also ISO/IEC 1443-2 complaint to ensure successful RF communication with correspondent components at module 20.

[0089] In an exemplary operation, the module 20 is placed in proximity to reader 104 when the user wishes to conduct a transaction. The user simply waves the module 20 at a certain distance from the RF-based reader 104 until the reader 104 acknowledges that the information contained in the RF module 20 has been received. The RF-based reader 104 then utilizes at least a portion of the information provided by module 20 (such as, a user's account number associated with the transaction device) to complete the transaction. The reader 104 may receive the account information from the module 20 and verify the account information authenticity prior to forwarding the account information to merchant system 130. Alternatively, the reader 104 may forward the account information to a merchant system 130 (via the merchant system POS 110) which may provide the account information to a transaction device issuer system (via network 112) for transaction completion. The merchant system 130 forwards the account information to an account issuer system, which may complete the transaction under issuer defined business as usual protocol. Exemplary transaction completion methods and transaction device components are disclosed in the commonly owned 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, incorporated herein in its entirety.

[0090] With reference to Figure 3, after the card sheet 200 is prepared, including the RF module 20, the sheets may be cut into individual cards 1 by a known stamping process, including any necessary curing, burrowing, heating, cleaning and/or sealing of the edges. The individual transaction cards 1 are about 2" X 3.5" and conform to ISO standards for transaction card 1 shape and size. As used hereinafter, the transaction card 1 is termed the transaction device "transporter," since the transaction device issuer may provide the RF module 20 to a user when the module 20 is still affixed to the transporter 1 as described below.

[0091] In an exemplary embodiment, the laminated sheet 200 of 56 transaction device transporters 1 (including the RF module) are suitably cut in half on a guillotine device, resulting in two half-sheets of 28 transporters 1 and module 20 combinations. The half-sheets may be loaded onto any conventional card punch machine which aligns the sheets to a die (x and y axes) using predetermined alignment marks 202 visible to the optics of the machine. The half-sheets are then fed under a punch to punch out the desired transporter device 1 and module 20 (called "transaction device combination") shape. Particularly, a fixed distance feed is followed by another optic sensor search to stop the feed at the preprinted alignment mark, then the machine punches a row of four transaction device combinations out at one time, each punch being made along a preprinted alignment mark 202.

[0092] The preprinted alignment marks 202 indicate the perimeter boundaries of each transaction device transporter 1 to be cut from sheet 200. To separate each transaction device combination from the other, the cuts may typically be made along the preprinted alignment marks 202. In general, the preprinted alignment marks 202 are included in the sheet 200 as the writing is being added to the device material

layers 10, 12. A typical sheet 200 may yield over 50 transaction device combinations (typically 56). In general, the shape of the transporter 1 is kept consistent by using a cutting apparatus having a preformed cutting dye formed in the desired shape. For example, the cutting dye may be formed in any shape, such as, for example, a traditional credit card shape as shown in Figure 1. Alternatively, the shape is cut by using, for example, a laser or other cutting apparatus guided by any suitable preprinted alignment marks 202. The resulting individual transaction device combination may then be distributed for immediate activation and use.

[0093] Conventional methods of fabricating, manufacturing and cutting transaction devices, such as, credit cards, smart cards, RF key fobs are well known. As such, one skilled in the art will understand the machinery and processes for fabricating, manufacturing, and/or cutting as they are included in the scope of this invention. Indeed, in the interest of brevity, conventional methods of fabricating, manufacturing and cutting transaction devices will not be discussed in detail herein. For instruction on manufacturing and fabricating a typical transaction card, see U.S. Patent Application No. 10/092,681, entitled "TRANSACTION CARD," filed March 7, 2002, and incorporated herein in its entirety.

[0094] While the foregoing describes an exemplary embodiment for the fabrication of transaction device combination, one skilled in the art will appreciate that any suitable method for incorporating text 30, logos 50, a magnetic stripe 40, a signature field, holographic foil 15 onto a substrate in accordance with accepted 160 standards, is within the scope of the present invention. Moreover, the holographic foil, RF module 20, logo 50, magnetic stripe 40, signature field or any other compound may be included on the transporter 1 by any suitable means such as, for example, heat, pressure, adhesive, grooved and/or any combination thereof. In accordance with one embodiment, the text 30, logo 50, magnetic stripe 40, or holographic foil 15 may

additionally be included in one surface use of the module 20 on a portion easily viewable by casual inspection.

[0095] As noted, various card manufacturers are producing RF transaction devices that are irregularly shaped. As such, the irregular shaped transaction devices are typically cut using a cutting dye, or other method discussed above, which is designed to cut a sheet 200 into the desired transaction device shape. Consequently, manufacturers must often retrofit their machinery to cut the irregular shape. Returning now to Figure 5, a teardrop shaped RF transaction device (key fob) 500 is shown. To provide transaction devices of similar shape as device 102, a card manufacturer may typically use a cutting machine including a teardrop shaped cutting dye, or a cutting means guided by the preprinted device 102 alignment marks 502 (also shown in Figure 7). As can be seen, the RF transaction device 102 may include a logo 50.

[0096] In accordance with one aspect of the invention, a credit card manufacturer may provide an irregularly shaped RF transaction device 102 using a manufacturing process that is coextensive with the manufacturing process used for traditional transaction card 1 shapes. That is, the transaction devices 102 and transporters 1 may be manufactured, cut, perforated, or impressed without need to manufacture the devices independently of the transporter 1. Figure 8 depicts an exemplary overview of any transaction device combination manufacturing method according to the invention. As shown in Figure 8, and with continued reference to Figure 7, a transaction device sheet 200 (shown best in Figure 9) including a plurality of conjoined RF transaction device combinations 1 is provided using any of the manufacturing methods discussed herein (step 802). The transporter 1 may include an outline of irregularly shaped transaction devices 102 defined by alignment marks 502. Alignment marks 502 may ordinarily be imprinted and pressed within the outline of the transporter 1 defined by the preprinted alignment marks 202. The

sheet 200 may be prepared using conventional RF transaction device and transaction card fabricating methods. The outline of the irregular shaped removable RF transaction device 102 which is shown as preprinted alignment marks 502 in Figure 7, may be pressed into, and contained substantially inside, the preprinted alignment marks 202 of the transporter 1 (step 804). The alignment marks 502 may be pressed into the surface of the transponder and substantially therethrough. In one embodiment, the alignment marks 502 are pressed into the surface of the transporter 1 such that the transporter 1 and transaction device 102 are in physical contact. However, the irregular shaped removable RF transaction device 102 may then be removed from (*i.e.*, "punched out" of) the transporter 1 by using minimal physical force at preprinted alignment marks 202 (step 806). The resulting RF transaction device 102 may then be used in completing a RF transaction under any merchant or account provider business as usual standards (step 808).

[0097] To assist in punching out or removing the transaction device 102, the RF transaction device 102 preprinted alignment marks 502 may be pressed into the body of transporter 1 defined by preprinted alignment marks 202. As noted, the transporter 1 may be formed with one or more material layers, such as, for example, front layer 10, and back layer 12. The pressing action may result in indentations, or perforations being impressed into or through one or more layers of the multilayer transaction device. However, the perforations or indentations may not traverse completely through the card body. Instead, the perforations or indentations are impressed at such sufficient depth to permit the transaction device 102 to be removed from the transporter 1 with the application of minimal physical force. Thus, the perforations or indentations are typically provided along the transaction device 102 preprinted alignment marks 502 to facilitate the removal of the transaction device 102 from the transporter body. In one exemplary embodiment, the perforations and indentations, which may be used to form the outline of the

transaction device 102, may also be arranged to form an outline of a shape, a picture, a security enhancing visage, or the like as desired by the manufacturer or system user. Suitable methods for providing perforations are disclosed in U.S. Patent Application No. 10/288,945, entitled "PERFORATED TRANSACTION CARD," filed November 6, 2002, incorporated herein by reference in its entirety.

[0098] Figure 10 illustrates various exemplary embodiments of a method for providing to a user RF transaction device 102 which may be removed from a transporter 1. In accordance with step 802, each exemplary embodiment begins with the fabrication of a multilayer sheet 200 of a plurality of conjoined transaction device combinations.

[0099] In accordance with one exemplary embodiment of the present invention, the transaction device 102 outline (lines 502) is impressed within the outline of the transporter 1 drawn by alignment marks 202. For example, the preprinted sheet 200 of transaction device combinations is provided with the transporter 1 alignment marks 202 preprinted on the combination's front or rear surface 10, 12, and the transaction device outline 502 ("alignment marks 502") is impressed within the alignment marks 502 (step 804).

[00100] Once the impression of the transaction device 102 is made in the transporter 1, the transaction device manufacturer may remove the transaction device 102 from the transporter 1 and provide the transaction device 102 to an end user. In one exemplary embodiment, the transaction device 102 is removed from the transporter 1 by the manufacturer (step 808) prior to providing the transaction device 102 to a user for device activation and device usage (step 810). In this way, the transaction device 102 may be provided to a user independent of the transporter 1. The user may use the transaction device 102 to complete a transaction by placing the transaction device 102 in proximity to the reader 104 as described above (step 830).

[00101] In an alternate embodiment of the invention, the RF transaction device 102 is not removed by the manufacturer, but instead the RF transaction device 102 is removed from the transporter 1 by the end user (step 812). For example, a transaction device provider may provide a user with the transaction device combination, including the transporter 1, and the transaction device 102, which includes RF module 20 (step 814). The user may then decide whether to remove the transaction device 102 from the transporter 1, which may be removed at the user's leisure (step 816). Should the user remove the transaction device 102, the user may additionally decide whether to remove module 20 (step 818). The user may remove the transaction device 102 to complete a transaction independent of the transporter 1 (step 830). The user may remove the transaction device 102 from transporter 1 by applying minimal physical force at the transaction device outline 502. The transaction device 102 may be removed manually or by cutting, tearing, or the like, (step 820). The user may use the transaction device 102 by placing the transaction device 102 in proximity to reader 104, as described above (step 830). The RF module 20 may then provide transaction device account information to a RFID reader 104 for transaction completion.

[00102] The transaction device 102 may include an aperture 503, which may be formed by pressing the shape of the aperture 503 in the transporter 1 along alignment lines 502, perforating the transaction device 102 shape in the transporter 1 using any conventional machinery or method as described above. The aperture 503 may then be punched out or removed, wherein the portion of the transporter 1 within the aperture 503 is removed leaving an opening therein. The transaction device 102 may then be secured to a user's person or often used personal article by inserting one end of a tether-like means (not shown) through aperture 503 and securing the other end of the tether-like means to a transaction device 102 user person or often used personal article (*e.g.*, keychain, fob chain, key ring, string,

strap, belt, rope, etc.) which is ordinarily easily portable (step 820). The user may then use the transaction device 102 in similar manner as discussed above (step 830).

[00103] In another exemplary embodiment of the invention, user or transaction device manufacturer may remove the RF module 20 from the transporter 1 to enable use of the module 20 to complete a transaction independent of any other portion of the transporter 1 or the transaction device 102 (step 822). In this instance, the transaction device issuer may configure the stamping machinery to preprint alignment marks which closely mimic the shape of the module 20. As shown in Figure 11, the transporter 1 may include a square shaped module 20 including alignment marks 220. In similar manner as previously described, the issuer may perforate the transporter 1 along the alignment marks 220 to facilitate easy removal of the module 20 from the transporter 1 by the user or the issuer. The module 20 outline may be pressed substantially, but not completely, through transporter 1 body. In this way, the user may remove module 20 from transporter 1 with minimal physical force (step 822). The user may then use the module 20 to complete a RF transaction by positioning the module 20 in proximity to the reader 104 in similar manner as was described with the transaction device 102 (step 830).

[00104] Figure 12 shows the RF module 20 removed from the transporter 1. As shown, the module 20 may include the offset printed text described above (*e.g.*, logo, text 30, logo 50, active through date, telephone numbers, etc.), which is perceptible to the casual observer by visual inspection. The module 20, may be a self-contained device in that the module may be used to complete transactions irrespective of the transporter 1. In exemplary embodiment, the module 20 may be of sufficient size that it is easily punched out or removed from the transporter 1. For example, the module may be 1x1 9/16", although other suitable sizes are contemplated.

[00105] In one exemplary embodiment, the user may use the module 20 with any portable form factor configured to secure the module 20 during transaction completion (step 824). In one embodiment, the form factor is embodied in an article frequently used by the module user. For example, the module 20 may be secured to any portable apparatus which may be manually transported by the module 20 user, and which may be used to facilitate manually presenting the module 20 to a RFID reader 104 for transaction completion. A suitable portable apparatus may include means for securing the module 20 to the apparatus.

[00106] Figure 13 shows an exemplary apparatus for securing and presenting the module 20 for transaction completion which may be used in accordance with the present invention. As shown, the apparatus may be a nontraditional transaction device, such as, a conventional cellular phone 300 although any portable form factor including a microprocessor may be used. For example, the apparatus may be a personal digital assistant (PDA), mini personal computer or the like. The cellular phone 300 may include a recess 302 which may be configured to accept the module 20 therein. The recess 302 may be included in one surface of the phone 300 at sufficient depth to substantially recess the RF module 20 therein, to secure the module 20. The recess 302 may further be configured to hide the RF module 20 from view. The module 20 may thereby be inserted in the recess 302 and secured by any fastening means such as clips, molded clips and fittings, screws, glue, soldering or the like. The module 20, may be inserted into the recess 302 of the cellular phone 300 prior to providing the phone 300 to the user. Alternatively, the module 20 may be provided to the user in a transaction device combination, and the module may be removed from the transporter 1 and the transaction device 102 and inserted in the recess 302 by the user. Further still, the module 20 may be provided to the user in the transporter 1 or the transaction device 102, and the user may remove the module 20 at the user's leisure.

[00107] In yet another exemplary embodiment, as shown in Figure 14, a portable carrier 400 may be provided to the user for securing the module 20 during transaction completion. Carrier 400 may be of any desired shape and may be of sufficient size to substantially enclose the module 20 in use. The carrier 400 may be constructed of any durable or sturdy material such as metal, plastic, composite materials or the like. The carrier 400 may additionally be transparent or translucent to permit casual viewing of the module 20 when the module 20 is secured therein.

[00108] For example, in the embodiment shown, carrier 400 is of similar shape as the module 20 depicted in Figure 12 (*e.g.*, square), although the carrier 400 may take any shape. In one embodiment, the carrier 400 may be dimensionally larger than the module 20 to ensure that the module may be enclosed therein although any carrier 400 shape or size may be used. The carrier 400 may include a recess 402 in which the module 20 may be snuggly fitted. The carrier 400 may include a first 404 and second 406 carrier door. First 404 and second 406 carrier door may include the recess 402 included in one panel of each door. The recess 402 forms a cavity when the doors 404, 406 are positioned one on the other. The module 20 may be secured in the cavity. The doors 404 and 406 may be in communication along one side by hinges 408, which permit the doors 404, 406 to be closed one on top of the other with the module 20 interposed in between. The doors 404, 406 may be secured one to the other by the hinges 408 and a suitable latch 410 configured to ensure that the doors 404, 406 remain fastened one to the other and the module 20 remains inside the carrier 400 during transaction completion.

[00109] Carrier 400 may further include an aperture 412 in at least one end of the door 404, 406. The aperture 412 may be used in similar manner as with aperture 503 of Figure 7. That is, the carrier 400 (which may include the module 20) may be secured to a user's person or to an apparatus the user frequently handles.

[00110] Alternatively, the carrier may be secured to the apparatus, such as cell phone 300 using any suitable attachment method. For example, the carrier 400 including the module 20 may be fastened to the cell phone 300 using any attachment means, such as for example, screws, rivets, bonding compound, glue or especially made fastening construction operable to hold the carrier 400 in physical communication with the cell phone 1402. For example, one suitable attachment method may be the fastener described in U.S. Patent No. 6,669,263, entitled "Attachment Device," which issued December 30, 2003, to Asai, and U.S. Patent No. 6,643,076, entitled "Attachment Device," which issued November 4, 2003, to Montage, hereby incorporated by reference.

[00111] Returning now to Figure 8, in yet another exemplary method, the user may not wish to remove the module 20 or the transaction device 102 from the transporter 1 (steps 816 and 826). Instead, the user may wish to use the transaction device combination to complete a transaction. That is, the transaction device combination may be used with the module 20 and the transporter 1 intact. Figure 15 shows an exemplary depiction of a transaction device combination 600 in accordance with the present invention which may be used to complete a transaction. Figure 15 depicts a transaction device combination 600 which includes a transporter 1 and a RF module 20. The combination 600 may further include the impression of the transaction device 102 although not required. For example, the transporter 1 may include alignment lines 502 which trace a shape of a transaction device 102 including the RF module 20 the shape of which may be "formed from impressed alignment lines 220. Perforations may be made along the alignment lines 502, 220 which trace at least one of the shape of transaction device 1508 or the module 20.

[00112] The transporter 1 may be configured with a magnetic stripe 40 using any conventional method for attaching magnetic stripes as is commonly known. The magnetic stripe 40 may be compliant to International Standard Setting Organization

standards for the shape, location and the format of the data stored and retrieved from the magnetic stripe 40. The magnetic stripe 40 may be configured to include account data (*e.g.*, account, user, or transaction device identifier, code or number) stored thereon in Track 1 / Track 2 ISO magnetic stripe standard format. As such, the magnetic stripe 40 may be configured to be readable by any conventional magnetic stripe reader as is found in the art. Consequently, the user may use the transaction device combination 600 in similar manner as a traditional credit, debit, DDA, prepaid card, an the like. For example, the user may present the transaction device combination 600 to a magnetic stripe reader, which may retrieve the magnetic stripe 40 data and forward the data to an account issuer for transaction completion. Conventional methods for completing a transaction are well known and will not be repeated for brevity.

[00113] In one conventional construction of transaction device combination 600, the magnetic stripe 40 may be such that a portion of the alignment lines 502, including the impressed outline of the transaction device 102 may intersect the magnetic stripe 40, as shown in Figure 15 at character reference 608. In this way, the transaction device 102 outline overlaps the magnetic stripe 40. As such, the transaction device 102 including module 20 may be removed from the transporter 1 and a portion of the magnetic stripe 40 is removed therewith as shown in Figure 16. In this way, the user ensures that the transporter 1, including the remaining portion of the magnetic stripe 40, may not be used to complete transactions. This is true, since the magnetic stripe 40 will have a portion 606 of the magnetic stripe 40 removed when the device 102 is removed, thereby making the magnetic stripe 40 inoperable for transmitting complete magnetic stripe information. That portion 606 of the magnetic stripe 40, which is removed, may ordinarily be included as a portion of the transaction device 606 to ensure that the magnetic stripe 40 may be disabled when the transaction device 102 is removed. Once removed, the transaction device

102, or the module 20 may be used to complete a transaction in similar manner as was discussed above.

[00114] In still another exemplary embodiment, the removed RF module 20 may be placed in physical and logical communication with a microprocessor of a mobile device, such as for example, the cell phone 300 discussed with regard to Figure 3. As shown in Figure 17, the phone 300 may include a microprocessor 1702 for controlling the operation of the phone 300. The microprocessor 1702 may be in communication with a mobile device database such as cell phone database 1704, for data storage and retrieval. For example, in the case of cell phone 300, database 1704 may store personal contact information, calendars, pictures, or the like. The cell phone 300 may also include a modulator/demodulator 1706 connected to the processor 1702 and a cell phone antenna 1708, for transmitting signals received from the antenna 1708 to the microprocessor 1702. RF module 20 may be placed in physical or logical communication with the microprocessor 1702 using any conventional coupling methods for connecting electrical components.

[00115] In another exemplary method for placing the RF module 20 in physical and logical communication with microprocessor 1702, the RF module 20 may include contact points that are compatible with a mobile device expansion card slot. Expansion cards are typically cards which contain instructions or data which the processor may use to enhance the functionality of an electronic device including a processor or microprocessor. One popular example of an expansion card is the subscriber identity module (SIM).

[00116] Ordinarily, SIMs are configured to provide control applications to the mobile device for controlling and increasing the device's functionality. Most SIMs are in the form of a chip card that establishes the subscriber relationship with the mobile phone system operator. The chip card typically includes electrical contacts which mate with electrical contacts of the mobile device for placing the chip card in communication

with the mobile device processor. The mobile device mating contacts are usually included in a slot formed in the housing of the mobile device for receiving and securing the chip card thereto.

[00117] The SIMs are personalized with an IMSI, Ki, etc., prior to providing the SIMs to the mobile device user, at a "personalization" center run by the mobile phone network operator. Important individual subscriber data saved on the SIM facilitates the use of the mobile phone services. The SIM contains the mobile subscriber identification (IMSI), the secret individual subscriber key (Ki) an authentication algorithm (A3), a ciphering key generating algorithm (A8), a personal identification number (PIN) and other permanent and temporary data. The SIM contains at least one microchip which holds information on the subscription and which, when the SIM card is inserted in a mobile terminal, is connected thereto.

[00118] However, SIMs have a major drawback in that the SIMs ordinarily do not influence the behavior of the mobile device by managing presentation of new services (or software applications) to the user. To mitigate that drawback, GSM Recommendation 11.14 phase 2.sup.+ defines the ground rules for implementing a toolkit in the subscriber identity module, and for enabling operators to create their own specific applications independently of the mobile terminal used, provided that the terminal is compatible with GSM Recommendation 11.14 phase 2.sup.+. Furthermore, to make it possible to dialog with and to use the toolkit, GSM Recommendation 11.11 phase 2.sup.+ specifies the mechanisms that make the two portions (the mobile terminal and the subscriber identity module) interoperable. In other words, the SIMs may have commands available that it can have executed by the terminal.

[00119] For additional explanation on SIMs operation and protocol, please refer to ETSI publications prepared by various ETSI workgroups: GSM 02.19 Digital cellular telecommunications system (Phase 2+), Subscriber Identity Module Application

Programming Interface (SIM API), Service description; Stage 1; GSM 02.48 Digital cellular telecommunications system (Phase 2+), Security mechanisms for the SIM application toolkit; Stage 1; GSM 03.19 Subscriber Identity Module Application Programming Interface (SIM API); SIM API for Java Card (TM), Stage 2; GSM 03.48 Digital cellular telecommunications system (Phase 2+), Security Mechanisms for the SIM application toolkit; Stage 2; GSM 11.11 Digital cellular telecommunications system (Phase 2); Specification of the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface; (GSM 11.11); GSM 11.14: Specification of the SIM application toolkit for the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface; WAP WIM Wireless Application Protocol Identity Module Specification, available (for free) at www.wapforum.org; 3G TS 21.111 Version 3.0.0, USIM and IC Card Requirements; entitled Removable User Identity Module (R-UIM) for Spread Spectrum Systems (3GPP2 C.S0023) of December 9, 1999; CDMA Development Group Document #43, Smart Card Stage I Description, Version 1.1, May 22, 1996; GSM 02.17 - Subscriber Identity Module (SIM); Functional Characteristics; 3GPP 22.038 - SIM Application Toolkit (SAT), Stage 1; 3GPP 22.112 - USIM Toolkit Interpreter Stage 1; 3GPP 31.102 - Characteristics of the USIM Application; 3GPP 31.111 - USIM Application Toolkit (USAT); 3GPP 31.113 - USAT Interpreter Byte Codes; 3GPP 31.131 - C API for the USIM Application Toolkit; 3GPP 34.131 - Test Specification for the C SIM API; SCP 101.220 Integrated Circuit Cards (ICC); ETSI Numbering System for Telecommunication; Application Providers (AID); SCP 102.221 Smart Cards; UICC-Terminal Interface; Physical and Logical Characteristics; SCP 102.222 Integrated Circuit Cards (ICC); Administrative Commands for Telecommunications Applications; SCP 102.230 Smart Cards; UICC-Terminal interface; Physical, Electrical and Logical Test Specifications; SCP 102.223 - Smart Cards; Card Application Toolkit (CAT); SCP 102.224 Security mechanisms for the Card Application Toolkit: Functional requirements; SCO

102.225 - Secured packet structure for UICC applications; SCP 102.226 - Remote APDU Structure for UICC based Applications; SCP 102.240 - UICC Application Programming Interface, and all related text, which is hereby incorporated by reference.

[00120] While the SIMs are useful for expanding the functionality of the mobile devices, conventional SIMs are useful for converting the mobile device into a transaction device useful in completing transactions. The present invention solves this problem by providing a RF module configured to communicate with a mobile device microprocessor using connectors contained on the mobile device. For example, RF module may be configured to fit within a SIM slot and mate with a mobile device, SIM connectors.

[00121] Figure 18 depicts an exemplary alternate embodiment of RF module 20 including electrical connectors 1802 configured to communicate with, and be compatible with, conventional SIM connectors on a mobile device, such as, cell phone 300. RF module 20 of Figure 18 may have similar description as module 300. However, in this instance RF module 20 includes electrical connectors 1802 which may be in communication with the module protocol/sequence controller 208. The connectors 1802 may additionally place the RF module protocol/sequence controller 208 in communication with the mobile device microprocessor (*e.g.*, cell phone microprocessor 1702), for transmitting information thereto. Notably, the module 20 may be manufactured and provided to the end user using any of the methods described herein, for example, by using the methods described in Figures 8 and 10.

[00122] Figure 19 depicts the module 20 including connectors 1802 placed in physical and logical communication with the electrical connectors 1902 of a mobile device, such as, cell phone 300. As shown, the electrical connectors 1802 are placed in contact with the connectors 1902 so that information may be communicated between the RF module 20 and the microprocessor 1702. As described more fully

below, the cell phone 300 in communication with RF module 20 may be converted into a RF transaction device for completing a RF transaction.

[00123] Figure 20 illustrates an exemplary transaction processing method using the RF module placed in physical and logical communication with a mobile device microprocessor as described above. Figure 20 is best understood with reference to Figure 1, Figure 6, and Figure 21 described below. As illustrated, the transaction device 102 is a mobile device, such as for example, mobile phone 300, that is configured to process a transaction using a RF module 20 in physical and logical communication with the microprocessor 1702 of the mobile device 300. The RF module 20 is provided to the end user using any of the methods described herein. In one example, the RF module 20 is provided integral to the mobile device housing and in physical and logical communication with the microprocessor 1702. In this way, the RF module 20 may be included in the mobile device when the device is manufactured. In a separate example, the RF module 20 is provided to the end user independently of the mobile device. The RF module 20 is placed in communication with the mobile device microprocessor using electrical connectors.

[00124] With brief reference to Figures 6 and 21, the functional components of an exemplary RFID reader 104 is described. As shown, RFID reader 104 may include an antenna 2104 for providing an interrogation signal from RFID reader 104 to the RF module 20 antenna 204. RFID reader 104 antenna may be in communication with a reader transponder 2114. In one exemplary embodiment, transponder 2114 may be a 13.56 MHz transponder compliant with the ISO/IEC 14443 standard, and antenna 2104 may be of the 13 MHz variety. The transponder 2114 may be in communication with a modulator/demodulator 2106 configured to receive the signal from transponder 2114 and configured to modulate the signal into a format readable by any later connected circuitry. Further, modulator/demodulator 2106 may be configured to format (*e.g.*, demodulate) a signal received from the later connected

circuitry in a format compatible with transponder 2114 for transmitting to RF module 20 via antenna 2104. For example, where transponder 2114 is of the 13.56 MHz variety, modulator/demodulator 2106 may be ISO/IEC 14443-2 compliant.

[00125] Modulator/demodulator 2106 may be coupled to a protocol/sequence controller 2108 for facilitating control of the authentication of the signal provided by RF module 20, and for facilitating the formatting of the data received from RF module 20 in a format compatible with, for example, a merchant POS 110. In this regard, protocol/sequence controller 2108 may be any suitable digital or logic driven circuitry capable of facilitating determination of the sequence of operation for the RFID reader 104 inner-circuitry. For example, protocol/sequence controller 2108 may be configured to determine whether the signal provided by the RF module 20 is authenticated, and thereby providing to the RF module 20 account number to the merchant POS 110.

[00126] Protocol/sequence controller 2108 may be further in communication with authentication circuitry 2110 for facilitating authentication of the signal provided by RF module 20. Authentication circuitry 2110 may be further in communication with a non-volatile secure memory database 2112. Secure memory database 212 may be of similar description as database 212 described above. Authentication circuitry 2110 may authenticate the signal provided by RF module 20 by association of the signal to authentication keys stored on database 2112. Encryption circuitry 2116 may use keys stored on database 2112 to perform encryption and/or decryption of signals sent to or from the RF module 20.

[00127] Returning now to Figure 20, a typical transaction in accordance with this invention is described. The transaction may begin when an end user presents the transaction device (*e.g.*, 300) including a RF module 20 for transaction processing (step 2002). The RFID reader 104 provides an interrogation signal to the RF module 20 for activating the RF module 20 for transaction processing (step 2004). The RF

module 20 receives the interrogation signal (step 2006) and the RF module 20 and the RFID reader 104 engage in mutual authentication to determine if each is a valid device for operation on system 100 (step 2008).

[00128] Figure 22 is a flowchart of an exemplary authentication process in accordance with the present invention. The authentication process is depicted as one-sided. That is, the flowchart depicts the process of the RFID reader 104 authenticating the RF module 20, although similar steps may be followed in the instance that RF module 20 authenticates RFID reader 104. In some embodiments, the RF module 20 and the RFID reader 104 may engage in mutual authentication. In this context, "mutual authentication" may mean that operation of the system 100 may not take place until RF module authenticates the signal from RFID reader 104, and RFID reader 104 authenticates the signal from RF module 20.

[00129] As noted, database 2112 may store security keys for encrypting or decrypting signals received from RF module 20. In an exemplary authentication process, where RFID reader 104 is authenticating RF module 20, RFID reader 104 may provide an interrogation signal to RF module 20 (see step 2002 of Figure 20). The interrogation signal may include a random code generated by the RFID reader authentication circuit 2110, which is provided to the RF module 20, and which is encrypted using a unique encryption key corresponding to, for example, a RF module 20 unique identification code. In a typical scenario, the protocol/sequence controller 2108 may provide a command to activate the authentication circuitry 2110. Authentication circuitry 2110 may provide from database 2112 an interrogation signal including a random number as a part of the authentication code generated for each authentication signal. The authentication code may be an alphanumeric code which is recognizable (*e.g.*, readable) by the RFID reader 104 and the RF module 20. The authentication code may be provided to the RF module 20 via antenna 2104 (step 2202).

[00130] RF module 20 receives the authentication code (step 2204). The interrogation signal including the authorization code may be received at the RF module antenna 204. The authorization code may be provided to the modulator/demodulator circuit 206 where the signal may be demodulated prior to providing the signal to protocol/sequence controller 208. Protocol/sequence controller 208 may recognize the interrogation signal as a request for authentication of the RF module 20 (step 2206), and provide the authentication code to authentication circuit 210. Authentication circuit 210 or protocol/sequence controller 208 may retrieve an encryption key from database 212 and authentication circuit 210 may encrypt the authentication code using the retrieved encryption key (step 2208). RF module 20 may then provide the encrypted authentication code to the RFID reader 104 for verification (step 2210). The encrypted authentication code may be provided to the RFID reader 104 via RF module modulator/demodulator circuit 206, transponder 214, and antenna 202.

[00131] RFID reader 104 may then receive the encrypted authentication code and decryption it (step 2212). That is, the encrypted authentication code may be received at antenna 2104 and transponder 2114, and provided to authentication circuit 2110. Authentication circuit 2110 may be provided a security authentication key (*e.g.*, transponder system decryption key) from database 2112. The authentication circuit 2110 may use the authentication key to decrypt (*e.g.*, unlock) the encrypted authorization code. The authentication key may be provided to the authentication circuit 2110 based on the RF module 20 unique identification code. For example, the encrypted authentication code may be provided along with the unique RF module 20 identification code. The authentication circuit 2110 may receive the RF module 20 unique identification code and retrieve from the database 2112 a transponder system decryption key correlative to the unique RF module 20 identification code for use in decrypting the encrypted authentication code.

[00132] Once the authentication code is decrypted (step 2212), the decrypted authentication code is compared to the authentication code provided by the RFID reader 104 to verify its authenticity (step 2214). If the decrypted authorization code is not readable (*e.g.*, recognizable) by the authentication circuit 2110, the RF module 20 is deemed to be unauthorized (*e.g.*, unverified) (step 2216) and the operation of system 100 is terminated (step 2218). Contrarily, if the decrypted authorization code is recognizable (*e.g.*, verified) by the RF module 20, the decrypted authorization code is deemed to be verified or authenticated (step 2220), if so, the transaction is allowed to proceed (step 2222). In one particular embodiment, the proceeding transaction may mean that the RF module 20 may authenticate the RFID reader 104, although, it should be apparent that the RFID reader 104 may authenticate the RF module 20 prior to the RF module 20 authenticating the RFID reader 104.

[00133] With return reference now to Figure 20, upon successful mutual authentication, the RF module 20 transfers to the RFID reader 104 such data as is necessary to process a transaction request ("user account data") (step 2210).

[00134] The RFID reader 104 receives the user account data at the antenna 2104, and provides the data to the POS interface 2120 (step 2012). In one exemplary embodiment, the RFID reader authentication circuit 2110 may receive the data and provide the data to the RFID reader interface 2120. The RFID reader interface 2120 may then receive the data and convert the data to a merchant POS 110 recognizable format for providing to the merchant system 130. In an exemplary embodiment, the user account data is provided to the RFID reader 104 in magnetic stripe format. In yet another embodiment, the RFID reader 104 provides the user account data to the merchant POS 110 in magnetic stripe format.

[00135] The merchant system 130 may receive the user account data and use the data to form a transaction request (step 2014). The transaction request may include the user account data and any information related to the transaction. The merchant

system 130 may provide the transaction request to a user account issuer for processing under business as usual standards (step 2016). Notably, the transaction applications for processing the authentication signal and providing the user account data may be stored in a transaction application on for example, in the database 212 for use by the authentication circuit 210.

[00136] In one exemplary embodiment of the invention, the transaction device 102 (*e.g.*, mobile phone 300) may include a USB interface 2122 in communication with the protocol/sequence controller 2108. In this exemplary embodiment, the USB interface 2122 may be a RS22 serial data interface. Alternatively, the RFID reader 104 may include a serial interface such as, for example, a RS232 interface in communication with the protocol/sequence controller 2108. In either embodiment, the interface may be in communication with the protocol/sequence controller 2108 for providing user account data from the RF module 20 for transaction processing, using, for example, the transaction processing method of Figure 20.

[00137] To facilitate the user account data transfer from the RF module 20 to the interface 2122, the mobile phone 300 may be equipped with a USB interface 304 (shown in Figure 13) or the like. The mobile device USB interface 304 may be included in the mobile device 300, when the phone 300 is manufactured and prior to providing the phone to the end user. The mobile device USB interface 304 may be placed in communication with the USB interface 2122. In that regard, USB interface 304 may be compatible with USB interface 2122, such that the data received from the mobile phone 300 is recognizable by the RFID reader 104.

[00138] In a typical embodiment, the RF module 20 is in physical and logical communication with the mobile device (*e.g.*, mobile phone 300) microprocessor 1702, for transmitting user account data from the RF module 20 to the RFID reader 104. The module protocol/sequence controller 208 may retrieve the user account data from the module database 212 and provide the data to the microprocessor

1702. The microprocessor 1702 may then provide the user account data to the USB interface 304 for providing to the RFID reader USB interface 2122. USB interface 2122 may receive the user account data and provide the data to a merchant POS 110 for processing as described above.

[00139] It should be noted that although the present invention is described with respect to the mobile device USB being connected to a USB of a RFID reader 104, the invention is not so limited. For example, the mobile device USB may be connected to a similar port (*e.g.*, USB port) included on a kiosk, or personal computer, stand alone computing device, or the like. In this case, the user account data may be transmitted from the mobile device to the kiosk or other computer and to an offline or online account issuer or merchant system for transaction processing via an open or closed network. In this instance, an "open" network is one susceptible to eavesdropping.

[00140] Placing the RF module 20 in physical and logical communication has the advantage in that the RF module 20 may be powered by a power source of the mobile device. That is, the RF module 20 may share a similar power source as does the functional components of the mobile device. Another advantage is that the mobile device's user interface may be used to verify secondary information from the end user.

[00141] For example, the RF module 20 may need to be switched on prior to use for transaction completion. In this case, the end user may use the mobile device user interface (*e.g.*, keyboard 306) to enter a alphanumeric code for powering the RF module 20. The alphanumeric code may be received by the microprocessor 1702 and forwarded to the protocol sequence controller 2108 to commence a transaction using the RF module 20. In another instance, the end user may provide an alphanumeric code in response to a request from the RFID reader 104 for further authentication of the end user's identity. For example, the RFID reader 104 may

send a message to the RF module 20 that a secondary form of identification, such as a personal identification number (PIN), is required before a transaction may proceed. The RFID reader authentication circuit 2110 may receive a signal from the RF module 20 and recognize that the end user's identity may need to be verified using a PIN. The authentication circuit 2110 may then provide the RF module 20 with a request for the end user to provide the PIN before the RF module provides the user account data to the RFID reader 104.

[00142] In one exemplary embodiment, the reader 104 may provide the request for a PIN to the RF module 20 at antenna 204. The RF module transponder 214 may receive the request and provide the request for PIN to the protocol/sequence controller 208. The protocol/sequence controller 208 may provide the request to the mobile phone microprocessor 1702, and the microprocessor 1702 may send a prompt to the mobile device display unit, such as the display unit 308 of mobile phone 300. The display unit 308 may be any conventional display units that are used with mobile personal communication devices, such as, mobile phones, PDAs, personal computers or the like. Suitable display units which may be used with the invention include a liquid crystal display unit (LCD), image display device, or the like. The display unit may be any display unit capable of displaying messages to the end user.

[00143] The end user may then be permitted to input the PIN using the keypad user interface 306. The PIN may be provided to the microprocessor 1702, which may provide the PIN to the module protocol/sequence controller 208. The protocol/sequence controller 208 may provide the PIN to the module authentication circuit 210, which may retrieve from the database 212 (or from encryption circuit 216) a PIN verification key and use the verification key to authenticate the PIN. The authentication circuit 210 may use any authentication method as is found in the art, or disclosed herein to verify the PIN. In one exemplary embodiment, the

authentication circuit 210 may compare the PIN provided by the end user to the PIN verification key using any comparison method permitting the authenticity of the PIN to be verified.

[00144] Alternatively, the RF module protocol/sequence controller 208 may provide the PIN to the RFID reader 104 for authentication. The RFID reader authentication circuit 210 may receive the PIN and verify the PIN in a similar manner as is discussed with respect to the RF module 20.

[00145] Notably, the method by which the end user provides the PIN to the microprocessor 1702 may vary. For example, the user interface may include a touch screen display and a stylus as is found in the art. Additionally, the secondary form of identification may be provided using biometric or voice recognition technology. The mobile device may receive the biometric or voice data and convert it into data recognizable by the RF module protocol/sequence controller 208 for verification using the methods discussed above.

[00146] 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. Thus, the preceding detailed description is presented for purposes of illustration only and not of limitation, and the scope of the invention is defined solely by the appended claims and their legal equivalents when properly read in light of the preceding description. 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. In addition, although the present description illustrates the invention as embodied in a card, key fob, or cellular phone, the invention is not so

limited. That is, the present invention contemplates the incorporation of the inventive technology into a form factor presentable by hand.

Claims

1. A method for providing a Radio Frequency (RF) transaction solution to a nontraditional transaction device comprising:

a. receiving user account data from a transaction application stored on a RF module for use in transaction completion, the RF module in physical and logical communication with a nontraditional transaction device microprocessor; and

b. processing the user account data for transaction completion.

2. A method according to claim 1, comprising:

receiving the user account data from the RF module, where the user account data is provided subsequent to authentication of an end user secondary identifier, the secondary identifier being provided for authentication by the end user at a mobile device interface.

3. A method of claim 2, comprising receiving the user account data from the RF module via a mobile device universal serial bus (USB), the USB in communication with the RF module via the microprocessor.

4. A method of claim 3, comprising receiving the user account data via a user interface in communication with the mobile device USB.

5. A method of claim 1, wherein the RF module is integral to the mobile device housing, the RF module in electrical communication with the mobile device microprocessor.

6. A method of claim 1, wherein the RF mobile device is configured to communicate with the microprocessor using mobile device electrical connectors in communication with the microprocessor.

7. A method of claim 6, wherein the mobile device electrical connectors are configured to accept a subscriber identity module (SIM).

8. A method of claim 1, wherein the RF module is International Standards Organization ISO/IEC 14443 compliant.

9. A method of claim 1, mobile device includes a user interface configured to provide secondary identification to the microprocessor in response to a request for secondary identification for end user authentication, the request for secondary identification being provided to the end user via the user interface, the secondary identification being one of voice recognition data, biometric recognition data and alphanumeric data.

10. A method of claim 1, comprising receiving a user account data from a RF module, the RF module being activated by a mobile device user interface.

11. A method of claim 10, wherein mobile device activates the RF mobile device prior to transaction processing.

12. A system for providing a RF payment solution to a mobile device, comprising a RF module configured to be in physical communication with a nontraditional mobile device, the RF module including database for storing user account data and a transponder for transmitting the user account data via radio frequency, the database including a transaction application.

13. A system of claim 12, wherein the RF module is in physical and logical communication with a mobile device microprocessor, the mobile device being a nontraditional transaction device.

14. A system of claim 13, wherein the RF module is configured to provide user account data for transaction processing, the RF module being configured to provide the user account data via a mobile device USB port.

15. A system of claim 12, wherein the RF module is configured to provide the user account data subsequent to the verification of an end user provided secondary identification code, the mobile device including a user interface, the user interface being configured to receive the secondary identification code and provide the secondary identification code to the RF module for authentication.

16. A system of claim 13, wherein the mobile device is configured to activate the RF module prior to transaction processing.

17. A computer-readable storage medium containing a set of instructions for a general purpose computer configured for:

a. receiving user account data from a transaction application stored on a RF module for use in transaction completion, the RF module in physical and logical communication with a nontraditional transaction device microprocessor; and

b. processing the user account data for transaction completion.

18. A computer-readable storage medium of claim 17 for:

receiving the user account data from the RF module, where the user account data is provided subsequent to authentication of an end user secondary identifier, the secondary identifier being provided for authentication by the end user at a mobile device interface.

19. A computer-readable storage medium of claim 17 for receiving the user account data from the RF module via a mobile device universal serial bus (USB), the USB in communication with the RF module via the microprocessor.

20. A computer-readable storage medium of claim 17 for receiving a user account data from a RF module, the RF module being activated by a mobile device user interface.